Prawne i społeczne aspekty cyberbezpieczeństwa

pod redakcją
Sylwii Gwoździewicz
Krzysztofa Tomaszyckiego

Prawne i społeczne aspekty cyberbezpieczeństwa

pod redakcją
Sylwii Gwoździewicz
Krzysztofa Tomaszyckiego

Warszawa 2017

Redakcja naukowa:
Sylwia Gwoździewicz *(Wydział Administracji i Bezpieczeństwa Narodowego Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim)*
Krzysztof Tomaszycki *(Instytut Socjologii Wydział Nauk Społecznych Uniwersytetu Wrocławskiego, Komenda Głowna Policji)*

Komitet redakcyjny:
Amelin Oleksander, Błażejczak Karina, Chernovol Valeriia, Frankowski Gerard, Garwol Katarzyna, Goździewicz Sylwia, Gugulski Marcin, Jureczka Marlena, Konieczny Radosław, Kordaczuk – Wąs Marzena, Krupa Monika, Krzemińska Beata, Łazarski Daniel, Meyer Norbert, Miłostan Maciej, Nosov Vitalii, Nowocień Tomasz Adam, Orzechowska Anna, Popov Georgii, Prokopowicz Dariusz, Rvachov Oleksii, Sztumski Janusz, Tomaszycki Krzysztof, Wolaniuk Leszek.

Recenzja:
dr hab. Mieczysław Goc, prof. Wyższej Szkoły Bankowej w Gdańsku
Wiceprezes Polskiego Towarzystwa Kryminalistycznego w Warszawie
dr hab. Jan Maciejewski, prof. Uniwersytetu Wrocławskiego,

ISBN 978-83-945923-2-5

Wydawca / Publisher
Międzynarodowy Instytut Innowacji «Nauka – Edukacja – Rozwój» w Warszawie
International Institute of Innovativeness «Science-Education-Development» in Warsaw
www.instytutinnowacji.edu.pl
kontakt@instytutinnowacji.edu.pl

© Copyright by Authors
All Rights Reserved / Wszelkie prawa zastrzeżone. Kopiowanie, przedrukowywanie i rozpowszechnianie całości lub fragmentów niniejszej publikacji bez zgody autorów zabronione.
Drukowane wydanie I / ISBN 978-83-945923-2-5
Nakład / Paper copies: 100 egzemplarzy
Skład: Krzysztof Tomaszycki
Druk: Drukarnia Arebours.pl / Otwock
Projekt okładki: Krzysztof Tomaszycki / Magdalena Kośmider

Warszawa 2017

Spis treści:

Wstęp

Innowacje w technologiach informatycznych permanentnie wyznaczają tendencje do zapewnienia i tworzenia różnych ram cyberbezpieczeństwa. Wraz z rozwojem technologii sukcesywnie powinne być dostosowywane krajowe normy prawne do regulacji międzynarodowych, a w szczególności do prawa unijnego w zakresie zwalczania cyberprzestępstw i zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Zatem jeśli społeczeństwo XXI wieku definiowane jest już jako społeczeństwo informacyjne, to warto zadać szereg pytań:

- jakie znaczenie ma obecnie kwestia ochrony informacji (zwłaszcza tych prywatnych, wśród których dominującą rolę odgrywają dane osobowe),
- jaka jest ochrona baz danych i tajemnicy przedsiębiorstwa,
- jaka jest ochrona oprogramowania i infrastruktury krytycznej państwa,
- jaka jest ochrona osób małoletnich i rodzin w cyberprzestrzeni,
- jaką rolę i zadania w cyberbezpieczeństwie powinny pełnić służby państwowe i administracja publiczna oraz
- jak powinna wyglądać współpraca międzynarodowa w tym obszarze?

Podjęta Unijna ***Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*** oraz ***Strategia Cyberbezpieczeństwa RP na lata 2016-2022*** mają na celu poprawę bezpieczeństwa cybernetycznego, w tym także bezpieczeństwa społecznego i prawnego. Założeniem powyższych strategii jest uczynienie środowiska internetowego Państw Członkowskich Unii Europejskiej (PC UE) najbezpieczniejszym na świecie. Realizując strategię UE musi zwiększyć bezpieczeństwo w cyberprzestrzeni poprzez ustanowienie wspólnej polityki w tym zakresie na poziomie unijnym i krajowym. Strategia UE zakłada m.in. wprowadzenie przepisów prawnych, ustanawiających minimalne wymogi w zakresie bezpieczeństwa sieci i informacji na poziomie krajowym. Państwa członkowskie powinny już posiadać bądź powinny utworzyć w wyniku wyżej wymienionych strategii i innych przyjętych dyrektyw unijnych, własne strategie a przede wszystkim struktury przeznaczone do działań w zakresie odporności cybernetycznej, cyberprzestępczości i cyberobrony. Jednym z priorytetów jest osiągnięcie „poziomu zdolności" wymaganego do celów skutecznego

reagowania na incydenty cybernetyczne. Ponadto, podmioty działające na poziomie krajowym w sektorach takich jak: finanse, opieka zdrowotna, energetyka, transport i administracja publiczna muszą same dokonywać oceny zagrożeń bezpieczeństwa systemów informatycznych oraz zostały zobligowane do wymiany informacjami z krajowymi organami ds. bezpieczeństwa sieci i informacji, które powinny współpracować między sobą w całej UE. Według Komisji Europejskiej istnieje ryzyko, że Europa staje się nadmiernie uzależniona nie tylko od technologii informatycznych pochodzących z zewnątrz, ale również od rozwiązań w zakresie procedur bezpieczeństwa opracowanych poza jej granicami. Wg strategii cyberbezpieczeństwa należy zagwarantować, aby elementy sprzętu i oprogramowania produkowane w UE oraz importowane z państw trzecich, a które są stosowane w kluczowych usługach i w kluczowej infrastrukturze były wiarygodne i bezpieczne a także gwarantowały ochronę przetwarzanych danych osobowych. Wymogi te powinny dotyczyć również urządzeń mobilnych użytkowanych przez podmioty publiczne jak i przez osoby prywatne.

Przepisy i normy mające zastosowanie życiu codziennym, mają również zastosowanie w odniesieniu do cyberprzestrzeni. Zgodnie z tym, aby cyberprzestrzeń pozostała otwarta i wolna, w środowisku internetowym powinny mieć zastosowanie te same normy, zasady i wartości, które UE wspiera w świecie rzeczywistym. W cyberprzestrzeni należy zapewnić ochronę praw podstawowych, demokracji i praworządności. Nasza wolność, co za tym idzie i nasz dobrobyt w coraz większym stopniu uzależnione są od szybkiej, sprawnej i skutecznej wymiany informacji. Medium do wymiany informacji to internet, który dzięki innowacjom utrzymał swoją kluczową rolę w wspieraniu sektora prywatnego i społeczeństwa obywatelskiego. Wolność w środowisku internetowym wymaga jednak bezpieczeństwa i ochrony. Cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami, przy czym znaczącą rolę w zapewnieniu wolnej i bezpiecznej cyberprzestrzeni odgrywają administracje rządowe PC UE. Mają one szereg zadań: zapewnienie dostępu i otwartości, poszanowanie i ochronę praw podstawowych w internecie oraz utrzymanie jego niezawodności i interoperacyjności. Znaczna część cyberprzestrzeni jest jednak w posiadaniu i użytkowaniu sektora prywatnego i dlatego wszelkie inicjatywy w dziedzinie cyberbezpieczeństwa, jeśli mają

prowadzić do sukcesów, muszą uwzględniać jego wiodącą rolę. należy zaznaczyć, że technologie informacyjno-komunikacyjne stanowią obecnie fundament wzrostu gospodarczego i są zasobem o krytycznym znaczeniu, na którym opierają się finanse, opieka zdrowotna, energetyka czy transport. Ich złożoność a także różnorodność nie dają gwarancji ich bezpieczeństwa. Stanowią one obecnie podstawę złożonych systemów, które napędzają gospodarkę, ale z drugiej strony muszą być chronione, aby rozwój przebiegał bez zakłóceń i zdarzeń krytycznych. Funkcjonowanie w ramach poszczególnych układów społeczno-gospodarczych musi się opierać na nieprzerwanej dostępności internetu oraz sprawnym i niezawodnym funkcjonowaniu systemów teleinformatycznych.

W niniejszym opracowaniu zostanie podjęta próba odpowiedzi na pytanie, jak obecnie w perspektywie działań UE i Strategii Cyberbezpieczeństwa RP na lata 2016-2022 kształtują się prawne, technologiczne i społeczne aspekty cyberbezpieczeństwa. Istotne z punktu widzenia podjętego tematu jest również identyfikacja nowych zagrożeń, jakie generuje środowisko przestępcze w cyberprzestrzeni. Międzynarodowi badacze różnych problemów cyberbezpieczeństwa współpracujący ze sobą w różnych instytucjach naukowych oraz sektorach państwowych i prywatnych podjęli trud opisania uwarunkowań funkcjonowania bezpieczeństwa nie tylko tego realnego ale także wirtualnego. Owocem wzajemnej i międzynarodowej współpracy jest powstanie niniejszego opracowania pt. ***Prawne i społeczne aspekty cyberbezpieczeństwa,*** składającego się z dwóch części.
Pierwsza część zatytułowana ***Prawne i technologiczne aspekty cyberbezpieczeństwa*** zawiera rozważania na temat:

- prywatności w sieci w ujęciu przepisów prawa i analiz badawczych;
- rozwoju złośliwego oprogramowania ransomware jako nowego wymiaru cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków;
- rozwoju cyberprzestrzeni jako zagrożenia dla bezpieczeństwa baz danych;
- analizy bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware;

- automatycznego systemu identyfikacji daktyloskopijnej w policyjnej cyberpodprzestrzeni;
- outsourcingu cyberbezpieczeństwa w świetle problematyki współczesnych zagrożeń w cyberprzestrzeni;
- determinantów rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych; systemu dozoru elektronicznego w Polsce oraz
- wybranych problemów bezpieczeństwa systemów do zdalnej automatycznej identyfikacji opartej na RFID.

W drugiej części pt. ***Społeczne aspekty cyberbezpieczeństwa*** zostały zaprezentowane dotychczasowe wyniki międzynarodowych badań m.in. w zakresie:

- koncepcji cyberprzestrzeni;
- procesu migracji - realne czy wirtualne zagrożenie;
- szkolenia policjantów w aspekcie zastosowania kryminalistyki cyfrowej w dochodzeniu cyberprzestępstw;
- propagandy i świadomości w procesie radykalizacji - wzmacniania i osłabianie czynników ryzyka w cyberprzestrzeni;
- patologii cyfrowego dzieciństwa;
- cyberprzestrzeni jako miejsca spotkań migrantów i rodzin globalnych;
- „papierowego małżeństwa" jako efektu kontaktów w cyberprzestrzeni oraz
- kwestii dotyczących badania przestępstw związanych z cyberprzestępczością na Ukrainie.

Szczególne podziękowania składamy dla Pana dr hab. Mieczysława Goca, profesora Wyższej Szkoły Bankowej w Gdańsku, wiceprezesa Polskiego Towarzystwa Kryminalistycznego w Warszawie oraz Pana dr hab. Jana Maciejewskiego, profesora Uniwersytetu Wrocławskiego za recenzje naukowe oraz bezcenne wskazówki merytoryczne i techniczne udzielane podczas realizacji niniejszej monografii.

Sylwia Gwoździewicz i Krzysztof Tomaszycki

Nota o autorach:

Podrozdział	Autor	Afiliacja
2.8.	**Amelin Oleksander**	chief scientific officer of Scientific Research Institute of National Prosecution Academy of Ukraine e-mail: amelin.saha@mail.ru
2.7.	**Błażejczak Karina**	kpt. SG mgr Instytut Socjologii Wydział Nauk Społecznych Uniwersytetu Wrocławskiego e-mail: k.blazejczak@interia.pl
2.3.	**Chernovol Valeriia**	Narodowy Uniwersytet Spraw Wewnętrznych w Charkowie e-mail: kalerija97@gmail.com
1.5.	**Frankowski Gerard**	Poznańskie Centrum Superkomputerowo-Sieciowe e-mail: gerard.frankowski@man.poznan.pl
1.1.	**Garwol Katarzyna**	dr Wydział Matematyczno-Przyrodniczy, Uniwersytet Rzeszowski e-mail: kgarwol@ur.edu.pl

Podrozdział	Autor	Afiliacja
1.4. **1.7.**	**Gwoździewicz** **Sylwia**	dr Wydział Administracji i Bezpieczeństwa Narodowego Akademia im. Jakuba z Paradyża w Gorzowie Wielkopolskim Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie e-mail: sylwiagwozdziewicz@gmail.com
1.3.	**Gugulski** **Marcin**	mgr Instytut Socjologii Wydział Nauk Społecznych Uniwersytet Wrocławski e-mail: marcing@crann.pl
2.6.	**Jureczka** **Marlena**	mgr Instytut Socjologii Wydział Nauk Społecznych Uniwersytet Wrocławski e-mail: marlena.jureczka@gmail.com
1.6.	**Konieczny** **Radosław**	Poznańskie Centrum Superkomputerowo-Sieciowe e-mail: radoslaw.konieczny@man.poznan.pl
2.4.	**Kordaczuk –** **Wąs Marzena**	mł. insp. dr Komenda Główna Policji e-mail: mk-w@wp.pl

Podrozdział	Autor	Afiliacja
2.5.	**Krupa Monika**	mgr Wydział Nauk Pedagogicznych Akademia Pedagogiki Specjalnej w Warszawie e-mail: monika.krupa.ol@wp.pl
1.5.	**Krzemińska Beata**	podinsp. mgr Centralne Laboratorium Kryminalistyczne Policji e-mail: beata.krzeminska@policja.gov.pl
1.8.	**Łazarski Daniel**	mgr Sąd Okręgowy Warszawa - Praga w Warszawie Akademia Pedagogiki Specjalnej im. Marii Grzegorzewskiej w Warszawie e-mail: lazarskidaniel@gmail.com
1.6.	**Meyer Norbert**	dr inż. Poznańskie Centrum Superkomputerowo-Sieciowe e-mail: meyer@man.poznan.pl
1.6.	**Miłostan Maciej**	dr inż. Poznańskie Centrum Superkomputerowo-Sieciowe, Instytut Informatyki Politechniki Poznańskiej e-amail: maciej.milostan@man.poznan.pl

Podrozdział	Autor	Afiliacja
2.3.	**Nosov Vitalii**	dr prof. katedry Cyberbezpieczeństwa Narodowego Uniwersytetu Spraw Wewnętrznych w Charkowie e-mail: vitnos.g@gmail.com
1.6.	**Nowocień Tomasz Adam**	mgr inż. Poznańskie Centrum Superkomputerowo-Sieciowe e-mail: nowocien@man.poznan.pl
1.3.	**Orzechowska Anna**	mgr Instytut Socjologii Wydział Nauk Społecznych Uniwersytet Wrocławski e-mail: orzechowskaania1@gmail.com
2.8.	**Popov Georgii**	prorector – director of Scientific Research Institute of National Prosecution Academy of Ukraine e-mail: georgepopov3000@gmail.com
1.2. **1.4.** **1.7.**	**Prokopowicz Dariusz**	dr Wydział Nauk Historycznych i Społecznych, Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie e-mail: darprokop@poczta.onet.pl

Podrozdział	Autor	Afiliacja
2.3.	**Rvachov Oleksii**	starszy wykładowca katedry Cyberbezpieczeństwa Narodowego Uniwersytetu Spraw Wewnętrznych w Charkowie e-mail: rvachyov@ukr.net
2.1.	**Sztumski Janusz**	prof. zw. dr hab. dyrektor Instytutu Nauk Społecznych, Górnośląska Wyższa Szkoła Handlowa im. Wojciecha Korfantego, Katowice. e-mail:
2.2. **2.7.**	**Tomaszycki Krzysztof**	mł. insp. dr inż. Instytut Socjologii Wydział Nauk Społecznych Uniwersytet Wrocławski Komenda Główna Policji e-mail: ktomaszycki@wp.pl
1.9.	**Wolaniuk Leszek**	ppłk rez. dr inż. Wydział Nauk o Bezpieczeństwie Wyższa Szkoła Oficerska Wojsk Lądowych imienia generała Tadeusza Kościuszki we Wrocławiu e-mail: l.wolaniuk@wso.wroc.pl

1. Prawne i technologiczne aspekty cyberbezpieczeństwa

1.1. Prywatność w sieci w ujęciu przepisów prawa i analiz badawczych

Definicje prywatności

Problematyka prywatności pojawia się w różnych dyscyplinach nauki. Jej koncepcje funkcjonują w psychologii, prawie, socjologii, antropologii, filozofii, ekonomii, a także w architekturze, urbanistyce, planowaniu przestrzennym czy poradnictwie psychologicznym. W każdej z tych dyscyplin rozpatrywane są jednak inne aspekty prywatności. Filozofowie uważają ją za jeden z podstawowych wymiarów ludzkiej egzystencji i postrzegają ją jako stan bycia implikujący wolność i odpowiedzialność. Podobnie do tego zagadnienia podchodzą prawnicy według których jest ona zasadniczym jednostkowym uprawnieniem podlegającym ochronie prawnej. Psychologowie podkreślają jej znaczenie dla rozwoju „Ja". Socjologowie skupiają się natomiast na roli jaką pełni prywatność w utrzymywaniu relacji interpersonalnych oraz w szczególności związków o charakterze intymnym. W takim ujęciu lokuje się ona w obszarze mikrosocjologii, funkcjonowania grup społecznych oraz problematyce więzi społecznych i zagadnień dynamiki interakcji (Dopierała, 2013, s.13).

Wraz z rozwojem technologii oraz możliwości internetu prywatność znalazła się w obszarze szczególnego zainteresowania naukowców, polityków, publicystów oraz specjalistów z branży IT. Wydaje się być zasadnym pytanie, jak rozległy jest obszar prywatności współczesnego człowieka, który nieustannie nagrywany jest przez kamery ulicznego monitoringu, „namierzany" przez stacje telefonii komórkowej gdy przemieszcza się wraz ze swoim telefonem, każda jego aktywność w internecie jest rejestrowana a służby państwowe posiadają różnego stopnia uprawnienia do nagrywania rozmów telefonicznych i śledzenia korespondencji e-mailowej. Czy prywatność we współczesnym świecie jest więc jedynie pozorna?

Te kwestie od czasu boomu technologicznego znalazły istotne miejsce w naukowym dyskursie a badacze w zależności od dyscypliny, którą reprezentują toczą ze sobą na tym polu zaciekłe spory. Prywatność jest bowiem

wielowymiarowa i nie można jej rozpatrywać jednostronnie. Burgoon określa prywatność jako możliwość kontrolowania i ograniczania dostępu jednostki (lub grupy do której należy) w jednym z czterech wymiarów (Kołodziejczyk, 2014, s. 18):

- Wymiar fizyczny – stopień do jakiego jednostka jest fizycznie dostępna dla innych. Przestrzeń biologiczna może tu być naruszona np. przez obserwację, wykrocznie w osobistą przestrzeń czy bezpośredni kontakt;
- Wymiar interakcyjny – zwany także społecznym lub komunikacyjnym. Określany jest przez możliwość oraz wysiłek jaki niezbędny jest to kontrolowania kontaktów z innymi (np. ich długości trwania, częstotliwości, treści komunikatów). Naruszeniem tego wymiaru prywatności może być tu m.in. nietaktowne komentowanie czy niedyskretne pytanie, a także nieodpowiednie miejsce konwersacji;
- Wymiar psychologiczny – jest to kontrola racjonalnych i emocjonalnych bodźców, możliwość ich autonomicznego wartościowania oraz określenie z kim, czym i w jakich okolicznościach odbędzie się dzielenie intymnymi lub poufnymi informacjami. Naruszenie może mieć tu postać np. próby obniżenia czyjeś wartości lub przekonania do swoich racji;
- Wymiar informacyjny – określa w jaki sposób, kiedy i do jakiego stopnia informacja o jednostce może być przekazana innym. Ujawnianie informacji odbywa się tutaj całkowicie poza kontrolą jednostki, np. podczas przekazywania detali czyjegoś życia osobistego innej osobie.

Rozgraniczenie, którego dokonał Burgoon jest przejrzyste, jednak w wielu definicjach granice pomiędzy wymiarami prywatności są rozmyte a zakres znaczeniowy jednego wymiaru wkracza w zakres drugiego. We współczesnych ujęciach prywatności na szczególną uwagę zasługują dwie teorie, które pojawiły się w latach gdy internet i media społecznościowe stały się nierozłącznym elementem współczesnego świata. Pierwszą z nich jest teoria integralności Nissenbaum a drugą teoria zarządzania prywatnością Petronio (Kołodziejczyk, 2014, s. 19).

Nissenbaum podkreśla, że błędem byłoby takie rozumienie prywatności w której utożsamia się ją z wolnością lub autonomią. Prywatność nie jest również tym samym co odosobnienie lub samotność. Nie można też opierać się na niejasnym przeciwstawieniu tego co prywatne, temu co publiczne. Należy raczej zrozumieć

na czym polega różnica pomiędzy działaniem w którym człowiek koncertuje się na własnych celach, a cele innych uwzględnia o tyle o ile zgodzili się na udział w jego przedsięwzięciach, od działań w których odnosi się do drugich, włączając w to tych, którzy nie wyrazili zgody na integrowanie ich w te działania. „Istotne dla zrozumienia prywatności nie jest bowiem to, czy nasze działanie pojawia się, czy też nie w sferze, którą określamy mianem<<publicznej>>, lecz to, czy w działaniu tym pojawia się odniesienie do drugich i sposób w jaki owi drudzy uczestniczą w tym działaniu" (Chyrowicz SSpS, 2009, s. 11). Nissenbaum twierdzi, iż powinniśmy posiadać obszar osobistej wolności, w którym będą realizowane własne cele zarówno za zgodą innych, jak i bez ich zgody. Ten obszar nazywany byłby właśnie prywatnością. Ograniczeniem sfery prywatności byłby natomiast potencjalnie krzywdzący charakter naszych działań wobec innych osób (Chyrowicz SSpS, 2009, s. 11).

Petronio z kolei poddaje szczegółowej analizie system granic służących zarządzaniu poziomem dostępności do prywatnych informacji osoby, który jest, według założeń autorki, oparty na precyzyjnych zasadach. Zasady prywatności są dynamiczne i zmieniają się w zależności od okoliczności. Koncepcja ta uwzględnia również fakt, iż pewne informacje są dzielone z innymi i możemy stać się ich współposiadaczami, co z kolei pociąga za sobą odpowiedzialność za ochronę informacji prywatnych, a to wymusza znowu wynegocjowanie zasad determinujących wyjawianie lub ukrywanie dzielonych informacji i zobowiązuje do wzajemnego przestrzegania wypracowanych reguł. Rezultatem tych działań jest kolektywna kontrola nad przepływem informacji, przy czym trzeba pamiętać, że nie wszystkie próby kontrolowania zasad prywatności kończą się sukcesem. Koncepcja Petronio porusza też kwestie następstw ewentualnych porażek w tym obszarze i omawia jak ludzie przywracają koordynację i kontrolę (Jędruszczak, 2005, s. 204).

Koncepcje te nie odnoszą się wprost do prywatności w świecie mediów cyfrowych, ale w dużej mierze można je tam zastosować. Współczesna rzeczywistość zmieniła się tak bardzo, że prywatność często wręcz jest „wystawiana na sprzedaż". Ludzie często dzielą się w sieci całym swoim życiem, pokazując swoje dobra materialne, dzieci, współmałżonków, wyjazdy, czerpiąc przy tym rodzaj swoistego zadowolenia, gdy ich zdjęcia i wpisy są obserwowane i komentowane przez innych. Właśnie to stało się przyczynkiem tego,

iż w ostatnich latach wielką karierę zdobyło słowo o*vershare*, co zostało uhonorowane tytułem „Słowa Roku" przyznawanym przez Webster Dictionary w 2008 r. Oznacza ono zbytnie dzielenie się, a wręcz obarczanie innych szczegółowymi informacjami ze swojego życia. Idealnym medium dla osób uprawiających *oversharing* jest właśnie internet, a zwłaszcza media społecznościowe. Można wręcz odnieść wrażenie, iż ludzie zadają sobie sporo trudu aby pozbawić się prywatności i publikując niemal każdy swój ruch w sieci, nie licząc się często z zagrożeniami jakie niesie ze sobą nadmierne dzielenie się swoim życiem z innymi (Młynarska – Sobaczewska, 2013, s. 42).

Regulacje prawne dotyczące prywatności użytkowników w sieci

Jednym z głównych zagadnień związanych z korzystaniem z internetu jest prawo do ochrony prywatności przez jego użytkowników. Pomimo, iż internet jest medium ogólnodostępnym, to każdy z niego korzystający ma prawo do zachowania swojej prywatności tak jak to ma miejsce na ulicy, w sklepie, czy w każdym innym miejscu publicznym. Aby to zagwarantować ustawodawca wydał regulacje prawne obejmujące prawa i obowiązku użytkowników sieci, dostawców usług internetowych oraz administratorów portali.

Do niedawna panowało przekonanie, iż człowiek korzystający z internetu jest anonimowy. Obecnie wzrosła świadomość społeczna i wiadomo, iż każdy ruch w sieci pozostawia po sobie cyfrowy ślad, dlatego w interesie użytkowników jest dostosowanie do współczesnej rzeczywistości systemu prawnego zapewniającego efektywną ochronę danych osobowych. Pracę nam nim podjęła Komisja Europejska w 2012 roku i przedłożyła projekt rozporządzenia wspólnotowego[1].

Zanim jednak to miało miejsce, przepisy regulujące zasady przetwarzania danych osobowych zostały wprowadzone do polskiego ustawodawstwa ustawą o ochronie danych osobowych z dnia 29 sierpnia 1997 r. (Dz.U. z 2002 r. Nr 101, poz. 926 ze zm.). Uchwalenie pierwszej w Polsce Ustawy o ochronie danych osobowych było wzorowane w dużej mierze na zasadach ustanowionych Dyrektywą 95/46/WE Parlamentu Europejskiego i było zgodne z powszechną

[1]http://orka.sejm.gov.pl/wydbas.nsf/0/aa1e06213f088c33c1257d0e00491563/$file/infos_173.pdf.

polityką państw europejskich w tym obszarze[2]. Potwierdzało konstytucyjne prawo do ochrony prywatności i w art.1 pkt. 2 wskazywało możliwość przetwarzania danych osobowych ze względu na dobro osoby, której one dotyczą, dobro osób trzecich lub dobro publiczne. Przedmiotem ochrony uczyniło dane dotyczące pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej a także dane dotyczące stanu zdrowia, kodu genetycznego, nałogów, orientacji seksualnej, dane dotyczące skazań, orzeczeń o ukaraniu lub mandatów karnych (art. 27) (Bógdał-Brzezińska, Gawrycki, s. 296). Wprowadzenie takich przepisów do polskiego systemu prawnego umożliwiło podpisanie przez Polskę 21 kwietnia 1999 roku oraz ratyfikowanie 24 maja 2002 r. Konwencji nr 108 Rady Europy[3]. Ustawa była ważna również z punktu Konstytucji RP, której art. 47 mówi, iż „Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym”[4]. Art. 51 Konstytucji RP gwarantuje natomiast prawo do ochrony informacji dotyczącej obywatela, a jego treść brzmi[5]:

1. „Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczących jego osoby.
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym.
3. Każdy ma prawo dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa.
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą.
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa”.

Zgodnie z art. 76 ustawy zasadniczej władze publiczne są zobowiązane do ochrony konsumentów, użytkowników i najemców przed działaniami

[2] http://www.giodo.gov.pl/144/id_art/112/j/pl/.
[3] http://www.giodo.gov.pl/144/id_art/112/j/pl/.
[4] http://www.sejm.gov.pl/prawo/konst/polski/2.htm.
[5] Tamże.

zagrażającymi ich zdrowiu, prywatności i bezpieczeństwu, a także przed nieuczciwymi praktykami rynkowymi[6].

W Konstytucji RP nie ma definicji pojęcia „dobra osobiste", co uzasadnia charakter ustawy zasadniczej. W doktrynie pojęcie ochrony dóbr osobistych jest oparte na istnieniu praw podmiotowych. Konstytucja zalicza więc prywatność do kategorii praw podstawowych, natomiast konieczność jej ochrony zostaje wyprowadzona bezpośrednio z zasad demokratycznego państwa prawa i obowiązujących norm prawa międzynarodowego. Trybunał Konstytucyjny różnicuje sferę prywatności na ścisła i otwartą. Stwierdza, że prywatność zawiera sferę intymną, która powinna być całkowicie chroniona oraz sferę rodzinną, której ochrona powinna być ograniczona i uzasadniona usprawiedliwionym zainteresowaniem (M. Pryciak, s. 221-222).

Świat w przeciągu kilkunastu ostatnich lat zmienił się tak bardzo, że obowiązujące przepisy prawne okazały się niedostosowane do współczesnej rzeczywistości cyfrowej. W 1995 roku, gdy wchodziła w życie unijna dyrektywa prawna dotycząca danych osobowych, około 1% mieszkańców Europy korzystało z internetu. Z tego też powodu w roku 2012 Komisja Europejska podjęła inicjatywę stworzenia efektywnego systemu prawnego ochrony danych osobowych, co wywołało ogromne emocje i liczne spory wśród przedstawicieli poszczególnych państw. Projekt aktu został przyjęty w marcu 2014 roku i skierowany do Rady Unii Europejskiej[7]. W dniu 4 maja 2016 r. w Dzienniku Urzędowym Unii Europejskiej L 119 zostały opublikowane oficjalne teksty aktów prawnych składających się na reformę ochrony danych[8]:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów

[6] Tamże.
[7] http://orka.sejm.gov.pl/wydbas.nsf/0/aa1e06213f088c33c1257d0e00491563/$file/infos_173.pdf.
[8] http://www.giodo.gov.pl/1520147/id_art/9278/j/pl/.

zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW.

Zgodnie z art. 99 ogólnego rozporządzenia o ochronie danych, wchodzi ono w życie 20 dnia po publikacji w Dzienniku Urzędowym UE i będzie stosowane od dnia 25 maja 2018 r. Dyrektywa obowiązuje natomiast od pierwszego dnia po opublikowaniu w Dzienniku Urzędowym Unii Europejskiej[9].

Gruntowna reforma przepisów Unii Europejskiej zobowiązuje państwa członkowskiego do implementacji nowych przepisów o ochronie danych osobowych. Przepisy ustawy o ochronie danych osobowych mają zapewnić stosowanie w polskim porządku prawnym rozporządzenia 2016/679. Projekt Ministerstwa Cyfryzacji wskazuje na sposób realizacji tego celu. Założeniem projektowanej regulacji jest również zapewnienie obywatelom możliwości skutecznego egzekwowania ochrony swoich danych, w tym również przyśpieszenie postępowania o ich naruszenie[10]. Średni czas trwania postępowania w sprawach z tego obszaru obecnie w Polsce wynosi 295 dni do czasu wydania decyzji I instancji przez GIODO, a 437 dni do decyzji II instancji. Uzyskanie prawomocnego orzeczenia w sprawie dotyczącej ochrony danych osobowych wynosi średnio 600 dni, a w 2015 roku wiele spraw rozpatrywano nawet ponad 3 lata[11].

Nowe przepisy zakładają co najmniej kilka dróg dochodzenia swoich praw przez pokrzywdzonych. Będzie można wystąpić do ograniu i po wydaniu przez niego decyzji udać się do sądu administracyjnego lub wystąpić do organu i równocześnie do sądu powszechnego. Kolejną możliwością będzie wystąpienie do sądu powszechnego lub wniesienie powództwa z tytułu naruszenia dóbr osobistych. Kolejne instytucje będą zobowiązane informować się o podjętych postępowaniach aby nie zajmować się tą samą sprawą równolegle[12].

[9] Tamże.
[10] https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych.
[11] http://prawo.gazetaprawna.pl/artykuly/1030778,nowa-ustawa-o-ochronie-danych-osobowych.html.
[12] https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf.

Zabezpieczenie danych osobowych jest ważne nie tylko z punktu widzenia pojedynczego obywatela ale również z punktu widzenia bezpieczeństwa państwa, co może wydawać się mało oczywiste. Trudno bowiem wyobrazić sobie sytuację w której ich kradzież lub zniszczenie będzie związane bezpośrednio z przeprowadzeniem ataku terrorystycznego na infrastrukturę informatyczną państwa. Rozpatrując jednak sprawę bezpieczeństwa tychże systemów nie sposób pominąć tematykę zabezpieczania danych osobowych i systemów za pomocą których są one przetwarzane. Te systemy i sieci informatyczne mogą zarazem sterować infrastrukturą, która stanie się celem ataków terrorystycznych, a same dane również mogą dla terrorystów być cenne (Suchorzewska, s. 272-273). Dobre prawo obejmujące przepisy zarówno dotyczące zabezpieczania danych jak i możliwości ich udostępniania jest cenne nie tylko z punktu widzenia zwykłego użytkownika sieci, ale również z punktu widzenia bezpieczeństwa całego państwa.

Zagrożenie terrorystyczne a ochrona prywatności w sieci

Z jednej strony przepisy mające chronić prywatność użytkownika w sieci są zaostrzane, z drugiej rosnące zagrożenie terrorystyczne sprawia, że rządy wielu krajów, w tym Polski, przyznają służbom coraz szersze uprawienia do sprawdzania aktywności użytkowników w sieci. Zdobywanie informacji niejawnych, dotyczących zarówno wrogów jak i sojuszników jest jednym z zadań realizowanych przez służby specjalne. W 2013 r. opinią publiczną na świecie wstrząsnęły informacje ujawnione przez byłego pracownika wywiadu USA, dotyczące skali inwigilacji elektronicznej prowadzonej przez służby wywiadowcze. Szokowały przecieki mówiące o powszechnym i masowym gromadzeniu prywatnych danych, które należały do zwykłych ludzi co też uświadomiło użytkownikom internetu jak bardzo ich dotyczą kwestie cyberbezpieczeństwa o których do tej pory często zazwyczaj nie myśleli (Grzelak 2014, s. 165-166).

W Polsce szerokim echem odbiła się tzw. ustawa inwigilacyjna, będąca nowelizacyjną ustawy o Policji (Dz.U. 2016 poz. 147). Nowelę przygotowaną przez posłów PiS sejm uchwalił 15 stycznia 2016 (co odbyło się przy sprzeciwie całej opozycji), senat przyjął ją bez poprawek 29 stycznia 2016, a prezydent Andrzej Duda podpisał 3 lutego 2016 r.

1.1. Prywatność w sieci w ujęciu przepisów prawa i analiz badawczych

Nowelizacja obejmuje kilkanaście ustaw regulujących działania Policji, Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego, Centralnego Biura Antykorupcyjnego, Agencji Wywiadu, Żandarmerii Wojskowej, Służby Kontrwywiadu, Wywiadu Wojskowego, Służy Centralnej i kontroli skarbowej. Wśród uwag dotyczących noweli, najwięcej z nich dotyczyło zapisów o danych internetowych (np. adresów odwiedzanych stron, wpisów w wyszukiwarce, adresów e-mail itp.). Dotychczas po dane tego typu służby występowały do dostawców internetu w ramach prowadzonych postępowań pisemnie i taką drogą je również dostawały. Nowelizacja wprowadziła dostęp do nich on-line, przez tzw. bezpieczne połączenie internetowe, które największe firmy informatyczne utworzą na swój koszt. Służby mogą sięgać po te informacje nie tylko na potrzeby prowadzonych postępowań ale także prewencyjnie, w celu zapobiegania lub wykrycia przestępstw, w celu ratowania życia lub zdrowia ludzkiego a także działań poszukiwawczych oraz przy realizacji zadań ustawowych. Na pozyskanie ich nie potrzeba już obecnie zgody sądu[13].

Takie uprawniania służb budzą niepokój zarówno polityków nie związanych z obozem rządzącym jak również Rzecznika Praw Obywatelskich Adama Bodnara, Krajowej Rady Sądownictwa, Rady ds. Cyfryzacji, Naczelnej Rady Adwokackiej, Krajowej Rady Radców Prawnych oraz organizacji pozarządowych. Czy słusznie? Na to pytanie nie można udzielić jednoznaczniej odpowiedzi. Ustawodawca broni noweli podkreślając, iż w wielu krajach Europy przepisy dotyczące uprawniania służb w śledzeniu działań obywateli w internecie są równie a niekiedy jeszcze bardziej obszerne. Za przykład podaje się tu Francję i Hiszpanię, gdzie również uchwalono kontrowersyjne ustawy wbrew protestom organizacji pozarządowych. W Wielkiej Brytanii i Finlandii natomiast prace nad nimi są bliskie ukończenia. Największe zastrzeżenia budziła ustawa francuska z lipca 2015 roku, która pozwala m.in. na masowe zbieranie danych internetowych za pomocą instalacji u dostawców tzw. czarnych skrzynek. Powody tego typu działań mogą daleko wykraczać poza powszechnie rozumiane bezpieczeństwo i zagrożenie terroryzmem. Może być to np. dbałość

[13] http://prawo.gazetaprawna.pl/artykuly/921582,co-moga-sluzby-specjalne-ustawa-inwigilacyjna-ustawa-o-policji.html.

o zagraniczne interesy kraju, czy ochrona ekonomicznych, naukowych i przemysłowych interesów Francji[14].
Zapisy na temat instalacji „czarnych skrzynek" widnieją obecnie w ustawie hiszpańskiej oraz projekcie ustawy brytyjskiej. Techniczny dostęp do danych jest w tych przypadkach łatwiejszy niż ten, który uchwalił polski ustawodawca, jednak posiada znacznie większą kontrolę zewnętrzną nad działaniami służb niż to ma miejsce w Polsce, co właśnie na naszym gruncie budzi największe kontrowersje. W większości państw Unii Europejskiej, służby przed dokonaniem inwigilacji muszą zdobyć na to zgodę sądu, sędziego lub innego organu zewnętrznego. W Polsce taka kontrola będzie dokonywana w postaci przesyłanych co sześć miesięcy sprawozdań z działalności służb, co w praktyce oznacza, że odbędzie się ona po fakcie i może być nieskuteczna[15].

Prywatność w sieci w ujęciach badawczych
Badania na temat prywatności w sieci są podejmowane od momentu, gdy internet stał się medium ogólnie dostępnym i powszechnie używanym, co na gruncie polskim zaczęło mieć miejsce pierwszych latach XXI wieku a do tego czasu liczba jego użytkowników rośnie lawinowo. W roku 2008 było w Polsce 14 mln internautów, a 2015 już 25,7 mln[16]. Najnowsze analizy na temat dostępu do internetu mówią, że w kwietniu 2017 roku 27,8 mln Polaków korzystało z sieci, co pokazuje nieustanną tendencję wzrostową[17].
W 2015 roku CBOS wydał raport „Bezpieczeństwo w internecie". Badania przeprowadzono wśród 634 internatów a autorów interesowało przede wszystkim jakie informacje i komu w sieci Polacy je udostępniają. Jak wynika z deklaracji, najczęściej informacje udostępniane on-line, to adres e-mail, który niemal dwie trzecie internautów umieściło w internecie (63%, w tym 13% dla wszystkich), data urodzenia (56%, w tym 15% dla wszystkich) oraz zdjęcie z widoczną twarzą publikującego (52%). Na uwagę jednak zasługuje fakt, iż zdjęcia są typem informacji, które są najrzadziej w sieci publikowane bez

[14] https://wiadomosci.wp.pl/inwigilacja-internetu-nie-tylko-w-polsce-jak-wyglada-kontrola-dzialan-sluzb-w-europie-6025256964621441a.
[15] Tamże.
[16] https://pl.wikipedia.org/wiki/Historia_Internetu_w_Polsce.
[17] http://pbi.org.pl/raporty/polscy-internauci-kwietniu-2017-analiza/.

ograniczenia grupy odbiorców (24%). Nieco ponad jedna trzecia internatów udostępniała on-line informacje o miejscu w którym aktualnie przebywa (37%), adresie zamieszkania (35%), informacje o swoim zawiązku lub stanie cywilnym (35%), o poglądach, zainteresowaniach lub przynależności do grupy (35%) oraz o numerze telefonu (31%). Jeszcze rzadziej umieszczano dane na temat miejsca pracy lub miejsca zatrudnienia (27%) oraz wypowiedzi na jakiś temat podpisane imieniem i nazwiskiem (23%). Najrzadziej natomiast dzielono się materiałami wideo na których można rozpoznać osobę, która je publikowała (13%) (Flisiak, 2015, s. 1-2). Analizując te dane, widać, iż Polacy są ostrożni w dzieleniu się informacjami na swój temat w sieci, zwłaszcza tymi, które określa się jako tzw. „dane wrażliwe".

Wśród badań na temat prywatności w internecie na szczególną uwagę zasługują te przeprowadzone przez Związek Pracodawców Branży Internetowej IAB. Odbyły się one w dwóch edycjach. Pierwsza miała miejsce w roku 2013, natomiast druga została przeprowadzona w roku 2016. Badanie z 2016 roku zrealizowano 15-30 marca metodą wywiadów indywidualnych wspomaganych komputerowo (CAWI) i wzięło w nim udział 1500 internautów w wieku 15 lat i więcej[18]. W porównaniu do badania z 2013 roku wyraźnie widać, iż internauci są coraz bardziej świadomi kwestii prywatności i coraz częściej korzystają z zabezpieczeń przeglądarek internetowych. Rzadziej natomiast umieszczają w sieci swoje zdjęcia. W roku 2013 nie umieszczało swoich zdjęć 21% respondentów, natomiast w roku 2016 było ich już 47%. Internauci w porównaniu z badaniem sprzed trzech lat częściej czyścili historię przeglądania internetu (39% - 2013, 57% - 2016), kasowali bądź blokowali pliki cookies (23% - 2013, 37% - 2016), wykorzystywali programy blokujące reklamy (25% - 2013, 29% - 2016) oraz korzystali z przeglądarki w trybie prywatnym (13% - 2013, 27% - 2016)[19].

Dane te pokazują jak wśród polskich internautów wzrósł poziom świadomości na temat zagrożeń sieciowych, lecz pomimo tego swoją wiedzę na temat cyberbezpieczeństwa uznali jako niedostateczną. Zdaniem autorów raportu stwarza to pole do dalszych działań edukacyjnych w które powinny być

[18] https://www.iab.org.pl/wp-content/uploads/2017/03/IAB_Polska_Prywatnosc_w_sieci_2016_2017_raport.pdf.
[19] http://pbi.org.pl/patronaty/prywatnosc-w-sieci-raport-iab-polska/.

zaangażowane podmioty kształtujące środowisko cyfrowe, dostawcy usług i regulatorzy. Chociaż respondenci zdawali sobie sprawę z zagrożeń jakie dotyczą prywatności w sieci, to wszelkie zakazy, obostrzenia i ograniczenia w przestrzeni wirtualnej postrzegali negatywnie. Budziło to ich irytacje i niechęć do korzystania z sieci. Respondenci wyrazili również chęć aby treści i reklamy on-line były dopasowane do ich zainteresowań i równocześnie byli świadomi, że aby takie dopasowanie miało miejsce to muszą się podzielić informacjami na swój temat. Internet był przez nich traktowany jako przestrzeń publiczna (lub częściowo publiczna) z wyjątkiem prywatnych stron www [20].

Parlament Europejski regularnie zleca badanie opinii publicznej w państwach członkowskich Unii Europejskiej. Analizy takie odgrywają znaczącą rolę w podejmowaniu decyzji na poszczególnych etapach działalności parlamentarnej. Są źródłem informacji na temat europejskiej opinii publicznej, a ich wyniki pokazują rozkład odmiennych postaw obywateli UE wobec szeregu kwestii gospodarczych, klimatycznych oraz pokazują czego Europejczycy oczekują od Parlamentu Europejskiego[21]. Wyniki ich można znaleźć w zakładce Eurobarometru[22] na stronach internatowych Parlamentu Europejskiego.

W badaniach Eurobarometru z 2016 roku (badanie: E-privacy. Poland. 2016), znalazły się kwestie prywatności w sieci. Wynika z nich, że niemal 93% wszystkich Polaków uważa, że firmy powinny uzyskać dostęp do danych gromadzonych na ich komputerze, tablecie lub smartfonie jedynie za ich zgodą. 90% naszych rodaków stwierdziło, że ważne jest dla nich zachowanie prywatności maili oraz informacji przekazywanych poprzez komunikatory. 80% stwierdziło natomiast, że nie chce być śledzona w sieci bez ich zgody i jest to dla nich kwestia ważna lub bardzo ważna[23]. Połowa Polaków (55%) uznała, że każdy powinien mieć możliwość szyfrowania swoich maili oraz połączeń telefonicznych. Duża liczba respondentów dbała też o ochronę prywatności przeglądanych informacji. 59% zmieniało domyślne ustawienia prywatności w przeglądarkach internetowych, natomiast 52% unikało konkretnych stron

[20] Tamże.
[21] http://www.europarl.europa.eu/poland/pl/strona_glowna/eurobarometr_1.html.
[22] http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124.
[23] https://panoptykon.org/wiadomosc/badania-co-polki-i-polacy-mysla-o-prywatnosci-w-sieci.

www w obawie przed śledzeniem ich aktywności. Dla porównania europejska średnia w tym wypadku wynosiła 40%. Mniejszą popularnością wśród Polaków cieszyły się aplikacje blokujące reklamy on-line. Używało ich 41% badanych. Najmniejsze grono zwolenników zdobyły sobie natomiast programy zapobiegające monitorowaniu użytkowników w sieci – jedynie 25% z nich się przyznała do ich stosowania[24].

Przeglądając literaturę przedmiotu widać, iż badaniem prywatności w sieci częściej zajmują się instytucje rządowe lub społeczne oraz firmy z branży IT niż środowiska naukowe w instytutach badawczych lub na uczelniach. Widać to zwłaszcza na polskim gruncie gdzie analizy dotyczące tej problematyki są nieliczne, a jeśli takowe się pojawiają to grupa respondentów zazwyczaj jest mocno zawężona. Jedną z nich Jednym z nowszych badań jest „Badanie postaw dotyczących prywatności użytkowników mediów społecznych", którego celem było przede wszystkim sprawdzenie jak aktywni użytkownicy internetu, a w szczególności mediów społecznych, traktują kwestie zamieszczania informacji osobistych w sieci. Badanie przeprowadzono w formie ankiety, pogłębionych wywiadów indywidualnych, a następnie podjęto próbę weryfikacji faktycznej dostępności danych prywatnych w Internecie osób, z którymi przeprowadzono wywiady i skonfrontowano wyniki z informacjami otrzymanymi w trakcie badania. Respondentami byli studenci pierwszego roku studiów Informacji Naukowej i Studiów Biologicznych Uniwersytetu Warszawskiego. 61% z nich stwierdziło, iż ich prywatność i wizerunek w sieci są dla nich ważne, a 30% uznało, że raczej tak. Niewielu badanych uznało, że nie posiada pełnej kontroli nad informacjami dotyczącymi ich osoby, jakie znajdują się w internecie. Odpowiedzi *raczej nie* lub *zdecydowanie nie* udzieliło tu 16% z nich. Wśród odpowiedzi na pytania wywiadu przeważały natomiast opinie, że prywatność jest obecnie zagrożona, przez wszechobecną technologię i trzeba świadomie i nieustannie dbać o to, aby jej nie utracić (Kołodziejczyk, 2014, s. 95-133).

Powyższe analizy pokazują, iż na polskim gruncie pole do badania kwestii prywatności w sieci jest olbrzymie i jeszcze mocno niezagospodarowane. Cykliczne badania ten temat prywatności pokazują jak zmienia się świadomość

[24] https://panoptykon.org/wiadomosc/badania-co-polki-i-polacy-mysla-o-prywatnosci-w-sieci.

internatów w tej kwestii i jak wraz z postępem technologicznym starają się bronić swojej sieciowej intymności. Programy telewizyjne, kampanie społeczne, prywatne rozmowy a zwłaszcza zasoby samego internetu edukują użytkowników w kwestii bezpieczeństwa w wirtualnym świecie i zwiększają ostrożność w korzystaniu z niego.

Podsumowanie

Prywatność jest prawem i wartością, której żaden człowiek nie powinien być pozbawiony. Z drugiej strony nowoczesne technologie, które nas obecnie otaczają, a zwłaszcza otwarta przestrzeń internetu i wszechobecne smartfony sprawiają, że prywatność staje mocno ograniczona. M. Merkwa pisze: „wolność wypowiedzi, a także pozyskiwania informacji nie może uwzględniać jedynie tradycyjnych, analogowych mediów. Musi być związana z nowym sposobem wymiany informacji, jakim jest Internet" (Merkwa, 211, s.32). Można do tej listy dodać także prywatność, która powinna mieć takie samo znaczenie zarówno w świecie analogowym jak i świecie cyfrowym.

Przepisy prawa w ostatnich latach musiały zostać dostosowane do zmieniającej się rzeczywistości i z jednej uwzględniać prawa obywateli do prywatności, tajemnicy korespondencji i bezpieczeństwa danych osobowych, a z drugiej strony wraz z pogłębiającym się na świecie terroryzmem, pozwalać służbom w coraz większym zakresie sprawdzać aktywność ludzi w cyberprzestrzeni. Uprawnienia te często budzą sprzeciw, gdyż internet dotychczas był kojarzony niemal z nieograniczoną wolnością poruszania się w nim. Z drugiej strony ludzie są coraz bardziej świadomi zagrożeń jakie czyhają na nich w sieci i sami zabezpieczają na różne sposoby swoje przeglądarki internetowe i sprzęt przed zewnętrznymi atakami. Badania obszaru prywatności w sieci dają obraz tego jak duża jest ta świadomość i jak się ona zmienia wraz z postępem technologicznym. Analizy na tym polu to nieustanne odkrywanie nowej wiedzy, gdyż znaczenie prywatności nieustannie ewoluuje a ludzie niejednokrotnie bardziej lub mniej świadomie wyzbywają się jej przed osobami, które nie koniecznie powinny mieć dostęp do wielu informacji z ich życia.

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

Zmiana charakteru cyberprzestępczości w ostatnich latach

Pochodzące z banków i organów prewencji, informacje trafiające do mediów dotyczące działalności przestępców włamujących się na różne sposoby do banków, wpływają na świadomość klientów odnośnie kwestii bezpieczeństwa i potrzeby doskonalenia bankowych systemów zabezpieczeń (Gąsiorowski, Podsiedlik, 2015, s. 37). Również w literaturze popularno-naukowej oraz w powieściach i opowiadaniach beletrystki naukowej, pisarze podejmują się opisania spektakularnych faktycznych lub fikcyjnych zdarzeń ingerencji przestępców w instytucje bankowe, wpływając na świadomość klientów banków dotyczącą ryzyka utraty zdeponowanych w banku oszczędności, uszczuplenia stanu bankowego skarbca czy ostatnio także kradzieży tożsamości i danych osobowych przez hakerów (Gwoździewicz, Prokopowicz, 2016a, s. 395) i ingerencji przestępców bezpośrednio na kontach internetowej bankowości elektronicznej z poziomu słabo zabezpieczonego smartfona lub zdiagnozowanych przez internetowych przestępców luk w systemach operacyjnych, przeglądarkach internetowych i nieaktualnych programach antywirusowych zainstalowanych w komputerach i urządzeniach mobilnych klientów. Ingerencja ta zwykle sprowadza się do kradzieży danych niejawnych, w tym osobowych klientów określonych usług oferowanych przez portale informacyjne i społecznościowe oraz do defraudacji środków finansowych zgromadzonych na kontach użytkowników bankowości internetowej (*Yahoo Discloses 2013 Breach that Exposed …,* 2016).

Od lat 90. XX wieku włamania do informatycznych systemów bankowych zmieniły swój charakter. Zaobserwowane w ostatnich latach zmiany są tak znaczące, że dotyczą także stosowanego nazewnictwa odnoszącego się do tej

niezgodnej z prawem działalności osób włamujących się, ingerujących w informatyczne systemy bankowe. Osoby te już od wielu lat rzadziej określa się hakerami, obecnie dominuje określenie cyberprzestępców. Natomiast przestępcza dziedzina polegająca na ingerencji w systemy elektronicznej, w tym internetowej bankowości, zwykle celem dokonania kradzieży danych osobowych i defraudacji pieniędzy określana jest mianem cyberprzestępczości (Trejderowski, 2013, s. 62). Obecnie jedną z jej odmian, związaną z rozwojem separatystycznych działalności organizacji terrorystycznych jest analizowaną obecnie przez znawców problematyki jest rozwijający się także problem cyberterroryzmu (Górka, red. 2014, s. 48).

Przede wszystkim jeszcze w latach 90. ubiegłego wieku włamania hakerskie bezpośrednio do bankowych systemów informatycznych zdarzały się relatywnie częściej niż do komputerów klientów banków. Natomiast w ostatnich latach tendencja ta uległa odwróceniu. Elektroniczni włamywacze wykorzystują częściej komputery klientów aby przejąć kontrolę nad kontem elektronicznej bankowości klienta, ponieważ komputery te są zwykle słabiej zabezpieczone (Prokopowicz, Dmowski, 2010, s. 341). Komputery ale także już nie tylko komputery, również urządzenia mobilne typu notebooki, tablety, smartfony mają zainstalowane często nieaktualne oprogramowanie antywirusowe, nieaktualne firewalle lub nie są wyposażone w te zabezpieczenia w ogóle. W ostatnich latach analiza danych pochodzących z banków, policji i innych instytucji zajmujących się przestępczością zorganizowaną wymierzoną w system finansowy wskazuje, że dominujące jeszcze w latach 90. włamania do fizycznych oddziałów banków metodą „na Kwinto" lub poprzez sterroryzowanie pracowników banku przez przestępcę wyposażonego w broń lub jej atrapę w ostatnich latach nie należą już do najczęstszych form ingerencji przestępców wobec podmiotów bankowych. Również analiza danych dotyczących przestępczości odnotowywanej w Polsce wskazuje, że coraz częściej przestępcy włamują się do banków poprzez systemy internetowej bankowości elektronicznej wykorzystując słabe punkty w systemach zabezpieczeń już nie tylko samych banków ale także urządzeń z których korzystają klienci i zainstalowanych w nich aplikacji (Kosiński, 2015, s. 52).

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

Z badań historii zmieniających się technik działalności przestępców włamujących się do banków wynika, że już z początkiem obecnego wieku sukcesywnie rośnie i od kilkunastu lat zaczyna dominować przestępczość elektroniczna, w niej internetowa. Już od kilkunastu lat do coraz częstszych technik stosowanych przez przestępców, które zalicza się do działalności przestępczej dla której niezbędnym medium transmisji danych jest internet zalicza się przede wszystkim phishing i spamming. Ponieważ w okresie ostatnich kilkunastu lat co najmniej kilkukrotnie zarówno w informatycznych systemach bankowych jak i w komputerach i urządzeniach mobilnych klientów zmieniały się systemy operacyjne, zmieniane były wersje przeglądarek internetowych, programów antywirusowych oraz stosowanych przez banki zabezpieczeń bankowości elektronicznej oraz także samych urządzeń informatycznych umożliwiających łączenie się klienta z jego internetowym kontem w banku więc także techniki hakerskie, w tym dominujące stosowane przez przestępców formy np. phishingu ulegały wielokrotnym modyfikacjom (Król, 2017, s. 46).

Spam ukryty w aktualizacji oprogramowania

Od początku XX wieku jedną z najszybciej rozwijających się przestępczych technik służących do pozyskiwania poufnych danych osobistych jest tzw. spam. Przestępcy rozsyłając spam posługują się różnymi metodami podszywania się pod renomowane instytucje. Na przykład spam rzekomo wysyłany z przeglądarki Google, który odkryty został już w ostatnim tygodniu sierpnia 2006 roku, pojawiał się w skrzynkach odbiorczych z tytułem „Google, # 1 Search Engine". Wówczas w rozsyłanej wiadomości mailowej zalecano użytkownikom pobranie najnowszej wersji paska narzędziowego Google Toolbar, który zablokuje reklamy typu pop-up i oprogramowanie szpiegujące (spyware). Użytkownicy kierowani byli do strony internetowej, gdzie miał się odbyć proces aktualizacji narzędzia. Firma SurfControl, producent oprogramowania do filtrowania poczty elektronicznej i treści pobieranych z internetu ostrzega, że sugerowany do pobrania plik jest poważnie zainfekowany wirusami.

Już w 2016 roku zespół badawczy SurfControl zanotował kilka aspektów tej wiadomości e-mail pokazujących, że jest on mistyfikacją. Adres nadawcy

wskazywał raczej na jedną osobę niż zespół Google. Ponadto adres IP odnośnika, skąd użytkownicy mieli pobrać plik pasował do podejrzanych stron internetowych sprzedających podręczniki typu „The Essential Underground Handbook" (przewodnik prezentujący schematy oszustw).
Specjaliści firmy SurfControl zajmujący się tego typu internetowymi przestępstwami odkryli również, że spamerzy coraz częściej wykorzystują zdjęcia i grafiki w swoich wiadomościach, zamiast standardu HTML. Technika ta pozwalała spamerom ominąć ochronę antyspamową oferowaną przez oprogramowanie Microsoft Outlook w ówczesnej wersji 2003, który powinien blokować podejrzaną grafikę bazującą na HTML. Ponadto, odkąd tekst stał się integralną częścią grafiki, więc nie podlegał również funkcjom skanowania tekstu stosowanym w tradycyjnych filtrach antyspamowych (Krebs, 2016).

Kradzież poufnych informacji osobistych czyli phishing
W 2004 roku pojawiły się nowe odmiany spamu, którego celem była kradzież poufnych informacji osobowych. Jedna z form tego cyberprzestępczego procederu reprezentowała niebezpieczną odmianę spamu powiązanego z tzw. phishingiem tj. przekierowywania użytkowników bankowości elektronicznej na fałszywe strony banków zakładane przez cyberprzestępców w celu dokonania kradzieży poufnych informacji oraz defraudacji pieniędzy z kont klientów instytucji finansowych. Od 2004 roku jedną z odmian tego typu rozsyłanego przez cyberprzestępców spamu były np. reklamy środków poprawiających potencję.
Kilka lat temu do jednych z popularniejszych przestępstw popełnianych za pośrednictwem internetu zaliczano wyłudzenia numerów kart kredytowych oraz numerów kont i loginów do kont w bankach oferujących możliwość obsługi rachunku poprzez internet. Popularną metodą wyłudzania takich danych jest wspomniany phishing, czyli forma cyberprzestępczego pozyskania informacji niejawnych, poprzez podszywanie się pod instytucję godną zaufania. Najczęściej cyberprzestępcy stosujący technikę phishingu podszywają się pod funkcjonujące w danym kraju lub globalnie banki poprzez zakładanie w Internecie fałszywych

stron internetowych które są graficznymi kopiami ich pierwowzorów tj. stron internetowych określonych banków (Polasik, 2008, s. 61).
Początkowo technika phishingu polegała głównie na wysyłaniu korespondencji elektronicznej do dużej ilości kont emailowych osób, w tym klientów danego banku. W treści spreparowanej wiadomości maila cyberprzestępcy sugerują klientom banków, aby odwiedzili witrynę internetową banku, w którym posiadają konto bankowości elektronicznej. Jednak podany link przekierowujący na stronę banku po jego kliknięciu przenosi odbiorcę tej wiadomości na fałszywą stronę banku. W ten sposób cyberprzestępcy wyłudzają od klientów bankowości internetowej szczególnie poufne informacje typu: login i hasło dostępu do konta internetowego banku (Gacki, 2006).
Najbardziej klasyczny mechanizm wyłudzenia tego typu danych niejawnych polega na tym, że w rozsyłanych mailach cyberprzestępcy np. informują klientów danego banku o deaktywacji, reorganizacji systemu konta bankowego i proszą o powtórne podanie danych konta czy rachunku, niekiedy nawet paradoksalnie uzasadniając tę czynność koniecznością poprawienia sytemu bezpieczeństwa danego rachunku (Gwoździewicz, 2016). Fałszywa strona internetowa, służąca do wyłudzania informacji niejawnych spreparowana jest przez cyberprzestępców w taki sposób aby wizualnie wyglądała identycznie jak jej pierwowzór, tj. rzeczywista witryna określonego banku. Działalność tego typu przestępstw ułatwiał dodatkowo błąd w popularnej przeglądarce MS Internet Explorer, który pozwalał zamaskować także rzeczywisty adres fałszywej strony oraz także pozwalał na umieszczanie w lewym górnym rogu okna przeglądarki, na początku pasku adresu www spreparowanego obrazu tej małej zielonej zamkniętej kłódeczki co ma symulować wysoki poziom zabezpieczeń strony przez atakami hakerskimi (Boruch, 2012, s. 37).
Jedną z odmian phishingu jest również tworzenie w sieci fałszywych sklepów internetowych, oferujących różne produkty lub usługi w promocyjnych, okazjonalnie wyjątkowo niskich cenach. Celem kradzieży są w takiej sytuacji numery i daty ważności kart kredytowych. Pozyskane w ten sposób dane odnośnie kart kredytowych mogą być przez przestępców wykorzystywane

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

do zakupów w rzeczywistych sklepach poprzez dokonywanie płatności na rachunek oszukanej osoby (Grzywacz, 2016, s. 47).

Niekiedy wykrycie phishingu przez odpowiednie instytucje prewencji nie jest łatwe, ponieważ wiadomości takie zawierają zazwyczaj fałszywe adresy zwrotne, co także ma wprowadzać w błąd użytkowników bankowości elektronicznej i sugerować, że otrzymana wiadomość mailowa została otrzymana od faktycznie istniejącej renomowanej firmy lub banku. Aby nadać dla fałszywego maila cechy autentyczności cyberprzestępcy dodają różne elementy graficzne nawiązujące do typowych składników witryny internetowej danej instytucji jak np. znaki towarowe, logo oraz oryginalną skopiowaną grafikę witryny danej instytucji. Z badań przeprowadzonych przez firmy technologiczne wynika, że w tych materiałach graficznych wklejonych lub załączonych do treści maila może być ukryte złośliwe oprogramowanie, które po zainfekowaniu komputera będzie np. sczytywać wpisywane z klawiatury loginy i hasła do kont bankowości elektronicznej. W ten sposób w jednym mailu cyberprzestępcy zastosować mogą co najmniej dwie różne techniki ataku na konta użytkowników bankowości internetowej.

O skali tego procederu świadczą dane instytucji, które zajmują się badaniem tego typu przestępstw. Do tego typu instytucji należy Centrum Przeciwdziałania Oszustwom Internetowym RSA Cyota (RSA Cyota Anti-Fraud Command Center). Według danych tej instytucji od początku 2006 roku phishing stał się jedną z najszybciej rozpowszechniających się metod internetowego oszustwa, polegającego głównie na oszukiwaniu klientów instytucji finansowych (Szkodzin, 2006). Już w połowie 2006 roku zanotowano 48% wzrost liczby tego typu ataków. Według danych wymienionej instytucji celem ataku najczęściej były instytucje amerykańskie (75%). 20% zaatakowanych marek ma swoje korzenie w Europie, a pozostałe 5% to przeważnie instytucje azjatyckie. Z drugiej strony przestępcy działający w ten sposób funkcjonują głównie w USA (63%), poza tym z Niemiec (9%) i Australii (7%). Od tego czasu skala tego procederu nadal rośnie. W sytuacji gdy sfishingowane, fałszywe strony zostaną wykryte i zablokowane przez organy ścigania cyberprzestępstw to na innych serwerach, w innych miejscach globu zostają założone inne kolejne tego typu

fałszywe strony banków i innych instytucji finansowych. W ostatnich latach cyberprzestępcy stworzyli różne techniki i odmiany phishingu.

HYIP czyli wyjątkowo atrakcyjna oferta inwestycyjna

Termin „HYIP" to skrót od zwrotu „High-Yield Investment Program", który stał się synonimem podejrzanych programów inwestycyjnych na długo zanim nierzetelni doradcy inwestycyjni zaczęli prowadzić w Internecie przestępczy proceder. W klasycznej postaci jest to rodzaj przestępstwa gospodarczego, polegający na oferowaniu uczestnikom programu rzekomego dostępu do wyjątkowo korzystnych transakcji, jakie mają odbywać się na elitarnym rynku międzybankowym (*Forex - jak uniknąć oszustwa* 2006).

HYIP-erowy proceder polegał zazwyczaj na prezentowaniu super atrakcyjnej oferty inwestycyjnej jako cykle operacji finansowych oparte na całkowicie bezpiecznych papierach wartościowych, gwarantowanych przez wiodące instytucje bankowe ma świecie, stąd też oszustwa tego rodzaju znane są również pod nazwą „prime bank fraud". Przestępcy organizujący te „prime bank frauds" sugerują, że dzięki dostępowi do rynku międzybankowego kupują wybrane instrumenty finansowe z ogromnym upustem, a następnie sprzedają je w obrocie wtórnym po znacznie wyższych stawkach.

W ostatnich latach silnie rozwija się nowa odmiana HYIP polegająca na zakładaniu anonimowych stron internetowych, których twórcy przestawiają się jako utalentowani specjaliści z zakresu nieszablonowych technik inwestycyjnych na rynku Forex albo akcji i proponują niezwykle korzystne warunki zarządzania kapitałem. Najczęściej spotykany proceder HYIP wymaga od łatwowiernych klientów wpłat nie przekraczających kilku dolarów, obiecując jednocześnie stopy zwrotu rzędu kilka procent dziennie, które ma wypracowywać przy użyciu bardzo zaawansowanych instrumentów finansowych. Ponieważ autorzy programów HYIP nie oczekują od swoich klientów zbyt wiele, a obiecują im w zamian bardzo dużo, programy tego rodzaju są bardzo popularne w internecie. Nie jest możliwe dokładne oszacowanie skali tego przestępczego procederu, ale warto zauważyć, że wyszukiwarka Google deklaruje dla słowa „HYIP" ok. 3.140.000 rezultatów wyszukiwania, MSN -

134.440, a Yahoo! - ok. 1.400.000. Inne przykłady powstających fałszywych tego typu ofert prezentowanych na spreparowanych przez cyberprzestępców stronach internetowych dotyczą różnego typu okazjonalnych konkursów w których użytkownik internetu zostaje powiadomiony, że został wylosowany i wygrał atrakcyjną nagrodę rzeczową. Jednak aby tę nagrodę otrzymać musi najpierw wpłacić kaucję lub podać określone dane osobowe.

Technika kotłowni czyli „boiler rooms"

Analogicznie jak omówione powyżej programy HYIP jest to typ oszustw skierowany do klientów rynku Forex oraz rynków akcji i derywatów. Zasadnicza różnica między programem HYIP a „boiler room" polega na tym, że w tym drugim przypadku z przestępcami współpracują lub są nimi profesjonalni sprzedawcy, którzy dzwonią do upatrzonych osób i kreując atmosferę sensacyjnej okazji zachęcają do zakupu instrumentów finansowych znajdujących się w ich ofercie. Zwykle po zakupie super atrakcyjnego instrumentu finansowego, kontakt z „boiler room" staje się co najmniej bardzo utrudniony (Polasik, 2008, s. 116).

Pozornie „boiler room" sprawia wrażenie renomowanej firmy maklerskiej. Na pozorny efekt profesjonalnego wrażenia składa się zarówno rozległa wiedza sprzedawcy na temat rynku finansowego, jak również „fachowo brzmiąca" nazwa firmy, np. typu „financial Corporation". Klient zwykle nie wie, że tego rodzaju „financial Corporation" można założyć w zasadzie tak samo łatwo, jak kupić frytki w budce za rogiem. Podstawowym czynnikiem sukcesu tego przestępczego procederu jest wykreowanie gorącej atmosfery wokół oferowanych w promocji instrumentów finansowych (Grzywacz, 2016, s. 58). Stąd nazwa tego rodzaju przestępstwa, tj. „boiler room", czyli „kotłownia". Nazwę tę spopularyzował ją film Boiler Room z 2000 roku w reżyserii Bena Youngera, który w Polsce dystrybuowany był pod tytułem „Ryzyko". W filmie tym trafnie przedstawiono analizowany przestępczy proceder, w tym fikcyjną firmę tego rodzaju o nazwie JT Marlin.

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

Internetowe manipulacje instrumentami finansowymi

Do niedawna przestępstwa typu „boiler room" zdarzały się najczęściej w tych państwach, w których tego rodzaju marketing telefoniczny (tzw. cold calls) jest dozwolony przez prawo i często stosowany przez maklerów i doradców finansowych. Z drugiej strony rozwój internetu umożliwił modyfikację tego przestępczego procederu poprzez zastąpienie marketingu internetowego na internetowy z pomocą masowego rozsyłania spamu w poczcie elektronicznej oraz atrakcyjnie brzmiących ofert wyświetlających się na stronach internetowych. Zdarza się również, że rozsyłane w ten sposób informacje są reklamowane za pomocą linków sponsorowanych.

Interesujące jest również to, że zawarte na forach internetowych dyskusje i internetowe plotki często dotyczą także transakcji dokonywanych na rynku forem oraz rynku papierów wartościowych, w tym akcji, obligacji i derywatów. Ulubionym obiektem internetowych naciągaczy są akcje spółek o niskiej kapitalizacji i niewielkiej płynności, ponieważ ich kursem można łatwo manipulować za pomocą rozpowszechnienia stosownej w treści plotki. Często są to również działający w Internecie doświadczeni inwestorzy, którzy kupują pakiety tzw. śmieciowych akcji albo kontraktów, a następnie usiłują je sprzedać z zyskiem, podbijając ich kurs poprzez rozpowszechnianie nieprawdziwych informacji m.in. na dyskusyjnych forach internetowych, w których sugerują że określony emitent papierów wartościowych jest w dobrej kondycji finansowej i planuje kolejne akwizycje, inwestycje itp. Niekiedy również tego typu przestępstwa realizowane są drogą rozsyłania tysięcy maili zachęcających w swej treści do zakupu określonego instrumentu, przedstawianego jako silnie niedowartościowanego przez rynek (Dutko, Karciarz, 2011, s. 67).

Jednym z pierwszych tego typu przypadków była akcja mailingowa 24-letniego obywatela Australii, George Hourmouzisa, który wysłał w świat cztery miliony e-maili z wiadomością, że wartość akcji spółki Rentech wzrośnie w najbliższym czasie z ok. 33 centów do ponad trzech dolarów. Po rozesłaniu tej wiadomości cena akcji tej spółki podwoiła się i giełda odnotowała ponadprzeciętny wzrost obrotów. Autor tej akcji miał pecha, ponieważ obrót akcjami Rentechu został zawieszony. Pomysłowy przestępca dostał wyrok dwóch lat więzienia.

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

Inną odmianą cyberprzestępczego procederu wirtualnych „kotłowni" jest tworzenie przez stosujących przestępcze praktyki inwestorów specjalnych programów komputerowych z systemami transakcyjnymi, które służą do automatycznego zarządzania procesem inwestycyjnym na rynku akcji i derywatów. Programy te mogą być rozpowszechniane bezpłatnie do pobrania plików instalacyjnych bądź funkcjonujące na spreparowanych przez cyberprzestępców witrynach internetowych. W rzeczywistości programy te zawierają proste algorytmy i ukryte sugestie nakłaniające do inwestowania w określony sposób lub w określone papiery. Często dotyczy tych programów, których stosowanie zapewnić ma szybkie podwojenie kapitału w odpowiednio krótkim czasie (Kosiński, 2015, s. 241).

Wzrost aktywności złośliwego oprogramowania ransomware w 2016 roku

W 2016 roku do najczęściej odnotowywanych w bankach i innych instytucjach rodzajów cyberprzestępstw należały wymuszenia online dokonywane poprzez ataki typu ransomware. Osoby zarządzające systemami bezpieczeństwa w instytucjach finansowych wskazują na wysokie ryzyko możliwości sparaliżowania systemów płatności, zablokowania funkcjonowania określonych aplikacji bankowych, włamania się do platform internetowych instytucji i dokonania w nich określonych niepożądanych modyfikacji celem uniemożliwienia prawidłowego działania systemu (Gąsiorowski, Podsiedlik, 2015, s. 47). Jeżeli te hakerskie interwencje dokonywane poprzez włamywanie się do systemów informatycznych określonych firm, instytucji finansowych lub publicznych mają na celu wymuszenie okupu to wówczas ten rodzaj złośliwego oprogramowania, którym w tym procederze posługują się cyberprzestępcy przyjęto nazywać ransomware (Malak, 2017, s. 49).

Oprócz złośliwego oprogramowania typu ransomware w ostatnich kwartałach cyberprzestępcy rozsyłają w mailach ukryte wiadomości, które ujawniają się podczas otwierania wiadomości mailowych, które jak się później okazuje były fałszywymi informacjami generowanymi przez hakerów tworzących spam wzorowany na mailach rozsyłanych do użytkowników, klientów firm energetycznych, operatorów telefonii komórkowej oraz ostatnio także firm

kurierskich. Jeszcze 2-3 lata temu tego typu spam rozsyłany hakerską metodą typu Business E-mail Compromise (*Billion-Dollar Scams* …, 2016) ukierunkowany był w stronę różnych podmiotów, instytucji i klientów indywidualnych określonych powszechnych usług. Natomiast w ostatnich kilku kwartałach metodą BEC cyberprzestępcy atakują systemy informatyczne dużych firm i banków, tj. swą działalność przestępczą ukierunkowują na podmioty dysponujące znacznymi nadwyżkami finansowymi bądź osoby odpowiedzialne za podejmowanie decyzji finansowych. Skuteczne zablokowanie działania kluczowych funkcji aplikacji internetowych bądź wewnętrznych systemów informatycznych tego typu podmiotów oznacza duże prawdopodobieństwo wymuszenia okupu za zdjęcie nałożonej blokady. Cyberprzestępcy stale doskonalą wspomnianą mailową metodę BEC rozsyłając zainfekowany spam wprost do osób podejmujących decyzje w firmach odnośnie dokonywania płatności za dostarczone usługi (Leopando, 2016).

Działający w Internecie naciągacze stosując stale udoskonalane techniki inżynierii społecznej i socjotechniki tworzą fałszywe maile wyglądające pozornie niemal identycznie jak ich pierwowzory z firm energetycznych, gazowni, firm windykacyjnych, czy nawet instytucji sektora publicznego obsługujących przedsiębiorstwa (Gąsiorowski, Podsiedlik, 2015, s. 48). Straty wynikające z zapłacenia fałszywych faktur zwykle nie są wysokie, tym bardziej że po zapłaceniu jednej lub dwóch spreparowanych przez hakerów faktur zaatakowane metodą BEC firmy zauważają, że padły ofiarą oszustwa. Mimo niewysokich stary dla konkretnej firmy czy instytucji, która uległa tej formie oszustwa to jednak działający w Internecie przestępcy potrafią wyłudzić w ten sposób pokaźne kwoty, ponieważ spam typu BEC rozsyłają przez systemy botnetowe w milionach sztuk fałszywych maili (*Raport Trend Micro …,* 2017). Poza tym ze względu na relatywnie niskie kwoty wpisane do poszczególnych fałszywych faktur firmy, które padły ofiarą oszustwa i szybko to zauważyły, następnie udoskonaliły swe systemy bezpieczeństwa podejmują często decyzję o nieupublicznianiu tych faktów i na wszelki wypadek nie powiadamiają także stosownych służb, instytucji organów ścigania i prewencji, w tym Policji. Jeżeli przeważająca większość firm i instytucji, które padły ofiarą ataków metodą BEC

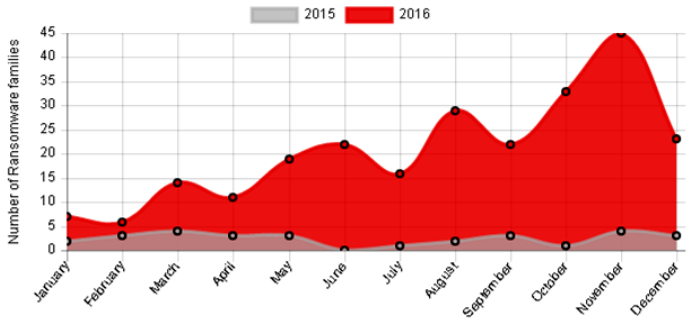
nie upublicznia tych faktów i nie zgłasza na Policję tych zdarzeń wówczas cyberprzestępcy mogą czuć się bezkarnie nadal działać w swym przestępczym procederze. Zaatakowane metodą BEC oraz ransomware firmy i instytucje często decydują się na pozostawieniu tych zdarzeń w tajemnicy przez opinią publiczną z obawy o pogorszenie wizerunku marki firmy, utratę zaufania ze strony klientów. W sytuacji, gdy zaatakowane podmioty należą z definicji do instytucji zaufania publicznego jak np. banki komercyjne (Prokopowicz, Dmowski, Sarnowski, 2005, s. 217), wówczas tego typu wstrzemięźliwość z publikowaniem informacji o tych zidentyfikowanych przestępczych procederach staje się problemem systemowym i w konsekwencji może doprowadzić do nieoczekiwanego paraliżu prawidłowego działania całego systemu bankowego. O skali rosnącego zagrożenia informują liczby. Otóż w 2016 roku analitycy wydziału Smart Protection Network™ w firmie Trend Micro™ wykryli i ustanowili blokady dla ponad 81 miliardów przypadków różnych form ataków online i innych cyberzagrożeń. Ustanowione blokady dotyczyły głównie ograniczenia ingerencji rozsyłanego przez cyberprzestępców spamu i trafiających do skrzynek mailowych e-mali z załącznikami zawierającymi złośliwe oprogramowanie malware i ransomware oraz BEC.

Wzrost rodzin programów złośliwych ransomware i dokonywanych za ich pomocą ataków

Z danych raportu technologicznej firmy badawczej Trend Micro „*TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats*" wynika, że tego typu ataków hakerskich odnotowano już ponad miliard i szybko rośnie liczba różnych wariantów ataków typu ransomware, a konkretnie liczba rodzajów złośliwych programów, które tworzone są przez cyberprzestępców aby po uaktywnieniu się w komputerach użytkowników na różne sposoby blokowały działanie systemów informatycznych, określonych funkcji aplikacji komputerowych czy zmieniały działanie sprzętu informatycznego. Mechanizm działania cyberprzestępców poprzez ataki typu ransomware w zasadzie nie jest zupełnie nową techniką hakreską. Firma Trend Micro jest światowym liderem w dziedzinie zabezpieczeń cybernetycznych prowadzącym badania i cyklicznie

publikującym raporty na temat aktualnych trendów w zakresie cyberprzestępczości i bezpieczeństwa systemów informatycznych oraz transferu danych w Internecie (*Raport Trend Micro ..,* 2017).Z opublikowanego w I kwartale 2017 roku rocznego raportu firmy Trend Micro na temat bezpieczeństwa pt. „*TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats*" wynika, że w 2016 roku najwięcej ataków dokonywanych poprzez internet dotyczyło wymuszeń kierowanych głownie do dużych firm i banków. Wykryto ponad miliard ataków typu ransomware na całym świecie. Liczba tych nadużyć w Polsce to 4% wszystkich ataków dla regionu EMEA. Cyberprzestępcy głównie inicjowali ataki typu ransomware i BEC (*Business Email Compromise*), celem wyłudzenia okupu od przedsiębiorstw i instytucji finansowych, w tym banków.

Rysunek 1. Miesięczny wzrost liczby nowych rodzajów tzw. rodzin programów złośliwych ransomware.



Źródło: *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raport firmy analitycznej Trend Micro, 28.02.2017, (www.trendmicro.com/vinfo /us/security/research-and-analysis/threat-reports/roundup).

W 2016 r. analitycy firmy Trend Micro wraz z zespołem z firmy technologicznej Zero Day Initiative (ZDI) wykryli aż 780 nowych luk w zabezpieczeniach systemów informatycznych, aplikacji, dostępu do internetu i sprzętu komputerowego. Przeważająca większość tych luk, ponieważ aż 678 zostało

zgłoszonych przez firmę ZDI do programu nagradzania informatyków, którzy wykryli luki w zabezpieczeniach mogące stanowić źródło nowych zagrożeń dla systemów informatycznych firm i banków. Po wykryciu przez ZDI luki w zabezpieczeniach informowany jest producent oprogramowania celem usunięcia zdiagnozowanej luki. W porównaniu z 2015 r. Trend Micro i ZDI znalazły w oprogramowaniu Apple o 188 proc. więcej luk, a w oprogramowaniu Microsoft – o 47 proc. mniej, co wyraźnie wskazuje na odmienne tendencje w tym zakresie, w kwestii bezpieczeństwa korzystania z aplikacji tych dwóch czołowych producentów oprogramowania (Krebs 2016). Poza tym w 2016 roku zdiagnozowano spadek wobec roku poprzedniego zastosowania w działalności cyberprzestępców nowo powstałych luk w zabezpieczeniach z wykorzystaniem zestawów eksploitów. Odnotowano w tym zakresie spadek działalności przestępczej o 71 proc. Spadek ten powiązano głównie z przeprowadzonym w czerwcu 2016 r. aresztowaniem znacznej części cyberprzestępców stosujących eksploita Angler (*Raport Trend Micro ...,* 2017).

Fałszywe niby złośliwe oprogramowanie WannaCry nakłaniający do opłacenia okupu

Interesującą kwestią, którą należy także poruszyć w niniejszym artykule to generowane przez hakerów fałszywe oprogramowanie niby złośliwe typu ransomware. W 2016 roku firma Trend Micro wykryła znaczący wzrost liczby ataków dokonywanych z użyciem wygenerowanych przez cyberprzestępców programów RANSOM_WANA.A i RANSOM_WCRY.I. Po kilku tygodniach od wykrytego wzrostu aktywności w sieci internet złośliwego oprogramowania WannaCry pojawiły się w nowe wersje programów WannaCry, które próbują naśladować, imitować te poprzednie jednak nie zawsze są w rzeczywistości realnie szkodliwe.

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

Rysunek 2. Komunikat fałszywego niby złośliwego oprogramowania WannaCry nakłaniający do opłacenia okupu.

Źródło: *Podsumowanie Ransomware: Analiza WannaCry Surze* [in] portal internetowy "Trend Micro", Analiza firmy analitycznej Trend Micro,, Dział: „Aktualności – Bezpieczeństwo, 30.05.2017 r., (www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-business-as-usual-after-wannacry-surge).

W odróżnieniu do realnie szkodliwego złośliwego ransomware WannaCry, fałszywe warianty WannaCry są zdolne wyrządzać znacznie mniejsze szkody lub w ogóle nie są w rzeczywistości szkodliwe. Jeden z takich podszywających się pod „ransomware" programów znany jako Ransom_FAKEWCRY wykryła firma Trend Micro w maju 2016 roku. jako) zostało wykryte w maju jako Fałszywy ransomware Ransom_FAKEWCRY zawarty był w skompilowanym pliku wykonywalnym Microsoft Intermediate Language (MSIL). Po uaktywnieniu tego programu na ekranie monitora zainfekowanego komputera użytkownika wyświetlane jest żądanie do zapłacenia okupu za odblokowanie systemu komputerowego podczas, gdy do żadnego zablokowania nie doszło. Wyświetlone okienko dialogowe zawierające żądanie zapłacenia okupu jest imitacją analogicznego powiadomienia wyświetlanego w komputerach zainfekowanych prawdziwym złośliwym programem WannaCry. Poniższy

rysunek przedstawia przykład wyświetlanego okienka dialogowego wygenerowanego przez fałszywy WannaCry z żądaniem okupu w wysokości 300 USD (*Podsumowanie Ransomware ...,* 2017).

Pomimo braku realnej szkodliwości tego typu fałszywego niby złośliwego oprogramowania WannaCry, to jednak zdarzały się sytuacje wyłudzenia zapłacenia okupu. Powodem może być brak precyzyjnego określenia potencjalnych szkód, które zostały niby wyrządzone w sytuacji wyświetlenia informacji o zaszyfrowaniu plików lub zablokowaniu określonych aplikacji do czego jednak w rzeczywistości nie doszło. Poza tym w wielu przypadkach użytkownicy zainfekowanych tym fałszywym WannaCry komputerów nie byli w stanie odróżnić tego typu rodzaju oszustwa z użyciem nieszkodliwego niby złośliwego oprogramowania od rzeczywistego złośliwego oprogramowania ransomware WannaCry (*Podsumowanie Ransomware ...,* 2017). W takiej sytuacji, gdy fałszywe WannaCry doskonale imitowały te realnie szkodliwe ich pierwowzory wielu użytkowników nie mając pewności z czym ma do czynienia jednak decydowało się zapłacić okup obawiając się uaktywnienia szkodliwej działalności programu, który wyświetlił żądanie zapłacenia okupu.

Specyfika cyberprzestępczości wykrytej w 2016 roku i wzrost presji na doskonalenie systemów bezpieczeństwa elektronicznego transferu danych w internecie

Inną globalnie działającą instytucją analityczną badającą cyberzagrożenia transferu danych w Internecie i wdrażającą techniki oraz procedury bezpieczeństwa jest notowana na rynku giełdowym NASDAQ pod akronimem CSCO technologiczna firma Cisco. Firma Cisco w raporcie z przeprowadzonych badań „Annual Cybersecurity Report" (*Cisco 2017 Annual Cybersecurity Report ...,* 2017) podaje, że w ostatnich kwartałach do najpowszechniej stosowanych technik przejmowania kontroli nad komputerem użytkownika, było wcześniejsze zainfekowanie złośliwym oprogramowaniem typu adware lub rozsyłanego w ogromnej ilości spamu. Z raportu tego wynika, że (Król 2017, s. 46):

- w 2016 roku nastąpił drastyczny, największy od 2010 roku wzrost liczby rozsyłanych maili typu spam,

- aż 65 % ruchu mailingowego zalicza się do spamu,
- szacuje się, że złośliwe oprogramowanie ukryte jest w co dziesiątej trafiającej do skrzynki mailowej wiadomości zaliczanej do kategorii spamu.

Zgodnie z wynikami badań ankietowych przeprowadzonych przez firmę informatyczną Cisco wśród ponad 3 tys. dyrektorów ds. bezpieczeństwa systemów informatycznych oraz innych osób kierujących wydziałami bezpieczeństwa biznesowego zatrudnionych w różnych firmach 13 krajów rozwiniętych istniej szereg powodów potwierdzających niechęć do upubliczniania tego typu zdarzeń, tj. sytuacji w której określona firma padła ofiarą ataku hakerskiego jednak kierownictwo tej firmy podejmuje decyzję o utrzymaniu w tajemnicy całego zdarzenia. Na podstawie wspomnianych badań ankietowych opracowano raport „Cisco 2017 Annual Cybersecurity Report" (*Cisco 2017 Annual Cybersecurity Report ...,* 2017), którego wyniki opisano w publikacji „Cisco Security Capabilities Benchmark Study". Z raportu tego wynika, że (Król, 2017, s. 46):

- tylko o połowie skutecznych ataków hakerskich zostały poinformowane media, tj. zostały upublicznione informacje o tych zdarzeniach,
- w firmach, które padły ofiarą tych ataków w wyniku obniżenia reputacji marki 22 % tych firm utraciło część klientów,
- u 40 % zaatakowanych przez hakerów firm utrata bazy klientów sięgnęła nawet ponad 20 % poprzedniej wielkości,
- prawie jedna trzecia firm, które upubliczniły informacje o tym, że padły ofiarą ataku hakerskiego, wykazała spadek przychodów w kolejnym okresie sprawozdawczym,
- u 38 % z tych firm spadek przychodów sięgnął ponad 20 %.
- 23 % firm wskazało, że ataki hakerskie okazały się znaczącym ograniczeniem rozwoju biznesu,
- u 42 % z tych podmiotów spadek dochodów również sięgnął ponad 20 %.

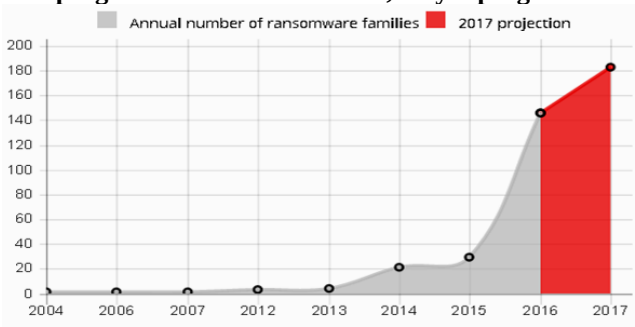
W związku z powyższym wiele firm i instytucji, które stały się obiektem ataków cyberprzestępców stara się informacje o tego typu negatywnych zdarzeniach zachować w tajemnicy z obawy o potencjalny spadek reputacji marki,

przychodów i dochodów. Z drugiej strony rosnąca ilość infekcji nie jest wynikiem jedynie nikłej świadomości potencjalnych zagrożeń części kadry pracowników niższego szczebla wielu firm.

Mimo doskonalonych w wielu firmach procedur bezpieczeństwa i poprawiania systemów informatycznych poprzez usuwanie wykrywanych luk w zabezpieczeniach to omawiana skala problemu cyberprzestępczości nie zmniejsza się. Tezę tę potwierdzają ostatnie wyniki analiz i testów przeprowadzonych i prezentowanych w cyklicznie publikowanych raportach firmy technologicznej Trend Micro. Otóż analitycy firmy Trend Micro przewidują 25 proc. wzrost liczby nowych rodzin złośliwego oprogramowania ransomware w 2017 roku wobec roku poprzedniego. Skala tego wzrostu oznacza średnio tworzenie przez cyberprzestępców miesięcznie 15 nowych rodzin złośliwych programów. Z przeprowadzonych analiz wynika, że przesilenie generowania dużej ilości nowych rodzajów złośliwego oprogramowania ransomware nastąpiło w 2016 roku. Natomiast w 2017 roku przewidywany jest trend w kierunku stabilizacji w tym zakresie, co może oznaczać, że cyberprzestępcy dokonywać będą dywersyfikacji swych strategii celem ukierunkowania nowych ataków w stronę większych firm i instytucji tj. do podmiotów korporacyjnych, od których mogą wyłudzić odpowiednio większej wartości okup (*Przewidywania dotyczące bezpieczeństwa ...,* 2016).Przewidywany jest również relatywny wzrost ataków prowadzących do naruszeń danych, w tym manipulacji informacją propagowaną np. w mediach społecznościowych oraz w zakresie wykradania danych niejawnych, w tym osobowych z kont użytkowników z portali określonych usług internetowych. Poza tym zastosowanie złośliwego oprogramowania typu ransomware stanie się jedną z najbardziej rozpowszechnioną formą naruszeń danych. Coraz powszechniej cyberprzestępcy realizują swój plan ataków z użyciem programów ransomware w modelu dwuetapowym. W pierwszym etapie przeprowadzanego ataku na systemy informatyczne i bazy danych określonych firm najpierw kradną poufne dane, aby je następnie sprzedawać na tzw. czarnym rynku. Natomiast podczas drugiego etapu ingerencji instalują programy ransomware, aby np. zablokować użytkownikom dostęp do istotnych informacji na serwerach

z danymi określonych firm i instytucji i w ten sposób zwielokrotniają zysk z tej cyberprzestępczej działalności.

Rysunek 3. Liczony w skali rocznej przyrost liczby rodzin złośliwego oprogramowania ransomware, w tym prognoza dla 2017 r.



Źródło: *Przewidywania dotyczące bezpieczeństwa. Następny poziom. Płaskowyż ransomware, większy kompromis z procesem biznesowym i boom cyberpropagandy - jakie powinnyśmy spodziewać się w 2017 roku?*[in] portal internetowy "Trend Micro", Raport firmy analitycznej Trend Micro, 6.12.2016, (www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017).

Problemem systemowym wykraczającym poza możliwości decyzyjne kierownictwa danej firmy jest kwestia podnoszenia bezpieczeństwa elektronicznego transferu danych w internecie. W ujęciu globalnym istnieje wiele organów ścigania międzynarodowo działających przestępców, w tym organizacji terrorystycznych, które sukcesywnie coraz większą część swej działalności przenoszą do internetu. Służby te nie są zainteresowane pełnym zabezpieczeniem internetu, doprowadzeniem do wykluczenia możliwości przestępczego działania określonych firm np. wyłudzających pieniądze od innych podmiotów, przeprowadzających pranie brudnych pieniędzy w systemie finansowym (Gąsiorowski, Podsiedlik, 2015, s. 49). Teoretycznie pełne zabezpieczenie internetu przed atakami hakerskimi nawet jeżeli technicznie był by możliwe na danym moment np. poprzez wprowadzenie

legislacyjnych rozwiązań zobligowania wszystkich użytkowników internetu do szyfrowania wszystkich wiadomości w poczcie mailowej to w praktyce oznaczać mogłoby utratę części potencjalnej bazy klientów rozważających skorzystanie z usług czy zakupu wytwarzanych produktów (Gwoździewicz, Prokopowicz, 2015, s. 211). Poza tym krajowe i międzynarodowe służby porządku publicznego, prewencji i ścigania przestępców takie jak Policja, Agencja Bezpieczeństwa Wewnętrznego w Polsce, działający internacjonalnie Interpol czy Narodowa Agencja Bezpieczeństwa w USA nie są zainteresowane tym aby cały ruch informacyjny elektronicznego transferu danych w Internecie był zaszyfrowany z zastosowaniem najnowszej generacji, najbardziej złożonych algorytmów szyfrujących ponieważ wówczas kontrola internetu i przechwytywanie korespondencji przestępczo działających organizacji byłoby znacząco utrudnione lub nawet niemożliwe. Zarządzanie ryzykiem systemów informatycznych i transferu danych w internecie (Domańska-Szaruga, 2013, s. 263).

Podsumowanie

Dokonujący się dynamicznie postęp w zakresie rozwoju technologii teleinformatycznych determinuje potrzebę bezustannego doskonalenia kwestii bezpieczeństwa systemów teleinformatycznych oraz dostosowywania regulacji prawnych w dziedzinie ochrony danych niejawnych jak również transferu tych danych do nowej rzeczywistości, w której korzystanie z internetu i powszechnych już portali społecznościowych generuje nowe źródła zagrożeń dla prywatności użytkowników. Zgodnie z obowiązującymi standardami podstawowa ochrona danych powinna być zapewniona przez podmioty gospodarcze prowadzące działalność w internecie w tym także instytucje wykorzystujące globalną sieć wyłącznie w celach komunikacyjnych. Niestety, stosowane zabezpieczenia systemów informatycznych często tworzone zostają wtórnie przez zatrudnionych w tym celu informatyków względem technologii wykorzystywanych przy budowie danych Big Data, przetwarzaniu danych w chmurze obliczeniowej, oprogramowaniu zainstalowanym w urządzeniach mobilnych typu tablety i smartfony. Dopiero gdy hakerzy znajdą i wykorzystają

w swej cyberprzestępczej działalności określone luki w zabezpieczeniach, dopiero wówczas problem zostaje zauważony i informatycy zatrudnieni w bankach, firmach i podmiotach sektora publicznego przystępują do tworzenia łat celem uszczelnienia procedur i systemów bezpieczeństwa dla aplikacji i infrastruktury informatycznej, którą zarządzają (Prokopowicz, Dmowski, Sarnowski, 2005, s. 132).

Zgodnie z powyższym szczególnie istotnym determinantem systemu ochrony danych osobowych i informacji niejawnych oraz infrastruktury teleinformatycznej jest permanentne przeprowadzanie testów i diagnostyki funkcjonujących w danej instytucji systemów i aplikacji informatycznych. Problematyka ta jest szczególnie istotna w perspektywie dalszego dynamicznego rozwoju usług finansowych świadczonych za pośrednictwem sieci internet oraz dokonującego się procesu cyfryzacji firm i urzędów publicznych. Obowiązujące regulacje prawne zapewniają jedynie najbardziej elementarny poziom ochrony danych niejawnych podczas realizacji określonych zamówień handlowych i transakcji finansowych. Z dużym prawdopodobieństwem można sądzić, że mogą one okazać się niewystarczające wobec dokonującego się bezustannie postępu w technologii teleinformatycznej wykorzystywanej przez firmy świadczące swe usługi za pośrednictwem globalnej sieci, w tym trudniące się budową baz danych niejawnych w technologii Big Data (Mayer-Schonberger, 2015, s. 37) lub tworzące instrumenty automatyzujące procesy badania informacyjnych zasobów internetu,. Kolejną dziedziną wyznaczającą nowe kierunki postępu w zakresie technologii teleinformatycznej jest doskonalenie technik badania zasobów informacyjnych zwartych w wypowiedziach i komentarzach tysięcy bądź milionów użytkowników portali społecznościowych i innych witryn internetowych gromadzących komentarze użytkowników danych stron. Dotychczas jednak to cyberprzestępcy jako pierwsi odnajdywali luki w zabezpieczeniach systemów informatycznych i wykorzystywali je do przeprowadzenia ataków z użyciem złośliwego oprogramowania ransomware (*Podsumowanie Ransomware* 2017).

Wobec powyższego należy uznać, że proces zarządzania ryzykiem systemów informatycznych, w tym ochrony informacji, danych osobowych i informacji

niejawnych w cyberprzestrzeni w dobie rozwoju bankowości internetowej wchodzi obecnie w kolejną dynamiczną fazę rozwoju i będzie prawnym wyzwaniem dla upowszechniających się technologii tzw. chmury obliczeniowej i big data (Szpor, red. 2013, s. 153). W Polsce doskonalenie procesu zarządzania ryzykiem systemów informatycznych obejmuje także dostosowywanie krajowych regulacji prawnych do normatywów i rekomendacji określonych przez organy instytucjonalne Unii Europejskiej (Gwoździewicz, Prokopowicz 2016b, s. 85).

Dotychczas dominował model łatania luk w zabezpieczeniach przez zatrudnionych w firmach i bankach informatyków, które wcześniej zostały wykryte przez hakerów. Biorąc pod uwagę silny wzrost aktywności niebezpiecznych programów ransomware model ten powinien ulec zmianie polegającej na odwróceniu kolejności działań. To zatrudnieni w firmach, bankach i instytucjach publicznych informatycy powinni profilaktycznie przeprowadzać testy działania infrastruktury teleinformatycznej, doskonalić procedury i procesy zarządzania ryzykiem, podnosić poziom bezpieczeństwa wewnętrznych systemów informatycznych i podłączonych do internetu aplikacji, którymi zarządzają. Procesy te powinny być przeprowadzane na tyle sprawnie, aby luki w zabezpieczeniach były wykrywane odpowiednio wcześnie i jeszcze przed ich zauważeniem przez potencjalnych cyberprzestępców. W związku z tym obecnie wzrasta potrzeba prewencyjnego, profilaktycznego w swej istocie procesu doskonalenia procesów zarządzania ryzykiem systemów informatycznych funkcjonujących w instytucjach finansowych, przedsiębiorstwa.

1.3. Rozwój cyberprzestrzeni zagrożeniem dla bezpieczeństwa baz danych

Wstęp

Wraz z dynamicznym rozwojem technologii na przestrzeni lat pojęcie cyberprzestrzeni znacznie się zmieniło. Obecnie to przede wszystkim wirtualna przestrzeń, w której połączone siecią komputery i inne media cyfrowe (telefony, tablety, radio, telewizja) komunikują się między sobą. To także nowego typu przestrzeń społeczna, w której na co dzień spotykamy się korzystając z narzędzi teleinformatycznych.

W obecnych czasach coraz częściej pojawiają się komunikaty prasowe dotyczących ataków hakerskich na systemy informatyczne. Obecnie cyberprzestrzeń, jest jednym z najczęściej podejmowanych tematów z zakresu bezpieczeństwa. Rozwój internetu doprowadził do ułatwień ale stworzył również nowe pola do działania dla przestępców. Instytucje, organizacje międzynarodowe, państwa zrozumiały iż bezpieczeństwo cybernetyczne jest bardzo ważne. Świadomość nastąpiła wraz ze wzrostem zagrożeń i przestępstw komputerowych.

Nasz kraj jak każdy inny na świecie stoi przed wyzwaniem stworzenia i wypracowania zmian prawnych, które będą chronić, bronić i uniemożliwiać ataki na sieci komputerowe, które dadzą poczucie bezpieczeństwa swoim obywatelom. Stworzenie zabezpieczeń jest niezwykle trudne ze względu iż temat jest stosunkowo nowy a „galopujący" rozwój opóźnia wprowadzanie odpowiednich regulacji w systemach prawnych.

Cyberprzestępczość - typologie zagrożeń teleinformatycznych

Termin cyberprzestrzeń (ang. cyberspace) stworzył i upowszechnił w 1984 r. William Gibson, w powieści pt. „Neuromancer". W swojej książce autor określił cyberprzestrzeń jako konsensualną halucynację, doświadczaną każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych (…). Graficzne odwzorowanie danych

z banków wszystkich komputerów świata. Niewyobrażalna złożoność (Gibson, 1999, s. 53). Znaczenie cyberprzestrzeni dla współczesnego państwa i społeczeństwa powoduje, że coraz ważniejszy staje się problem jej bezpieczeństwa. Jak stwierdzają Bogusław Pacek i Romuald Hoffman, bezpieczeństwo cyberprzestrzeni związane jest z brakiem ryzyka utraty danych informacyjnych (Pacek, Hoffman, 2013, s. 85)

Zagrożenia mogą dotyczyć każdego systemu informatycznego, niezależnie od obszaru jego wykorzystania i zastosowanych środków zabezpieczających. Szczególnie złośliwie atakowane są systemy informatyczne w instytucjach takich jak: zakłady opieki medycznej, linie lotnicze, systemy informatyczne administracji rządowej, instytucje finansowe.

Zacznijmy od definicji „ informacja" która posiada wiele alternatyw nie zawsze spójnych w swoim znaczeniu. I tak „informacja (łac. *informatio* – przedstawienie, wizerunek; *informare* – kształtować, przedstawiać) – termin interdyscyplinarny, definiowany odmiennie w rożnych dziedzinach nauki; najogólniej – właściwość pewnych obiektów, relacja między elementami zbiorów pewnych obiektów, której istotą jest zmniejszanie niepewności (nieokreśloności)"[25]. Informacją są to dane których zadaniem jest przekazanie wiedzy do odbiorcy w rożnych postaciach, mogą dotyczyć tekstu, liczb a także dźwięku.

W niniejszym opracowanie ogranicza się do analizy informacji cyfrowej, która aby mogła zostać przekazana musi zostać zdigitalizowana czyli przetworzona. Oznacza to że dane z postaci analogowej muszą zostać przekształcone na postać cyfrową w postaci zapisu binarnego, który następnie możemy przesyłać za pomocą fal elektromagnetycznych. Dzięki takim możliwościom, rozwojowi techniki oraz rozprzestrzenieniu się sieci informatycznej wszyscy mamy bardzo szybki i wygodny dostęp do wszelkiego rodzaju informacji.

W dzisiejszych czasach wartość informacji jest tak ważna, że bez niej nie moglibyśmy funkcjonować w środowisku które nas otacza. Dzięki przepływowi informacji możemy się kształcić, zdobywać wiedzę, rozwijać swoje kompetencje i umiejętności. Pod słowem informacja kryje się wiele „info" które wykorzystujemy w różnych dziedzinach naszego życia, można wręcz uznać

[25]http://pl.wikipedia.org/wiki/Informacja, (dostęp: 06.05.2017 r.)

że informacje są częścią nas samych. Najprościej możemy podzielić informacje na prywatne np. nr dowodu osobistego, numer pesel, ubezpieczenie oraz dane konta w banku i ogólnodostępne jak wiadomości telewizyjne, programy naukowe i rozrywkowe. Informacji ogólnodostępnych nie można ukraść ale jeśli chodzi o informacje prywatne to tutaj „ złodzieje" mają pole do popisu.
Kradzież nie zawsze ma znaczenie materialne, również bardzo często dochodzi do kradzieży moralnych, których odbudowanie nie jest tak proste jak finansowe. Ochrona informacji cyfrowej jest ważna nie tylko dla indywidualnych użytkowników. Z punktu widzenia firm działających w środowisku cyfrowym bezpieczeństwo informacji jest sprawą kluczową. Każda taka firma posiada bazę danych, w której przechowuje cenne dla niej informacje, np. o klientach, korporacji, pracownikach, obrotach, planach rozwoju itp. Dlatego ma to szczególne znaczenie aby w tajności powyższe informacje były przechowywane. Firmy które inwestują w systemy bezpieczeństwa są bardziej wiarygodne, maja lepsza reputacje i są konkurencyjne na rynku względem innych firm. Również dla państwa i jego obywateli bezpieczeństwo informacyjne jest niezmiernie istotne ponieważ daje nam poczucie bezpieczeństwa, które jest jednym z najważniejszych czynników dla każdego obywatela. Bezpieczne przechowywane tajne dokumenty gwarantują nam poczucie spokoju wewnętrznego dzięki któremu możemy się rozwijać jako państwo i jako jednostka. Często okazuje się, że pomimo zastosowania nadzwyczajnych środków zabezpieczających, już same działania socjotechniczne mogą doprowadzić do kradzieży informacji i tutaj okazuje się ze czynnikiem najsłabszym jest człowiek a nie technologia. Wartość skradzionych informacji bardzo trudno jest określić, wszystko zależy od tego jak bardzo pragniemy ją zataić przed innymi osobami. Równie trudno wyobrazić siebie co może się wydarzyć i do czego mogą zostać wykorzystane skradzione informacje, mało tego z dnia nadzień rozwój następuje tak szybko ze rzeczy dziś niemożliwe jutro mogą się wydarzy i narobić niewyobrażalnych szkód.
Należy zwrócić uwagę, że wartość i bezpieczeństwo informacji są elementami spójnymi, wzajemnie się uzupełniającymi i nierozerwalnymi. Dlatego dostęp do informacji to kolejny ważny element tej układanki. Wszystkie ważne osobiste dane przechowujemy aby z nich korzystać np. płacąc on-line za pomocą

systemów obsługi bankowej w internecie oraz udostępniając osobom do tego powołanych.

Obok wielu korzyści, jakie przyniósł nam rozwój techniczny, pojawiło się jednak wiele nowych zagrożeń związanych z bezpieczeństwem informacji. Największym z nich jest dostęp do informacji, których nie chcemy ujawniać. Jest to tym większy problem, że dane zastrzeżone są obecnie przechowywane w wielu miejscach, a ich ochrona często jest niedostateczna. Ewentualna kradzież informacji odbywa się najczęściej bez naszej wiedzy. Co więcej, nie jesteśmy w stanie przewidzieć wszystkich jej następstw oraz czasu, w którym przechwycona informacja zostanie wykorzystana przeciwko nam. Wyciek informacji może okazać się bardzo niebezpieczny i kosztowny, dlatego też wiele uwagi poświęca się mechanizmom i procedurom zabezpieczania informacji zastrzeżonej. Z drugiej strony coraz więcej grup pragnie uzyskać dostęp do tego rodzaju danych, łamiąc tworzone zabezpieczenia i osiągając przy tym wymierne korzyści finansowe. Tak więc strategia ochrony danych powinna uwzględniać w szczególności ciągłość w ich dostępności. Jest to szczególnie ważne np. w przypadku banków, które umożliwiają dostęp do konta drogą elektroniczną. W tym miejscu skupimy się jedynie na najważniejszych sposobach nieuprawnionego zdobywania informacji oraz metodach zakłóceń w jej dostępności i przetwarzaniu. Na początku przyjrzymy się najpopularniejszym narzędziom informatycznym, które wykorzystuje się do pozyskiwania informacji.

Przestępcy zajmujący się kradzieżą informacji dysponują ogromnym arsenałem środków technicznych pozwalających na dokonywanie włamań. Jeśli chodzi o narzędzia wykorzystywane przez hakerów do kradzieży jednym z bardziej znanych jest wirus komputerowy – jego główną cechą jest zdolność samo kopiowania. Wirusy komputerowe są pisane w językach niskiego poziomu. Dzięki temu wirus zajmuje stosunkowo mało miejsca, co utrudnia jego wykrycie. Wirus komputerowy, podobnie jak zwykły wirus, nie jest w stanie funkcjonować sam. Do działania potrzebuje innego programu, który infekuje stając się jego częścią. Efekty działania wirusów są trudne do przewidzenia. Czasami hakerzy tworzą wirusy dla rozgłosu reklamując w ten sposób swoje usługi.

1.3. Rozwój cyberprzestrzeni zagrożeniem dla bezpieczeństwa baz danych

Najczęściej wirusy są pisane po to aby kraść informacje a w szczególności hasła dostępu. Innym narzędziem jest robak[26] komputerowy którego głównym zadaniem jest rozprzestrzenianie się po komputerze ofiary. Robaki rozprzestrzeniają się poprzez załączniki do wiadomości e-mail, wiadomości wysyłane z komunikatorów czy internetu potrafią instalować inne programy bez wiedzy użytkownika np. Konie Trojańskie. Samodzielnie Koń Trojański podpina się pod aplikacje lub strony internetowe, którymi jest zainteresowany użytkownik. Implementują one dodatkowe programy np. szpiegujące, które następnie wysyłają do twórcy programu wszystkie znaki wpisywane poprzez klawiaturę, informują o otwieranych programach, stronach internetowych, umożliwiają kradzież danych itd.. W ten sposób twórca złośliwego oprogramowania potrafi przejąć cały komputer. Innym ciekawym programem jest Botnet należą do niego grupy komputerów zainfekowanych złośliwym oprogramowaniem. Właściciel komputera nie jest świadomy, iż ktoś inny wykorzystuje zasoby zainfekowanego komputera i w istocie sprawuje nad nim pełną kontrolę. Główną siłą sieci Botnetu jest jej wielkość zajęcie grupy komputerów może spowodować np. wysyłanie spamu lub otwieranie stron reklamowych które są własnością twórcy programu. Służą również jako narzędzie do zdobywania informacji oraz blokowania dostępu uczciwym użytkownikom do stron www. Ostatnim rodzajem ataku jest atak typu odmowa usług, który ma za zadanie uniemożliwienie funkcjonowania zaatakowanego serwera, sieci lokalnej lub strony www. Zazwyczaj polega on na zarzuceniu zaatakowaniu serwera ogromna ilością zleceń, która powoduje spowolnienie pracy lub brak reakcji systemu a w konsekwencji brak reakcji systemu na uczciwe zlecenia stałych jak i potencjalnych klientów serwera.

Rozwój sieci, powstawanie nowych aplikacji, zarządzanie płatnościami on-line wszystkie te nowoczesne nowinki niosą ze sobą ogrom zagrożeń, który powoduje ataki na informację cyfrową. Przestępcy mają najróżniejsze metody aby osiągnąć swój cel, często wykorzystują słabości systemów szukając

[26]**Robak** (ang. *worm*) jest podobny do wirusa, lecz w odróżnieniu od niego nie musi dołączać się do istniejącego programu. Robak używa sieci do przesyłania swoich kopii do podłączonych hostów. Robaki mogą działać samodzielnie i szybko się rozprzestrzeniać. Nie wymagają aktywacji czy ludzkiej interwencji. Samo rozprzestrzeniające się robaki sieciowe są o wiele groźniejsze niż pojedynczy wirus, gdyż mogą szybko zainfekować duże obszary Internetu.

w oprogramowaniu luk które mogą wykorzystać w ostatnim czasie przeszli na metody socjotechniczne najpierw poznają swoje ofiary badając mocne i słabe strony następnie przypuszczają atak.

Okazuje się iż największym niebezpieczeństwem jest brak rozsądku lub po prostu ludzka naiwność. Hakerzy wykorzystują takie osoby np. szukając zapisanych haseł do kont w ich komputerach. Innym przykładem jest wyłudzenie hasła, podszywając się pod godną zaufania osobę. Jeśli atakujący ma fizyczny dostęp do komputera, w którym przechowuje się poufne informacje, uzyskanie dostępu do nich może odbyć się np. poprzez instalację spreparowanego systemu. Wszystkie interakcje pomiędzy nieświadomym użytkownikiem a systemem będą wtedy rejestrowane i przesyłane do włamywacza, a ten bez problemu będzie w stanie uzyskać niezbędne hasła. Opisane powyżej przypadki uświadamiają nas jak ważne jest bezpieczeństwo. Najprawdopodobniej z tego powodu socjologowie oraz naukowcy innych dziedzin zajmują się bezpieczeństwem, interpretując swoje wnioski na podstawie badań. I tak prof. Jan Maciejewski w socjologiczno-psychologiczny sposób określił że „bezpieczeństwo oznacza brak zmartwień, kłopotów i przykrego uczucia strachu".

Żadnego z tych elementów nie można pominąć ponieważ wszystkie są ze sobą spójne i każde z nich pociąga za sobą ryzyko powstania kolejnych następstw. Na początku ludzkość miała jeden cel - przeżyć za wszelka cenę. Walka o byt przetrwania i troska zapewnienia bezpieczeństwa sobie i najbliższym były naturalną potrzebą. W miarę rozwoju cywilizacji i zmieniającego się świata potrzeba bezpieczeństwa człowiekowi już nie wystarczała, chciał czegoś więcej: stabilizacji, przewidywalności, rozwoju, dobrobytu i w końcu po prostu ludzkiego szczęścia. Dlatego jednoznacznie można stwierdzić, że bezpieczeństwo obejmuje zaspokojenie potrzeb takich jak: przetrwanie, istnienie, tożsamość, która mówi o identyczności, spokój, niezależność, posiadanie i możliwość dalszego rozwoju (Maciejewski, 2006, s. 65).

Definicja bezpieczeństwa jest wieloznaczna i brak jej jednolitej definicji. Według słownika terminów z zakresu bezpieczeństwa narodowego za bezpieczeństwo uważa się „ stan, który daje poczucie pewności i gwarancję jego zachowania oraz szansę na doskonalenie. Jest to jedna z podstawowych potrzeb człowieka" (*Słownik terminów z zakresu bezpieczeństwa narodowego*, 2002, s. 13) (Maciejewski, 2006, s. 65). Natomiast środowisko praktyków

bezpieczeństwo informacyjne uważa za ochronę informacji przed niepożądanym (przypadkowym lub świadomym) ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania. W tym celu są podejmowane środki bezpieczeństwa dla zapewnienia poufności, integralności i dostępności informacji. Ich celem jest wyeliminowanie zagrożenia dla informacji. W epoce rozwoju technologicznego i naukowego społeczeństwo stało się zachłanne, a element posiadania stał się wręcz najważniejszy, co postawiło go na pierwszym miejscu. Jest to jeden z czynników, który prowadzi na przestępczą stronę tej drogi. Jedni chronią swoje informacja a drudzy chcą je wykraść aby na tym skorzystać. Informacje są wykradane, niszczone i wykorzystywane w różnych celach. Najnowsze metody są już bardziej wyrafinowane należą do nich kradzież tożsamości lub poufnych informacji.

Prawne aspekty zwalczania cyberterroryzmu

W Polsce utworzono ponad dwieście aktów prawnych które maja zabezpieczać szeroko rozumiane interesy wszystkich obywateli. Do zapewnienia bezpieczeństwa przetwarzanych informacji firmy, jak i urzędy są zobligowane przez ustawy m.in. takie jak: ustawa o ochronie danych osobowych, ustawa o ochronie informacji niejawnych, ustawa o dostępie do informacji publicznej, – ustawa o prawie autorskim i prawach pokrewnych. Każda z właściwych ustaw narzuca na instytucję określone obowiązki w zakresie bezpieczeństwa informacji – obowiązki te dotyczą zarówno zachowania poufności określonych informacji, jak i ich dostępności i integralności (Gwoździewicz, Prokopowicz, 2016a,s.395). W obliczu postępującej informatyzacji społeczeństwa i ułatwionego dostępu do prywatnych informacji osób i podmiotów gospodarczych jednym z wymogów prawidłowego funkcjonowania gospodarki stała się prawna ochrona poufnych danych prywatnych. Nasze dane są obecnie przechowywane w wielu miejscach, a odpowiednie programy przetwarzają i klasyfikują je często bez naszej wiedzy ani przyzwolenia. Będąc użytkownikiem sieci udostępniamy swoje dane a z drugiej strony, walczymy o ochronę swojej prywatności i intymności odwołując się na zagwarantowane w konstytucji prawa dotyczące ochrony danych osobowych. Każdy obywatel który uważa ze jego prawa zostały naruszone może zwrócić się o zbadanie procesu przetwarzania jej danych do Generalnego Inspektora Ochrony Danych Osobowych.

Upowszechnianiu się technologii komunikacyjnych oraz wzrostowi zamożności obywateli świata towarzyszy rozwój społeczeństwa informacyjnego, który uzależniony jest od coraz bardziej zintegrowanych, konwergentnych narzędzi multimedialnych. Narzędzia te są źródłem swobodnego i nieskrępowanego dostępu do każdej informacji, o każdej porze i za pomocą każdego nośnika multimedialnego. „Wszystko to w oparciu o niewielkie koszty użytkowania sprawiło, że coraz więcej podmiotów (rządów, instytucji i firm), a także indywidualnych osób decyduje się przenosić różne elementy swojej codziennej aktywności do cyberprzestrzeni. Dostępny za pomocą komputerów, telefonów komórkowych, tabletów internet stał się jednym z podstawowych mediów, obok elektryczności, gazu i bieżącej wody. Stał się synonimem wolności słowa i nieskrępowanego przepływu informacji, a w pewnych przypadkach z powodzeniem służy jako narzędzie rewolucji i zmian społecznych" (Grzelak, Riedel, 2012, s. 126). Jak wcześniej wspomniano hakerzy tworzą złośliwe oprogramowania, niektóre śledzą naszą działalność w internecie zbierając różnego rodzaju dane lub służące do uszkodzenia systemów komputerowych bez wiedzy i zezwolenia ich właścicieli. Celowe szkodzenie systemów komputerowych, niszczenie danych lub ich zmiana czy kradzież to zadanie realizowane w drugiej kolejności, których skutki mogą być jednak bardzo kosztowne i nieodwracalne. Bardzo dobrym przykładem łamania prawa jest metoda „na wnuczka z facebooka" który jest kierowany do osób korzystających z bankowości elektronicznej. W ten sposób oszuści skłaniają internautę do zainfekowania własnego komputera prosząc go aby potwierdził operację kodem SMS. W obu przypadkach niezbędnym elementem tych oszustw jest dystrybucja złośliwego oprogramowania. Internetowi przestępcy wykazują się dzisiaj wystarczającym sprytem aby zbałamucić użytkowników poczty elektronicznej lub kont na portalach społecznościowych aby nieświadomie rozsyłali złośliwe oprogramowanie. W Polce (wg stanu na dzień 1 lipca 2017 r.) brak jest jednolitego ustawodawstwa regulującego instytucjonalno-prawny system ochrony cyberprzestrzeni RP. (Gwoździewicz i Jakubowski, 2017 s. 65) Przepisy określające wymagania w zakresie zarządzania bezpieczeństwem sieci i informacji systemów teleinformatycznych (dotyczące zarówno podmiotów prywatnych jak i jednostek sektora finansów publicznych) rozproszone są w różnych aktach prawnych m.in.:

1.3. Rozwój cyberprzestrzeni zagrożeniem dla bezpieczeństwa baz danych

1. ustawa z dnia 6 czerwca 1997r. *Kodeks karny;*
2. ustawa z dnia 29 sierpnia 1997r. *o ochronie danych osobowych;*
3. ustawa z dnia 27 sierpnia 2009r. *o finansach publicznych;*
4. ustawa z dnia 29 września 1994r. *o rachunkowości;*
5. ustawa z dnia 6 września 2001r. *o dostępie do informacji publicznej;*
6. ustawa z dnia 15 kwietnia 2011r. *o systemie informacji oświatowej;*
7. ustawa z dnia 28 kwietnia 2011r. *o systemie informacji w ochronie zdrowia;*
8. ustawa z dnia 14 lipca 1983r. *o narodowym zasobie archiwalnym i archiwach;*
9. ustawa z dnia 29 sierpnia 199 r. *Prawo bankowe;*
10. ustawa z dnia 18 września 2001r. *o podpisie elektronicznym;*
11. rozporządzenie PE i Rady z dnia 23 lipca 2014 r. *w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym;*
12. ustawa z dnia 18 lipca 2002r. *o świadczeniu usług drogą elektroniczną;*
13. ustawa z dnia 29 czerwca 1995 r. *o statystyce publicznej;*
14. ustawa z dnia 16 kwietnia 1993 r. *o zwalczaniu nieuczciwej konkurencji;*
15. ustawa z dnia 29 stycznia 2004 r. *Prawo zamówień publicznych.*

Poczynione uwagi pokazują, iż społeczne zapotrzebowanie na poczucie bezpieczeństwa skutkuje głównie pracami legislacyjnymi, nie tylko w obrębie prawa karnego, ale i w innych gałęziach prawa, ale nawet najlepsze regulacje prawne nie spełnią pokładanych w nich nadziei bez sprawnego funkcjonowania podmiotów, których zadaniem jest egzekwowanie przestrzegania tych regulacji.

Podsumowanie

Aby zadbać o cyberbezpieczeństwo należy jak najszybciej podjąć spójne i systemowe działania, mające na celu monitorowanie i przeciwdziałanie zagrożeniom występującym w cyberprzestrzeni oraz minimalizowanie skutków incydentów. Musimy skoordynować wszystkie podejmowane dobre inicjatywy, aby wyeliminować ich „wyspowy" charakter. Należy wdrożyć odpowiednie mechanizmy, w tym mechanizmy współpracy podmiotów prywatnych i państwowych (model oparty na współpracy administracji, biznesu i nauki) oraz odpowiedniego finansowania działań związanych z bezpieczeństwem IT.

Niezbędne jest określenie systemu finansowania zadań związanych z ochroną cyberprzestrzeni. I najważniejsze: „warunkami efektywnej ochrony cyberprzestrzeni jest przyjęcie ram prawnych krajowego systemu ochrony cyberprzestrzeni oraz wyznaczenie krajowego organu koordynującego działania innych podmiotów w zakresie ochrony cyberprzestrzeni” [27].

Pilne i niezbędne jest wdrożenie spójnego podziału kompetencji z zakresu obowiązków, procedur oraz szkoleń, treningów i kierunków prac badawczo-rozwojowych.

Zapewnienie bezpieczeństwa informacji jest wyzwaniem dla wszystkich podmiotów tworzących krajowy system cyberbezpieczeństwa, a więc podmiotów gospodarczych świadczących usługi przy wykorzystaniu systemów teleinformatycznych, użytkowników cyberprzestrzeni, organów władzy publicznej, a także wyspecjalizowanych podmiotów zajmujących się bezpieczeństwem teleinformatycznym w sferze operacyjnej. Jest to tym istotniejsze, iż Polska jest ściśle powiązana z innymi państwami poprzez współpracę międzynarodową w ramach takich organizacji jak UE, NATO, ONZ czy OBWE. Współpraca ta odgrywa istotną rolę w walce z rosnącą liczbą incydentów powodowanych nielegalnymi działaniami w cyberprzestrzeni, prowadzącymi do strat materialnych i wizerunkowych.

[27] https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf.

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

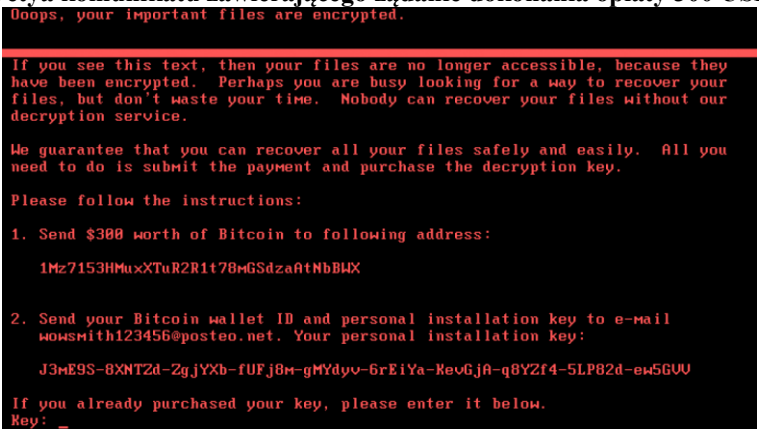
Wprowadzenie

W artykule opisano problematykę odnotowanego w 2016 roku silnego wzrostu aktywności w Internecie złośliwego oprogramowania typu ransomware, za pomocą którego cyberprzestępcy blokują działanie komputera, smartfona lub innego urządzenia podłączonego do globalnej sieci. W zainfekowanym w ten sposób komputerze lub innym urządzeniu ofiary cyberataku wyposażonym w mikroprocesor i internet wyświetlany jest komunikat z żądaniem zapłacenia okupu za przywrócenie prawidłowego działania zainfekowanego urządzenia (Gwoździewicz, 2016, s. 79). W obliczu narastających zagrożeń ataków hakerskich, w tym rozsyłania spamu zawierającego złośliwe oprogramowanie typu ransomware coraz więcej firm i banków tworzy dodatkowe zabezpieczenia systemów informatycznych i stale udoskonala pod tym względem wykorzystywane w prowadzonej działalności oprogramowanie i infrastrukturę informatyczną. Obecnie dominuje opinia, że proces ten nigdy się nie zakończy, przynajmniej dopóki realizuje się postęp technologiczny, ponieważ powstają nowe aplikacje i platformy internetowe, nowe wersje systemów operacyjnych oraz innowacyjne (Matosek, 2009, s. 34) urządzenia infrastruktury informatycznej powszechnie wykorzystywane przez użytkowników. Każda niedoskonałość systemów informatycznych, teleinformatycznych sieci internetowych, wewnętrznych procedur bezpieczeństwa zostaje szybko wykryta i wykorzystana przez cyberprzestępców (Dmowski, Prokopowicz, 2006, s. 79). Dotychczas dominował model łatania luk w zabezpieczeniach wcześniej wykrytych przez hakerów. Biorąc pod uwagę silny wzrost aktywności niebezpiecznych programów ransomware model ten powinien ulec zmianie polegającej na odwróceniu kolejności działań. To zatrudnieni w firmach, bankach i instytucjach publicznych informatycy powinni wyprzedzając

cyberprzestępców możliwie najwcześniej wykrywać luki w zabezpieczeniach (Prokopowicz, 2017, s. 104). W związku z tym obecnie wzrasta potrzeba prewencyjnego, profilaktycznego w swej istocie procesu doskonalenia procesów zarządzania ryzykiem systemów informatycznych funkcjonujących w instytucjach finansowych (Prokopowicz, 2011, s. 37), przedsiębiorstwach oraz podmiotach sektora publicznego.

27 czerwca 2017 wiele instytucji publicznych i przedsiębiorstw na Ukrainie i w kilku innych krajach w Europie zaatakowanych zostało przez cyberprzestępców z wykorzystaniem wirusa typu ransomware Petya. Według analityków firmy Microsoft około 70 proc. wszystkich zainfekowanych komputerów zlokalizowanych było na Ukrainie (Długosz, 2017). W skutecznie zaatakowanych komputerach wirus ten zachowuje się jak klasyczny ransomware tj. blokuje dostęp do komputera szurfując dane i wyświetla się komunikat z żądaniem zapłacenia okupu 300 USD w bitcoinach za odblokowanie komputera.

Rysunek 4. Obraz wyświetlonego w zainfekowanym komputerze wirusem Petya komunikatu zawierającego żądanie dokonania opłaty 300 USD.



Źródło: *Ransomware Recap: Petya Ransomware Outbreak Shakes Europe* [w:] Portal internetowy analitycznej firmy technologicznej „TrendMicro", 28.06.2017 (www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-petya-ransomware-outbreak-shakes-europe).

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

Jednak szczególna szkodliwość wirusa Petya wynika z jego specyficznej właściwości multiplikowania się w kolejnych komputerach połączonych w sieci. Otóż wirus ten po skutecznym zainfekowaniu komputera wyszukuje inne komputery w sieci danej firmy i je infekuje. Wirus ten szybko rozprzestrzeniał się w ten sposób w firmach funkcjonujących w jednej grupie kapitałowej lub w oddziałach danej organizacji połączonych określonym wewnętrznym systemem informatycznym.

Szczególnie istotną kwestią odróżniającą ten atak hakerski typu ransomware od innych podobnych tego typu ataków jest motyw przeprowadzenia tego ataku. Otóż wiele wskazuje na to, że typ tego wirusa, tj. skonstruowanie tego wirusa przez hakerów jako ransomware pozornie może sugerować bezpośrednio głównie finansowy charakter tego ataku hakerskiego. Wirusy typu ransomware tworzone są już od lat, jednak w ostatnich latach odnotowano nasilenie występowania przypadków ataków z użyciem tego typu wirusów. Większość tego typu ataków miała na celu wyłudzenie pieniędzy od firm i instytucji za odblokowanie zablokowanych poprzez infekcję określonym wirusem ransomware komputerów (*Konsekwencje ataku Petya*, 2017).

W związku z powyższym wiele wskazuje na to, że mimo stworzenia przez hakerów wirusa Petya jako ransomware to jednak głównym celem przeprowadzenia ataku na instytucje publiczne na Ukrainie z zastosowaniem tego wirusa nie był cel finansowy. Kierownik zespołu eksperckiego w ONZ ds. przestępczości cybernetycznej oświadczył, że nie można wykluczyć innego celu przeprowadzenia tego ataku oprócz celu finansowego. Nie można także wykluczyć ewentualności, że ewentualny cel finansowy o ile logistycznie w ogóle byłby możliwy miał być swego rodzaju kamuflażem dla innego celu, być może ważniejszego z punktu widzenia analizy strategii badania systemów bezpieczeństwa cybernetycznego. Potwierdzeniem tej tezy są następujące fakty (Długosz, 2017):

- atak został przeprowadzony w taki sposób co sugeruje, że jego celem były główne państwowe instytucje i przedsiębiorstwa Ukrainy,

- wykorzystany w atakach przeprowadzonych w końcówce czerwca 2017 wirus okazał się znacząco zmodyfikowaną wersją pierwowzoru wirusa Petya, którego hakerzy używali do przeprowadzania ataków w okresie od kilku do kilkunastu miesięcy poprzedzających omawiany w niniejszym artykule atak hakerski,
- źródła ataku hakerskiego z użyciem omawianej zmodyfikowanej wersji wirusa Petya wskazują na Rosję, która od kilku lat prowadzi agresywną, w tym z użyciem działań zbrojnych politykę wobec Ukrainy,
- atak ten błyskawicznie rozprzestrzenił się na terytorium Ukrainy i blokował komputery wielu instytucji publicznych, finansowych i przedsiębiorstw reprezentujących kluczowe strategicznie sektory krajowej gospodarki w tym logistyczny, komunikacyjny, transportowy, energetyczny itd.,
- atak wirusa Petya przeprowadzony został 27 czerwca głównie na Ukrainie jednak już tego samego dnia negatywna działalność tego wirus odnotowana została w co najmniej kilku innych krajach w Europie,
- wirus Petya błyskawicznie rozprzestrzeniał się w analogiczny sposób jak niedawne ataki hakerskie z zastosowaniem innego wirusa ransomware WannaCry,
- wirus Petya zbudowany został na podstawie wykradzionego i zhakowanego oprogramowania amerykańskiej Agencji Bezpieczeństwa Wewnętrznego,
- serwer hakerski na który użytkownicy zablokowanych komputerów mieli dokonywać wpłacania okupu 300 USD w bitcoinach został szybko i skutecznie zablokowany przez służby bezpieczeństwa cybernetycznego natomiast wirus Petya mógł nadal kopiować się w kolejnych komputerach połączonych w sieciach poszczególnych firm i instytucji.

W związku z powyższym także analitycy z firmy technologicznej Kasperski wskazywali, że z powodu zablokowania wspomnianego serwera hakerów użytkownicy zablokowanych komputerów nie będą w stanie przywrócić dostępu do zaszyfrowanych danych niezależnie od tego czy dokonają transakcji przelewu tych 300 USD z tytułu zapłacenia okupu (*Twórca wirusa Petya…*, 2017). W związku z powyższym rozwój technologii informatycznej i globalizacja przyniosły nowe wyzwania dla ochrony informacji w systemach

teleinformatycznych. Niezbędnym jest przeprowadzenie na bieżąco nowelizacji normatywów prawnych określających kluczowe kwestie transakcji przeprowadzanych w zakresie elektronicznej bankowości oraz główne zasady bezpieczeństwa systemów informatycznych w Polsce (Domańska-Szaruga, 2013, s. 267).

Bezpieczeństwo systemów informatycznych w ujęciu instytucjonalnym i indywidualnym w kontekście ataku z wykorzystaniem wirusa Petya

Z analizy skutków spowodowanych hakerskim atakiem z użyciem wirusa typu ransomware o nazwie Petya wynika, że o ile zakłócenia w funkcjonowaniu infrastruktury komunikacyjnej i teleinformatycznej odnotowane we Francji najprawdopodobniej były niezamierzonym wtórnym efektem rozprzestrzeniania się tego wirusa w skali europejskiej o tyle analogiczne problemy wywołane na Ukrainie już raczej nie były całkowicie przypadkowe. Tezę tę potwierdza skala szkód jakie ten wirus spowodował w tym kraju oraz specyficzny mechanizm rozprzestrzeniania się tego wirusa po instytucjach i firmach na Ukrainie. Zwolennicy teorii spiskowych wskazują na polityczne podłoże tego ataku hakerskiego, który jako celowe działanie określonych dywersyjnych służb rosyjskich miałby być wymierzony właśnie w Ukrainę. W okresie ostatnich kilkunastu lat na Ukrainie wystąpiły znaczące zmiany układu sił politycznych. Zmiany te były na tyle istotne, że Ukraina stała się krajem, który wyszedł spod strefy wpływów Rosji i coraz bardziej ukierunkowywał swoją politykę tak, aby była zbieżna z polityką Unii Europejskiej. Oczywistym jest więc, że to nie mogło iść w parze z linią polityczną Kremla i w końcu doprowadziło do agresji zbrojnej Rosji na terytorium Ukrainy. W związku z tym jeżeli wirus Petya wygenerowany został w Rosji i spowodował największe szkody w infrastrukturze instytucji publicznych i wielu przedsiębiorstw właśnie na Ukrainie to wiązanie tego ataku hakerskiego z napiętą polityką jaka od wielu już lat realizuje się między tymi krajami jest uzasadnione (*Ataki złośliwego oprogramowania Petya,* 2017).

Kolejnym czynnikiem, który potwierdzać może tę tezę z gatunku political fiction jest rodzaj oprogramowania, które jako pierwsze było zainfekowane wirusem Petya na Ukrainie. Kilka lat temu realizujący prounijną politykę Prezydent

Ukrainy Petro Poroszenko otrzymując sygnały o inwigilacji systemów informatycznych przez rosyjskie tajne służby celem potencjalnego ograniczenia możliwości tej dywersyjnej działalności, która mogłaby doprowadzić do poważnej destabilizacji krajowej infrastruktury teleinformatycznej i kluczowych przedsiębiorstw i instytucji na Ukrainie. W związku z tym Prezydent Petro Poroszenko zarządził wprowadzenie sankcji dla rosyjskich przedsiębiorstw działających na Ukrainie w sektorze IT. Jednym z elementów tych sankcji było zastąpienie rosyjskiego oprogramowania „1C" nowym, stworzonym w tym celu krajowym oprogramowaniem M.E. Doc, które zainstalowane zostało w większości ukraińskich urzędach i wielu firmach. Powszechność występowania tego oprogramowania na Ukrainie wynikała między innymi z faktu pełnienia istotnej roli w systemie podatkowym, ponieważ program ten stał się podstawowym systemem ułatwiającym prowadzenie raportowania finansowego i rozliczeń podatkowych za pośrednictwem internetu. Ta właśnie kwestia, tj. powszechność występowania i wykorzystywania tego oprogramowania przez wiele urzędów i firm w kraju miała kluczowe znaczenie dla błyskawicznego rozprzestrzenienia się wirusa Petya na Ukrainie. W związku z tym zainfekowanie powszechnie stosowanego oprogramowania M.E. Doc spowodowało bardzo szybkie, trwające zaledwie kilka godzin zmultiplikowanie tego ataku hakerskiego w obszarze całego kraju. Trudno więc podważyć tezę, że wybór tego oprogramowania na przeprowadzenie ataku z użyciem wirusa Petya nie było celowe i w związku z tym zainfekowanie oprogramowania M.E. Doc miałoby się okazać całkowicie przypadkowe (*Kogo zaraził wirus Petya?...*, 2017).

Z analiz przeprowadzonych przez ukraińskie służby bezpieczeństwa cybernetycznego i wydane przez departament Cyberpolicji Narodowej Policji Ukrainy na tej podstawie oświadczenie wynika, że infekcja oprogramowania M.E. Doc została dokonana poprzez przejęcie kontroli portalu służącego do automatycznej aktualizacji tej aplikacji. Szczególnie niepokojącą kwestią jest to, że infekcja oprogramowania M.E. Doc zrealizowana została na komputerach wyposażonych w system operacyjny Windows (Czechowicz, 2017) bez względu na jego wersję, tj. nie tylko starszych, nieaktualizowanych już przez producenta

tj. korporację Microsoft wersji, ale również powszechnie występującego w wielu firmach i instytucjach systemu operacyjnego Windows 7 a nawet wersji nowszej Windows 10 jeżeli nie była na bieżąco aktualizowana (Danes, 2016).
Zgodnie z powyższym atak hakerski z użyciem wirusa Petya spowodował paraliż działania systemów transakcyjnych, teleinformatycznych i infrastruktury wielu ukraińskich instytucji i przedsiębiorstw, od instytucji rządowych, publicznych, po instytucje finansowe, banki, lotniska, Metro w Kijowie, podmioty sektora energetycznego, w tym nieczynną elektrownię w Czarnobylu. Jednak wirus poprzez ponadnarodowe powiązania kapitałowe szybko rozprzestrzenił się na inne kraje w Europie. Wirus Petya zaatakował między innymi rosyjski Rosnieft, duński koncern A.P. Moeller-Maersk, brytyjską firmę WPP oraz port w Rotterdamie. Wirus ten dotarł także do co najmniej kilkunastu większych firm działających w Polsce takich jak MediaCom i Kronospan z branży medialnej, Intercars z branży motoryzacyjnej, TNT i Raben z branży logistycznej oraz wrocławska firma Mondelez.
Potwierdzeniem tezy sugerującej ponadnarodowe rozprzestrzenianie się wirusa Petya poprzez powiązania kapitałowe spółek są firmy, których komputery odnotowały atak tego wirusa zlokalizowane poza Ukrainą, Rosją i Polską. Tymi firmami były głównie koncerny charakteryzujące się globalnym zasięgiem działalności, których spółki matki lub spółki córki posiadają biura na Ukrainie. Ta sama zasada dotyczy także zainfekowanych tym wirusem komputerów działających w firmach zlokalizowanych w Polsce tj. wszystkie podmioty, które zostały zainfekowane w Polsce posiadają biura, centra logistyczne lub fabryki na Ukrainie (*Wirus Petya zaatakował Polskę…*, 2017).
Działające w Polsce Narodowe Centrum Cyberbezpieczeństwa nie odnotowało jednak wielu niepokojących zgłoszeń i skutków infekcji systemów informatycznych w związku z czym nie został znacząco podniesiony poziom w zakresie potencjalnych cyberzagrożeń. Z drugiej strony jednak wystosowany został w mediach apel do obywateli, aby w tym dniu zachowane zostały szczególne środki ostrożności w korzystaniu z komputerów podłączonych do sieci internet oraz podane zostały zalecenia, które miały ograniczyć

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

negatywne działanie tego już wówczas ponadnarodowego ataku hakerskiego z użyciem wirusa Petya.
Jedno z ostrzeżeń było apelem aby nie dokonywać żadnych czynności, a szczególnie nie dokonywać transakcji płatności 300 USD w bitcoinach czego żądali hakerzy w treści wyświetlanego komunikatu, który się pojawiał na monitorach zablokowanych komputerów. Zapłacenie tego okupu nie wiązałoby się że zdjęciem blokady, ponieważ już w 28 czerwca 2017 roku założony prze hakerów serwer, który miał przyjmować te wpłaty został zablokowany przez służby bezpieczeństwa cybernetycznego. W związku z zablokowaniem serwera hakerów, nie możliwym stało się wysłanie indywidualnego klucza generowanego na wyświetlanym na ekranie zablokowanego komputera komunikacie, tj. wygenerowanym przez wirus ransomware Petya żądaniu opłacenia okupu za odblokowanie komputera. Oznacza to, że w sytuacji dokonania tej płatności 300 USD pieniądze były by stracone, ponieważ hakerzy nie mieli by możliwości ich odebrania a nawet wyeliminowana została możliwość jakiegokolwiek kontaktu hakerów z tym serwerem i poszkodowanymi użytkownikami zablokowanych komputerów (*Kogo zaraził wirus Petya? ...,* 2017).

Wirus Petya znacznie groźniejszy od WannaCry

Ekspert w zakresie zabezpieczeń systemów informatycznych Aamir Lakhani z zespołu FortiGuard Labs firmy Fortinet wskazuje, że cyberprzestępcy tworzący złośliwe oprogramowanie ransomware od niedawna stosują dwie metody wykorzystania zdiagnozowanych luk w zabezpieczeniach systemów operacyjnych i aplikacji komputerowych. Nowe rodziny wirusów ransomware, które od końca 2016 roku pojawiały się w Internecie, w tym WannaCry i Petya są nowymi rodzajami wirusów, w których twórcy połączyli znane od lat techniki hakerskie z nowymi rozwiązaniami socjotechnicznymi opartymi na formule wymuszania okupu za odblokowanie zaszyfrowanych danych zawartych na dyskach komputerów. Najgroźniejszy cyberatak z zastosowaniem wirusa WannaCry przeprowadzony został w maju 2017 natomiast wirus Petya zainfekował nową odmianą ransomware wiele komputerów na całym świecie

pod koniec czerwca 2017 roku (Radzewicz, *FAQ: ransomware Petya …,* 2017). Otóż przy tworzeniu wirusa WannaCry hakerzy po raz pierwszy zastosowali innowacyjne rozwiązanie połączenia oprogramowania ransomware ze znanym sprzed lat robakiem (Stech, *Petya Wielki…,* 2017). Celem tego połączenia i zbudowania w ten sposób nowego rodzaju wirusa miało być znaczące przyśpieszenie procesu infekowania systemów operacyjnych w kolejnych komputerach i w związku z tym aby osiągnąć potencjalnie znacznie szerszą skalę cyberataku niż w analogicznych infekcjach z zastosowaniem wcześniej tworzonych rodzajów wirusów. W wyniku tego wymienionego powyżej połączenia funkcjonalności stworzono nowy rodzaj wirusa, którego nazwano jako „ransomworm", czyli robak infekujący system operacyjny komputera, blokujący dostęp do plików zawartych na dyskach i żądający zapłacenia okupu za odblokowanie zaszyfrowanych danych. Drugi z wymienionych powyżej wirusów, który pod koniec czerwca błyskawicznie rozprzestrzenił się w skali globalnej infekując komputery wielu firm i instytucji tj. wirus Petya okazał się kolejną generacją, tj. bardziej zaawansowaną formą tego typu wirusa, która przeprowadza atak infekując Master Boot Record systemu operacyjnego komputera. Realizowana w ten sposób infekcja w sytuacji nieopłacenia żądanego okupu przez użytkowników zainfekowanych komputerów wiąże się z utratą zawartych na dyskach zaszyfrowanych danych, a nawet potencjalnie może także oznaczać uniemożliwienie ponownego uruchomienia systemu operacyjnego (Stech, *Petya Wielki…,* 2017).

Jedną z firm technologicznych, które zajmują się monitorowaniem i badaniem problematyki bezpieczeństwa transferu danych w Internecie jest firma Trend Micro. Firma ta uznawana jest także za globalnego lidera w zakresie zabezpieczeń i bezpieczeństwa systemów informatycznych, w tym zakresie bankowości internetowej (*Raport Trend Micro: wzrost liczby ataków…*, 2017). Z przeprowadzonych analiz wynika, że skala potencjalnych zagrożeń, w tym przypadków cyberataków w ostatnich latach rosła szybciej niż innego rodzaju zagrożeń i prób dokonywania kradzieży danych i środków finansowych w firmach i bankach. O skali rosnącego zagrożenia informują liczby. Otóż w 2016 roku analitycy wydziału Smart Protection Network ™ w firmie Trend

Micro ™ wykryli i ustanowili blokady dla ponad 81 miliardów przypadków różnych form ataków online i innych cyberzagrożeń. Ustanowione blokady dotyczyły głównie ograniczenia ingerencji rozsyłanego przez cyberprzestępców spamu i trafiających do skrzynek mailowych e-mali z załącznikami zawierającymi złośliwe oprogramowanie malware i ransomware oraz Business E-mail Compromise. Jeszcze 2-3 lata temu tego typu spam rozsyłany był masowo metodą typu BEC (*Billion-Dollar Scams…*, 2016) do różnych podmiotów gospodarczych, instytucji i użytkowników indywidualnych. Natomiast w ostatnich kilku kwartałach cyberataki z użyciem oprogramowania złośliwego ransomware oraz metodą BEC przeprowadzane są głównie na systemy informatyczne korporacji i banków, tj. do podmiotów od których z większym prawdopodobieństwem można wyłudzić znaczne środki finansowe za odblokowanie zaszyfrowanego dostępu do komputera. Na podstawie przeprowadzonych analiz firma Trend Micro w raporcie „*TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats*" (*TrendLabs 2016 Annual Security Roundup…*, 2017) podaje, że samych tylko cyberataków z użyciem złośliwego oprogramowania ransomware odnotowano już ponad miliard i skala tego rodzaju cyberprzestępczości nadal szybko rośnie.

Marek Krauze ekspert ds. cyberbezpieczeństwa w firmie Trend Micro wskazuje, że odnotowany pod koniec czerwca 2017 roku cyberatak z użyciem wirusa Petya potencjalnie należał do jednych z najniebezpieczniejszych jakie do tej pory odnotowano w cyberprzestrzeni. Do stworzenia tego nowego rodzaju ransomware Petya zaimplementowano znane sprzed lat rozwiązania tzw. robaków internetowych w ich szczególnie niebezpiecznych wariantach. Wysoki poziom zagrożenia infekcją systemów informatycznych wynika z tego, że w tych nowych wersjach złośliwego oprogramowania określanego także jako ransomworm cyberprzestępcy wykorzystali zdiagnozowaną lukę w systemach bezpieczeństwa, do której penetracji wykorzystywane były w infekowanych systemach teleinformatycznych exploity, związane z tzw. wyciekiem Shadow Brockers. Ten spektakularny wyciek dotyczył zhakowania i wykradzenia przez hakerów eksploitów z amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA). Niektóre z tych wykradzionych z NSA eksploitów, wykorzystano przy

swego rodzaju udoskonalaniu i tworzeniu nowych, bardziej złośliwych programów ransomware WannaCry oraz Petya. Poza tym przy tworzeniu nowych odmian tych wirusów ransomware nie tylko zostały użyte wspomniane exploity, ale także narzędzia, z którego powszechnie korzystają hackerzy i administratorzy tj. pozwalających na wykonywanie poleceń w ramach zdalnej kontroli innych komputerów oraz dla komputerów pracujących w wewnętrznej sieci firmowej. Cyberataki przeprowadzane z wykorzystaniem zdiagnozowanych luk w systemach bezpieczeństwa sieci informatycznych nie jest łatwo skutecznie zablokować. W związku z powyższym przeprowadzone w maju i czerwcu ataki z użyciem ransomware WannaCry oraz Petya wskazały potrzebę przeprowadzania permanentnej diagnostyki i doskonalenia systemów bezpieczeństwa sieci informatycznych funkcjonujących w firmach i instytucjach finansowych oraz publicznych.

Z analiz firmy Trend Micro wynika, że przeprowadzony pod koniec czerwca w Polsce atak ransomware Petya zdiagnozowany został w głównie z w średnich i większych firmach, które powiązane są kapitałowo, logistycznie lub handlowo. Jednak z informacji prasowych wynika, że wirus Petya zainfekował także podmioty gospodarcze reprezentujące sektor MSP w Polsce, których większość nie ma żadnych powiązań z przedsiębiorstwami działającymi na Ukrainie. W związku z tym część infekcji w Polsce najprawdopodobniej dokonana została poprzez pocztę elektroniczną (Stech, *Petya Wielki…*, 2017).

Na Ukrainie zdiagnozowano dwie metody rozprzestrzeniania się ransome Petya. Jedna z tych metod, którą można by określić jako klasyczną jest rodzajem phisingu. Metoda tej infekcji została potwierdzona przez Służbę Bezpieczeństwa Ukrainy, oraz przez globalnie działające analityczne firmy technologiczne. Phishing ten polegał na infekowaniu systemu operacyjnego z załącznika przychodzącego z mailem imitującym wiadomość od zaufanej instytucji. Infekcja dokonana w jednym firmowym czy instytucjonalnym komputerze błyskawicznie rozprzestrzeniała się na inne komputery podłączone do sieci firmowej. Natomiast druga metoda infekowania komputerów, głównie firm i instytucji polegała na znakowaniu przez cyberprzestępców serwera, który sugerował użytkownikom przeprowadzenie aktualizacji popularnego

na Ukrainie oprogramowania do prowadzenia rozliczeń podatkowych M.E. Doc. Ponieważ program ten jest popularny, stosowany przez większość podmiotów gospodarczych i instytucji finansowych na Ukrainie, więc skala infekcji była wyjątkowo wysoka. Ten rodzaj infekcji potwierdziły już w dniu przeprowadzonego cyberataku firma analityczna Cisco Talos oraz ukraiński wydział policji zajmujący się cyberprzestępczością. Zdiagnozowana formuła cyberataków z użyciem ransomware Petya potwierdziła wcześniej już sformułowane tezy po przeprowadzeniu przez firmę Cisco badań dotyczących stanu cyberbezpieczeństwa w skali globalnej (*Cisco 2017 Annual Cybersecurity* …, 2017).

Podstawowe zasady bezpieczeństwa w zakresie ochrony systemów informatycznych przed cyberatakiem z użyciem wirusów ransomware

Powyższe spostrzeżenia potwierdzają analitycy z firmy Trend Micro wskazując, że ten cyberatak przeprowadzony z użyciem wirusa Petya posiadał typowe cechy ataku socjotechnicznego. Klasyczny socjotechniczny cyberatak polega na tym, że użytkownik komputera otrzymuje maila np. od dostawcy energii elektrycznej lub operatora telefonii komórkowej, do którego jest podpięty załącznik z rachunkiem do opłacenia. Wiadomość mailowa i załącznik wygląda niemal identycznie wobec tych jakie zwykle co miesiąc otrzymujemy. Socjotechnicznym zabiegiem twórców tych sfałszowanych maili i faktur jest np. wystawianie tych podrobionych rachunków ze wstawioną kilkukrotnie wyższą kwotą wobec tej, którą zwykle gospodarstwa domowej i firmy opłacają. Znaczna cześć nieświadomych potencjalnego zagrożenia użytkowników powodowanych najzwyklejszą ciekawością i niepokojem, niekiedy także emocjonalnie otwiera tę wiadomość i klika na załącznik co powoduje zainfekowanie komputera. Może się zdarzyć, że użytkownik przeglądający treść załącznika nadal nie jest świadomy infekcji swego komputera, ponieważ proces tej infekcji może odbywać się w tle systemu operacyjnego, czyli celowo tak aby ten proces infekcji nie został zauważony. Jest to celowy zabieg często stosowany przez cyberprzestępców, ponieważ w ten sposób zainfekowany komputer może

stać się instrumentem do przekazywania wirusa dla innych komputerów połączonych w sieci firmowej, domowej lub poprzez pocztę mailową.
Agencja informacyjna PAP już w dniu przeprowadzanego cyberataku podała, że analogiczne wnioski względem wstępnych analiz firmy Trend Micro podał Juliusz Brzostek, dyrektor Narodowego Centrum Cyberbezpieczeństwa w NASK w Polsce, oraz sformułował hipotezę, zgodnie z którą nie można wykluczyć podobnego cyberataku w Polsce nawet o porównywalnej skali infekcji jaka wystąpiła na Ukrainie. Według NASK skala potencjalnego zagrożenia była również w Polsce wysoka. Jednak z przeprowadzonych już na początku lipca analiz skali infekcji komputerów użytkowników domowych, firm i instytucji w Polsce wynika, że skala cyberataku w Polsce była wielokrotnie niższa niż ta odnotowana na Ukrainie. W Polsce zainfekowane zostały głównie przedsiębiorstwa sektora usługowo-handlowego i logistyki powiązane kapitałowo lub biznesowo ze spółkami działającymi na Ukrainie. Nie znaczy to jednak, że właściciele, kierownictwo firm i instytucji nie przestrzegali pracowników przez potencjalnym zagrożeniem dla prawidłowego funkcjonowania organizacji. W części firm pracownicy musieli się pogodzić z ewentualnością opóźnień wypłaty wynagrodzeń i oddelegowani zostali do domu, aby nie pracowali na komputerach firmowych w dniu, w którym przewidywany był cyberatak w Polsce. Biorąc pod uwagę globalny zakres infekcji komputerów dokonanej z zastosowaniem wirusa Petya to cyberatak przeprowadzony w dniach 27-28 czerwca 2017 roku przypominał pod wieloma względami ten z maja 2017 r., podczas którego wirus WannaCry, zainfekował kilkaset tysięcy komputerów w 150 krajach (*Wirus Petya. Jak działa …*, 2017).
Leszek Tasiemski, analityk ds. cyberbezpieczeństwa w firmie F-Secure przestrzega, że podobne cyberataki mogą się pojawić w przyszłości, i nie można wykluczyć, że użyte złośliwe oprogramowanie nie będzie stanowiło jeszcze większego zagrożenia cybernetycznego zarówno dla gospodarstw domowych jak podmiotów gospodarczych i instytucji publicznych. Sean Sullivan, ekspert ds. cyberbezpieczeństwa także z firmy F-Secure wskazuję, że cyberataki z zastosowaniem wirusów WannaCry i Petya zróżnicowane były także w zakresie grupy docelowej rodzajów użytkowników która stanowiła cel ataku.

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

Pod tym względem w przypadku przeprowadzonego w maju 2017 roku ataku z użyciem ransomware WannaCry grupa docelowa nie była precyzyjnie zdefiniowana, wirus zainfekował tysiące komputerów różnych rodzajów firm, instytucji oraz użytkowników indywidualnych w skali globalnej. Skala infekcji była tak duża, że analitycy ds. bezpieczeństwa rozważają hipotezę, czy aby ten cyberatak nie wymknął się spod kontroli hakerów, którzy ten proces zainicjowali (*Konsekwencje ataku Petya*…, 2017). Wirus Petya został w tej kwestii usprawniony tak aby nie był kierowany do wszystkich użytkowników tylko do komputerów funkcjonujących w większych firmach, instytucjach finansowych, publicznych i rządowych. W przypadku przeprowadzonego pod koniec czerwca cyberataku z zastosowaniem wirusa Petya to biorąc pod uwagę kwestię grupy docelowej przeprowadzanej infekcji komputerów powyżej wymienione fakty sugerują głównie finansowy cel stworzenia tego wirusa (*Wirus Petya. Jak działa* …, 2017).

W związku z powyższym eksperci firm technologicznych rekomendują podejmowanie następujących działań, które zmniejszają prawdopodobieństwo infekcji m.in. wirusami ransomware systemów informatycznych instytucji, finansowych publicznych i przedsiębiorstw:

- tworzenie kopii bezpieczeństwa danych na zewnętrznych dyskach pozbawionych dostępu do internetu,
- bieżące uaktualnianie systemów operacyjnych Windows oraz innych użytkowanych prze firmy i instytucje jak również instalowanie najnowszych wersji oprogramowania wykorzystywanego w tych podmiotach,
- cykliczne przeprowadzanie szkoleń dla wszystkich pracowników odpowiedzialnych za bezpieczeństwo systemów informatycznych oraz pracowników operacyjnych wykorzystujących firmowe komputery do codziennej pracy.

Jednak rozwijając te wymienione powyżej zalecenia należy dodać jeszcze kilka innych praktycznych porad, które mogą znacząco podnieść poziom bezpieczeństwa cybernetycznego w firmach i instytucjach. Otóż, w sytuacji gdy pojawia się wysokie prawdopodobieństwo zainfekowania użytkowanego komputera przez wirus z rodzaju ransomware to ważne jest stosowanie kilku

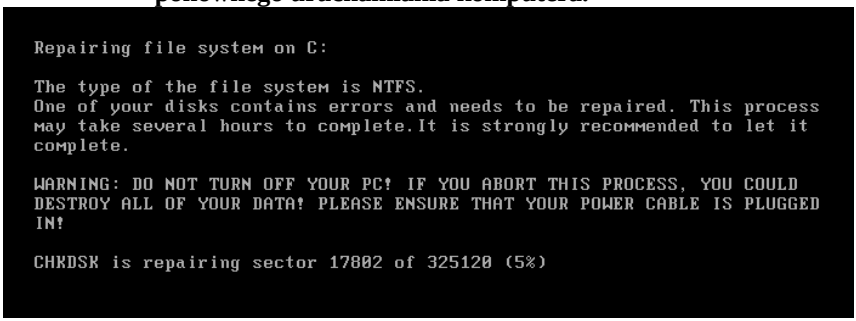
kluczowych zasad w kontekście obsługi komputera, które mogą uchronić infekowany komputer przez zaszyfrowaniem i bezpowrotną utratą istotnych danych. Jedną z tych zasad postępowania jest wyłączenie komputera w odpowiednim momencie, gdy pojawiło się podejrzenie o możliwości jego zainfekowania. Otóż w takiej sytuacji, gdy podczas uruchamiania komputera na monitorze pojawi się program CHKDSK, wówczas należy jak najszybciej wyłączyć komputer, aby wirus nie zdążył zaszyfrować zawartych na dyskach plików. W sytuacji, gdy użytkownik nie wyłączy komputera w tym momencie lub wyłączy komputer w kolejnym etapie uruchamiania systemu operacyjnego to wówczas zawarte na dyskach dane ulegną zaszyfrowaniu i nawet opłacenie okupu zgodnie z żądaniem hakerów wyświetlonym na ekranie zainfekowanego komputera może okazać się zupełnie bezskuteczne a zaszyfrowane dane praktycznie zostaną utracone jeżeli wcześniej nie wykonano ich kopii na innych dyskach pozbawionych dostępu do internetu.

Cechą charakterystyczną wirusa Petya jest to, że ten ransomware nie szyfruje pojedynczych plików tylko blokuje cały system operacyjny uniemożliwiając odczytanie danych z dysków zainfekowanego komputera. Jest to kolejny istotny czynnik świadczący o wysokiej potencjalnej szkodliwości tego wirusa. Blokowanie systemu operacyjnego polega na tym, że po początkowej infekcji systemu wirus dopełnia proces infekcji po ponownym uruchomieniu komputera i tym razem szyfruje główną tablicę plików (MFT) na dysku twardym. W związku z tym uruchomienie systemu przez Master Boot Record (MBR) staje się niemożliwe, ponieważ zaszyfrowane zostają niezbędne dla uruchomienia systemu operacyjnego oraz dla odczytania poszczególnych plików na dyskach informacje tj. nazwy, rozmiary i lokalizacje poszczególnych plików.

Innowacyjność w stworzeniu złośliwego oprogramowania Petya polega także, na tym, że wirus ten nie zachowuje się w sposób w pełni analogiczny jak wcześniej stworzone inne rozdaje ransomware. W sytuacji gdy wirus ten wymusza ponowne uruchomienie komputera wówczas na początku procesu uruchamiania systemu operacyjnego, pojawia się monit z informacją w języku angielskim następującej treści: „Nie wyłączaj komputera! Jeżeli przerwiesz

proces ładowania systemu, to spowodujesz utratę wszystkich swoich danych! Upewnij się, że kabel zasilania jest właściwie podpięty!" (Danes, 2016).

Rysunek 5. Wygenerowany przez wirus Petya krytyczny monit podczas ponownego uruchamiania komputera.



Źródło: L. Danes, *Wirus Petya. Jak się go pozbyć?* [w:] Witryna internetowa „Usuń Wirusa", 15.04.2016, (https://usunwirusa.pl/wirus-petya).

Jednak celem tego komunikatu wprowadzenie w błąd nieświadomego specyfiki przebiegu procesu infekcji i niedopuszczenie do przerwania ładowania systemu, który już jest zainfekowany i w tym właśnie momencie dokonywane jest szyfrowanie plików systemowych. W związku z tym aby uchronić dane przez zaszyfrowaniem do nich dostępu to należy zrobić dokładnie odwrotnie wobec polecenia zawartego w treści tego komunikatu i jak najszybciej wyłączyć komputer. Odpowiednio szybka właściwa reakcja użytkownika polegająca na wyłączeniu komputera na początku tego procesu może uchronić dane przed zaszyfrowaniem do nich dostępu (*Wirus Petya. Jak działa*…, 2017).

Dla użytkownika, który po raz pierwszy widzi ten komunikat to pozornie może to wyglądać jak typowy błąd systemu, z którym nie wiąże się zwykle ryzyko poważnych szkód w systemie operacyjnym Windows. Jeżeli zdezorientowany tym komunikatem użytkownik zainfekowanego komputera nie przerwie tego procesu to wówczas cel stworzenia tego wirusa Petya zostaje osiągnięty, ponieważ ten ransomware pracując w tle podczas wyświetlania wspomnianego komunikatu szyfruje pliki. Następnie po zakończonym procesie szyfrowania kluczowych dla prawidłowego działania systemu plików pojawia się kolejny

komunikat o już w pełni jednoznacznej treści: „Naciśnij dowolny klawisz!". Po wciśnięciu dowolnego klawisza, pojawia się kolejny komunikat z żądaniem okupu, z którego użytkownik komputera dowiaduje się, że jednak komputer został zawirusowany. Nawet jeżeli po tym komunikacie komputer zostanie zrestartowany to system operacyjny Windows się nie uruchomi a proces restartu zakończy się wyświetleniem tego samego komunikatu z żądaniem okupu za odblokowanie dostępu do plików.

Samodzielne odszyfrowanie plików przez użytkownika komputera, który nie jest informatykiem i specjalistą w zakresie hackingu jest w praktyce niemożliwe, ponieważ ransomware Petya stosuje wysoce zaawansowane algorytmamy szyfrujące RSA-4096 i AES-256, które stosowane są obecnie do przekazywania poprzez internet ściśle tajnych informacji z punktu widzenia bezpieczeństwa państwa, tj. wiadomości charakteryzujących się najwyższym priorytetem poufności jak np. tajnych, operacyjnych, strategicznych wiadomości przesyłanych przez narodowe siły militarne. Specjaliści od hakingu twierdzą, że tego typu kod szyfrujący jest w praktyce niemożliwy do złamania bez klucza deszyfrującego (Danes, 2016).

W sytuacji zaszyfrowania przez ransomware Petya dostępu do zawartych na dyskach danych wirus ten już jest głęboko ukryty w systemie, a wszelkie próby restartu komputera okazują się bezskuteczne ponieważ wirus ten dokonał już nadpisania plików uruchamiania systemu w tym tzw. Master Boot Record, który jest odpowiedzialny za prawidłowe załadowanie systemu operacyjnego. W związku z tym dopóki nie zostaną w komputerze przywrócone pierwotne ustawienia MBR, nie będzie możliwe usunięcie tego wirusa z komputera i odblokowanie zaszyfrowanych plików.

Jednak kolejną istotną specyfikacją tego ransomware Petya jest to, że nawet jeżeli udałoby się użytkownikowi dotrzeć do tych kodów systemowych i przywrócić pierwotne ustawienia systemowe MBR oraz usunąć wirusa z systemu, to jednak zaszyfrowane pliki z danymi na dyskach nadal pozostaną zablokowane. Pozbycie się wirusa z komputera oznaczać będzie usunięcie szkodliwego oprogramowania i jego w związku z tym jego dezaktywacje jednak nie rozszyfruje danych zawartych na dyskach, więc kluczowy problem nie

zostanie rozwiązany o ile te dane nie były wcześniej skopiowane na innych dyskach. Po usunięciu wirusa możliwe jest przywrócenie pełnej funkcjonalności komputera. W momencie pisania niniejszego artykułu pojawiły się już na rynku komercyjnego oprogramowania stosowne programy antywirusowe z pomocą których można usuwać wirusa Petya z zainfekowanego komputera.

Poza tym z przeprowadzonych przez analityków firmy Kaspersky badań, wynika, że istnieje jednak „szczepionka", tj. łata deaktywująca wirusa Petya. Aby stworzyć samodzielnie tę szczepionkę w notatniku należy stworzyć plik o nazwie perfc. Po stworzeniu tego pliku należy ten plik zapisać w katalogu systemowym C:\Windows i w jego właściwościach ustawić ten plik jako „tylko do odczytu" (*Wirus Petya zaatakował Polskę…*, 2017).

Na uwagę zasługuje także sam proces zarażenia systemu przez ransomware Petya. Proces tego zarażenia systemu może przebiegać w różny sposób co także dodatkowo zwiększa potencjalną zdolność szybkiego rozprzestrzeniania się wirusa poprzez internet i wewnętrzne sieci firmowe. Z jednej strony ransome Petya rozpowszechnia się w sposób klasyczny poprzez wiadomość emailowe. Z drugiej strony wirus ten także może być pobrany z portalu Dropbox jako plik „application folder-gepackt.exe". W takiej sytuacji wirus błyskawicznie aktywuje się już bezpośrednio po pobraniu i otwarciu pliku w danym komputerze. W związku z tym, że większość infekcji z zastosowaniem zarówno złośliwego oprogramowania ransomware jak i innych rodzajów wirusów dokonywana jest poprzez pocztę emaliową, to użytkownicy powinni zachowywać szczególną ostrożność przy korzystaniu z tego narzędzia komunikacji. Oznacza to przede wszystkim nie otwieranie maili nieznanego pochodzenia oraz ograniczone zaufanie wobec stosowanych przez usługodawcę mailowego filtrów antyspamowych i aplikacji antywirusowych, ponieważ użytkownik poczty mailowej zwykle nie posiada pełnej informacji na temat skuteczności tych narzędzi bezpieczeństwa (Prokopowicz, 2009, s. 65). Oprócz tego celem zwiększenia poziomu bezpieczeństwa korzystania z zasobów sieci internet każdy użytkownik powinien na bieżąco aktualizować oprogramowanie antywirusowe i cyklicznie wykonywać kopie zapasowe plików zawierających szczególnie istotne informacje.

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

Podsumowanie

Opisana w niniejszym artykule problematyka zagrożeń wynikających z cyberataku hakerskiego jaki został przeprowadzony 27 czerwca z użyciem wirusa ransomware Petya zapewne będzie jeszcze wnikliwie badana przez wydziały analityczne firm technologicznych i służb, których głównym celem jest zapewnienie bezpieczeństwa transferu danych w cyberprzestrzeni. Kluczową kwestią w kontekście skali rozprzestrzeniania się złośliwego oprogramowania jest sprawna i szybka reakcja mediów, w których podawane komunikaty ostrzegają obywateli o pojawiających się zagrożeniach. Kwestia ta dotyczy także odnotowanego z końcem czerwca 2017 roku ataku hakerskiego złośliwego oprogramowania typu ransomware Petya, za pomocą którego cyberprzestępcy blokowali działanie komputerów w wielu instytucjach publicznych, finansowych oraz firmach. Początkowo ten cyberatak dotyczył głównie instytucji i podmiotów funkcjonujących na Ukrainie jednak w kolejnych godzinach rozprzestrzeniania się wirusa Petya infekcje komputerów odnotowywane były także w nieco mniejszej skali w kilku innych krajach w Europie, w tym także w Polsce.

W zainfekowanym wirusem Petya komputerze wyświetlany był komunikat z żądaniem zapłacenia okupu 300 USD w bitcoinach po czym miało nastąpić przywrócenie prawidłowego działania zainfekowanego komputera. W obliczu narastających zagrożeń ataków hakerskich, w tym rozsyłania spamu zawierającego złośliwe oprogramowanie typu ransomware coraz więcej firm i banków tworzy dodatkowe zabezpieczenia systemów informatycznych i stale udoskonala pod tym względem wykorzystywane w prowadzonej działalności oprogramowanie i infrastrukturę informatyczną. W związku z odnotowywanym w ostatnich latach wzrostem aktywności w Internecie złośliwego oprogramowania ransomware sukcesywnie wzrasta znaczenie bezpieczeństwa elektronicznego przesyłania i przetwarzania danych za pośrednictwem globalnej sieci internet. Niezbędnym jest także stałe monitorowanie zagrożeń cyberprzestępczości i bezustanne doskonalenie instytucjonalnych rozwiązań systemowych przez służby odpowiedzialne za utrzymanie wysokiego poziomu bezpieczeństwa cybernetycznego (Gwoździewicz, Prokopowicz, 2015, s. 209).

Szczególnie istotna jest również rola mediów, do których powinny być na bieżąco przekazywane informacje mające szczególne znaczenie dla ostrzegania obywateli o pojawiających się zagrożeniach cyberataków w momencie zauważenia pierwszych przypadków niepokojących sytuacji związanych z internetem. Wirus Petya, który infekował komputery w końcu czerwca 2017 roku okazał się jednym z potencjalnie najgroźniejszych rodzajów wirusów ransomware. W związku z tym, że przy jego stworzeniu połączono technikę ransomware z ze znanymi od lat robakami, stworzono w ten sposób bardzo groźny rodzaj wirusa określanego jako ransomworm. Niezależnie od tego czy twórcom tego ransomworm zależało na wyłudzeniu dużej sumy pieniędzy od użytkowników zainfekowanych komputerów czy był to głównie cel polityczny destabilizacji działania instytucji państwowych Ukrainy to jednak potencjalne zagrożenia utraty zinformatyzowanych danych w działających w różnych krajach wielu instytucjach i firmach było wysokie. Jednak dzięki szybkiej reakcji mediów, w których nagłaśniano głównie poprzez media internetowe oraz TV przypadki odnotowywanych infekcji i zalecenia co należy zrobić aby zmniejszyć ryzyko infekcji to jednak nie doszło do globalnego cyberataku na wielką skalę. Tezę tą popierają także dane na temat wyłudzonych kwot pieniężnych z tytułu zablokowania komputerów przez poszczególne rodzaje wirusów ransomware odnotowane w okresie ostatnich kilku lat. Kwestię tę przedstawia poniższe zestawienie (*Globalne dochody bitcoin …*, 2017):

- wśród wirusów ransomware na uwagę zasługuje CryptoWall 2014, który pozwolił na wyłudzenie 325 milionów dolarów,
- przytoczony powyżej wirus WannaCry, z pomocą którego cyberprzestępcy przeprowadzili globalny cyberatak w maju 2017 roku, przyczynił się do wyłudzenia ponad 130 tys. dolarów,
- natomiast analizowany wirus Petya mimo również globalnego zasięgu przeprowadzonego ataku, to zgodnie z danymi opublikowanymi na portalu Blockchain.info na podany w żądaniu okupu adres 1Mz7153HMuxXTuR2R1t78mGSdzaAtNbBWX ofiary cyberataku wypłaciły już tylko 9 500 dolarów.

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

Dane te dotyczą cyberataku przeprowadzonego z użyciem wirusa Petya w dniach 27-28 czerwca 2017 roku i pochodzą z analizy przeprowadzonej 29 czerwca więc ta kwota 9, 5 tys. dolarów może jeszcze wzrosnąć, jednak jest to relatywnie niewielka kwota którą potencjalnie mogli pozyskać cyberprzestępcy z przeprowadzenia tego cyberataku biorąc pod uwagę jego globalny charakter, szybkość rozprzestrzeniania się w sieciach wewnętrznych firm i instytucji oraz wysoki poziom szkodliwości dla zainfekowanych w komputerach systemów operacyjnych. Za tę relatywnie niską skalę uzyskanych przez twórców wirusa Petya efektów finansowych względem potencjalnie wysokiej szkodliwości odpowiada szybka reakcja mediów, w których nagłośniono zagrożenia związane z przeprowadzanym atakiem. Pierwsze informacje na temat przeprowadzanego cyberataku pojawiły się już pod koniec dnia 27 czerwca, kiedy ten cyberatak rozpoczął się dopiero w niektórych krajach tj. na Ukrainie i w Rosji. Kolejnego dnia tj. 28 czerwca od samego rana w wiadomościach TV, radiowych i na wielu internetowych portalach informacyjnych informowano o przeprowadzonym cyberataku oraz o potencjalnym zagrożeniu jego kontynuacji w kolejnych krajach, w tym także w Polsce. W wiadomościach tych informowano użytkowników komputerów co należy zrobić, aby zmniejszyć ryzyko zainfekowania komputera. W związku z powyższym to szybkie, realizowane niemal w czasie rzeczywistym nagłośnienie problemu tego cyberataku w najbardziej powszechnych mediach znacząco przyczyniło się do ograniczenia skali szkód, które potencjalnie mogłyby być wywołane przez ten wirus ransomworm Petya.

Wobec powyższego kluczową kwestią bezpieczeństwa w cyberprzestrzeni i ochrony danych niejawnych oraz infrastruktury teleinformatycznej jest permanentne przeprowadzanie testów i diagnostyki funkcjonujących w danej instytucji systemów i aplikacji informatycznych. Problematyka ta jest szczególnie istotna w perspektywie dalszego dynamicznego rozwoju usług informacyjnych świadczonych za pośrednictwem sieci internet oraz dokonującego się procesu cyfryzacji firm i urzędów publicznych. Obowiązujące regulacje prawne powinny być na bieżąco nowelizowane (Gwoździewicz, Prokopowicz, 2016b, s. 397) celem bieżącego dostosowywania względem

dokonującego się bezustannie postępu w technologii teleinformatycznej wykorzystywanej przez firmy świadczące swe usługi za pośrednictwem globalnej sieci, w tym trudniące się budową baz danych niejawnych w technologii Big Data lub tworzące instrumenty automatyzujące procesy badania informacyjnych zasobów internetu (Gwoździewicz, Prokopowicz, 2016a, s. 232). Kolejną dziedziną wyznaczającą nowe kierunki postępu w zakresie technologii teleinformatycznej jest doskonalenie technik badania zasobów informacyjnych zwartych w wypowiedziach i komentarzach tysięcy bądź milionów użytkowników portali społecznościowych i innych witryn internetowych gromadzących komentarze użytkowników danych stron. Dotychczas jednak to cyberprzestępcy jako pierwsi odnajdywali luki w zabezpieczeniach systemów informatycznych i wykorzystywali je do przeprowadzenia ataków z użyciem złośliwego oprogramowania ransomware.

Dotychczas dominował model łatania luk w zabezpieczeniach przez zatrudnionych w firmach i bankach informatyków, które wcześniej zostały wykryte przez hakerów. Biorąc pod uwagę silny wzrost aktywności niebezpiecznych programów ransomware model ten powinien ulec zmianie polegającej na odwróceniu kolejności działań. To zatrudnieni w firmach, bankach i instytucjach publicznych informatycy powinni profilaktycznie przeprowadzać testy działania infrastruktury teleinformatycznej, doskonalić procedury i procesy zarządzania ryzykiem, podnosić poziom bezpieczeństwa wewnętrznych systemów informatycznych i podłączonych do internetu aplikacji, którymi zarządzają. Procesy te powinny być przeprowadzane na tyle sprawnie, aby luki w zabezpieczeniach były wykrywane odpowiednio wcześnie i jeszcze przed ich zauważeniem przez potencjalnych cyberprzestępców. W związku z tym obecnie wzrasta potrzeba prewencyjnego, profilaktycznego w swej istocie procesu doskonalenia procesów zarządzania ryzykiem systemów informatycznych funkcjonujących w instytucjach finansowych, przedsiębiorstwach oraz podmiotach sektora publicznego. Pod tym względem proces ten wzorowany może być na doskonaleniu zarządzania tradycyjnymi kategoriami ryzyka bankowego w instytucjach finansowych funkcjonujących

w Polsce od lat 90 (Prokopowicz, 2005, s. 98). W ostatnich latach rośnie presja rozwoju koncepcji zintegrowanego zarządzania ryzykiem (Prokopowicz, 2013, s. 37) w bankach, w tym także ryzyka systemów informatycznych.
Podsumowując, w kontekście coraz częściej pojawiających się tego typu ataków hakerskich szczególnie istotna jest rola mediów informujących w czasie rzeczywistym o kolejnych zagrożeniach wynikających z pojawiających się ataków hakerskich z zastosowaniem nowych odmian wirusów i technik włamywania się do systemów informatycznych przez cyberprzestępców. W kwestii roli mediów kluczowym jest informowanie o nowych zagrożeniach w czasie rzeczywistym dokonywania danego ataku z możliwie precyzyjnym wskazaniem czasu, miejsca, krajów, rodzajów komputerów, firm i instytucji zaatakowanych danym wirusem. Poza tym aby podnieść poziom bezpieczeństwa systemów informatycznych niezbędnym jest dokonywanie aktualizacji oprogramowania, w tym systemów operacyjnych oraz wykorzystywanych w firmach, instytucjach finansowych (Dmowski, Prokopowicz, 2010, s. 336) i publicznych poszczególnych aplikacji do nowszych, zwykle najnowszych wersji objętych supportem dostawcy. Poza tym zaleca się tworzenie backupów, kopii danych na zewnętrznych dyskach pozbawionych dostępu do sieci internet. W ten sposób ryzyko utraty danych w komputerach użytkowników oraz ryzyko systemów informatycznych funkcjonujących w instytucjach i podmiotach gospodarczych powinno zostać znacząco ograniczone. W związku z tym również ryzyko systemowe całego systemu finansowego oraz ewentualnej destabilizacji funkcjonowania całego Państwa w sytuacji pojawienia się nowych cyberataków będzie również znacząco mniejsze (Domańska-Szaruga, Prokopowicz, 2015, s. 39).

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

1.5. Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni"

Bezpieczna cyberpodprzestrzeń - wizja czy fikcja

Zawrotne tępo rozwoju technologii informatycznych wkracza mocno we wszystkie sfery życia prywatnego i publicznego wprowadzając nową jakość naszego funkcjonowania. Mechanizmem napędowym tego zjawiska są wciąż rosnące oczekiwania ze strony osób je wykorzystujących, np. przyzwyczajenie do inteligentnych gadżetów pozwalających na zdalne sterowanie różnymi przedmiotami. Czy ktoś z nas wyobraża sobie dzisiaj życie bez internetu? Telefony z nawigacją prowadzące do celu i na bieżąco modyfikujące tor przemieszczania się w zależności od miejsca położenia, tablety z „kopalnią wiedzy" pozyskiwaną za pomocą sieci lub inne urządzenia wydające na odległość polecenia sprzętom codziennego użytku lub kontrolujące stan mieszkań, to tylko kilka przykładów z całej gamy możliwości cyfrowego przekazu, jaką daje cyberprzestrzeń. Czym zatem jest ta cyberprzestrzeń?

Autorstwo tego wyrażenia przypisuje się Williamowi Gibsonowi, który po raz pierwszy użył je 33 lata temu w fantastyczno-naukowej (ang. *science fiction*) powieści *Neuromancer* (GIBSON W., tłum. CHOLEWA Piotr W.,2009) opublikowanej jako tom I tzw. *Trylogii Ciągu* (ang. *Sprawl Trilogy*). Początkowo nazywał ją matrycą (ang. *the matrix*), ale już wtedy kreślił wizjonerskie koncepcje sztucznej inteligencji, wirtualnej rzeczywistości i inżynierii genetycznej. Przyglądając się obecnie prowadzonemu dyskursowi na temat znaczenia tego pojęcia odkrywa się coraz większą głębie jego wydźwięku. Wydaje się, że każdy wie co to jest, ale przytaczane definicje są mocno uzależnione od potrzeb, na jakie zostały stworzone. Dla przykładu: Encyklopedia PWN określa cyberprzestrzeń, jako „*wirtualną przestrzeń, w której odbywa się komunikacja między komputerami połączonymi siecią Internetową*" (pojęcie: *cyberprzestrzeń* – http://encyklopedia.pwn.pl) zaś Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej definiuje ją, jako *„… przestrzeń przetwarzania i wymiany informacji tworzona przez systemy*

teleinformatyczne, określone w art. 3 pkt 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565, z późn. zm.) …" (http://www.cert.gov.pl).

Wspólnym i bezspornym elementem wszystkich tych definicji jest fakt, że cyberprzestrzeń jest przestrzenią (mat. pojęcie: *przestrzeń* – http://encyklopedia.pwn.pl). W potocznym tego słowa znaczeniu, można to rozumieć jako drugi, otaczający nas świat, który składa się ze specyficznych elementów i zachodzących między nimi relacji. Kluczowymi obiektami w tej przestrzeni są:

- sprzęt teleinformatyczny (ang. *hardware*) – komputery, okablowanie, urządzenia pośredniczące (np. switche, rutery), sieci teleinformatyczne;
- informacje, czyli dane gromadzone i przetwarzane na sprzęcie informatycznym oraz przesyłane za pomocą sieci teleinformatycznych;
- oprogramowanie (ang. *software*), które określa sposób gromadzenia, przechowywania i przetwarzania danych wraz z aplikacjami tworzącymi relacje pomiędzy nimi;
- człowiek, jako inicjator wszelkich zależności między nimi i pomysłodawca nowych technologii *hardwar*owych oraz *softwar*owych.

Pierwszy człon wyrazu „cyber" sugeruje powiązanie ze sterowaniem, kontrolą, a w potocznym tego słowa znaczeniu z informatyką (pojęcie: *Informatyka* – http://encyklopedia.pwn.pl), czyli dyscypliną naukową zajmującą się przetwarzaniem informacji [łac. *informatio* 'wyobrażenie', 'wizerunek', 'pomysł'] z użyciem komputerów. To od rozwoju tej dziedziny naukowej zależy, jakie obiekty będą przynależeć do tej cyfrowej przestrzeni i jakie relacje między nimi będą kreowane. Cały ten świat jest tworzony w celu gromadzenia oraz przetwarzania danych, przesyłanych niejednokrotnie po łączach sieciowych. Stąd często pojawia się skojarzenie cyberprzestrzeni z internetem.

Oczywistym jest, że kluczowym elementem tego obszaru jest informacja, i to ona musi być w należyty sposób chroniona. Zatem cały proces gromadzenia i przetwarzania danych musi być odpowiednio zabezpieczony przed możliwością ich zniszczenia lub zniekształcenia, a także skopiowania i kradzieży. Tylko gwarancja bezpiecznego transferu danych od nadawcy do odbiorcy może zapewnić ich integralności i wiarygodności.

1.5. Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni"

Z tych powodów ten cyberświat staje się kolejnym polem bitwy, na którym swoje siły mierzą ludzie go budujący („obrońcy") i osoby próbujące obalić ten porządek rzeczy („wrogowie"). Jednym z oręży używanych do ochrony informacji są polityki bezpieczeństwa, czyli zbiory zasad postępowania zapewniające nadzór nad zasobami cyberprzestrzeni. Jednak z pewnością szala zwycięstwa przechyliłaby się znacznie na korzyść „obrońców", gdyby stało się możliwym stworzenie wyizolowanego świata zwanego, **cyberpodprzestrzenią**. Należy ją rozumieć, jako nieograniczony, cybernetyczny podzbiór otwarty tylko dla danej społeczności i jednocześnie odizolowanego w stosunku do globalnej cyberprzestrzeni. Przestrzenie te mogłyby się wzajemnie zazębiać / przenikać, np. poprzez korzystanie z tych samych obiektów, ale w różny sposób tak, aby dane przetwarzane na potrzeby jednej grupy były chronione przed innymi.
Oczywiście nie ma jeszcze perfekcyjnych, cyberpodprzestrzeni, ale te które powstały zbliżają się do ideału. Obserwuje się niesamowity rozwój technologii tworzących coraz lepsze zapory fizyczne i programowe chroniące mniej lub bardziej skutecznie przed działaniami hackerskimi (ang. *hacker* – http://mkuliczkowski.pl/static/pdf/slownik.pdf, s. 49). Jednak wyniku tego wyścigu nie można przewidzieć z góry. Wydaje się, że najlepszym rozwiązaniem byłoby stworzenie takiej wydzielonej oraz wyizolowanej fizycznie cyberpodprzestrzeni, w której transmisja danych odbywałaby się w nowym typowym dla niej wymiarze, pozwalającym na skuteczną ochronę informacji przed wrogimi działaniami. Duże oczekiwania upatruje się w nowatorskich sposobach zarówno zapisu jak i przetwarzania informacji. Być może w przyszłości cyberświat zmieni swój wygląd, gdy nastanie era komputerów kwantowych, a może czekają nas kosmiczne sieci i bazy danych osadzone na bezawaryjnych serwerach postawionych w kosmicznej próżni. Jednak na dzień dzisiejszy wszystkie zabiegi informatyczne prowadzą do jak najlepszego, logicznego wyizolowania takich cyberpodprzestrzeni.

Policyjna cyberpodprzestrzeń

Policja jak każda instytucja, nie może funkcjonować we współczesnym świecie bez możliwości szybkiego i bezpiecznego przetwarzania informacji. W celu ochrony danych przetwarzanych na swoje potrzeby, dokonuje wszelkich starań

zmierzających do stworzenia własnej policyjnej cyberpodprzestrzeni. Musi ona być odseparowana od globalnego cyberświata, gdyż niesie on nie tylko profity, ale również zagrożenia.

Niewątpliwą wartością dodaną dla społeczeństwa jest rozwój rynku informatycznego w kierunku otwierania przed nim nowych możliwości edukacyjnych, wzajemnej komunikacji i wypoczynku, prowadzenia e-biznesów, promowania własnej wytwórczości i regulowania wszelkich zobowiązań. Sprzyja temu szeroka gama dostępnych urządzeń mobilnych pozwalających na zdalne zlecanie, wykonywanie i odbieranie projektów oraz wspieranie użytkowników na każdym etapie ich realizacji. Dzięki pozytywnym przekazom rośnie świadomość społeczna o poziomach życia w różnych krajach, oferowanych przez nich gwarantowanych świadczeniach socjalnych i ofertach pracy, prowadząc w prostej linii do zwiększonych ruchów migracyjnych na całym świecie. Niestety cyberprzestrzeń oprócz wymienionych powyżej zalet niesie ze sobą także coraz więcej zagrożeń. Począwszy od niebezpiecznych treści kierowanych dla określonych grup wiekowych lub społecznych, poprzez uzależnienia, zjawisko hejtu (pojęcie: *Hejt* – http://sjp.pwn.pl), cyberprzestępstwa, czyli działania godzące bezpośrednio w przetwarzaną informację (Kasprzak, Maj, Tarapata, 2015, s. 529), a także kradzieże tożsamości, informacji, pieniędzy, rekrutację do środowisk radykalnych, a skończywszy na cyberatakach (Piasecka, 2017, s. 47), również tych o charakterze militarnym lub cyberterroryzmie (Stojer-Polańska, 2015, s. 685-687).

Negatywne zjawiska spowodowały, że Policja powiększyła obszar swoich działań z otaczającej nas rzeczywistości do świata cybernetycznego. W celu ochrony bezpieczeństwa i porządku publicznego musi rozpoznawać, zapobiegać i wykrywać przestępstwa w obu domenach życia. Co więcej, skuteczność jej działania w dużej mierze zależy od bezpiecznego funkcjonowania zwłaszcza w tej drugiej, wirtualnej. Stąd bardzo istotne są jej dążenia do wydzielenia policyjnej cyberpodprzestrzeni niedostępnej dla osób postronnych i gwarantującej odpowiedni poziom ochrony przetwarzanych przez nią danych. Na dzień dzisiejszy jest to możliwe poprzez wdrażanie różnego rodzaju sprawdzonych rozwiązań *hardwarowych* i *softwarowych*, wprowadzanie

niezbędnych procedur i zasad postępowania z przetwarzaną informacją. Wyzwanie to jest tym większe, iż w przestrzeni tej pracuje wiele bazodanowych systemów informatycznych często współpracujących ze sobą, a także pozwalających na komunikację z innymi organizacjami pozapolicyjnymi.
Międzynarodowy charakter i skala zagrożeń dzisiejszych czasów stawia przed organami dbającym o bezpieczeństwo wymóg szybkiego reagowania na zjawiska niepożądane. Dlatego też obserwuje się coraz większą integrację i interoperacyjność[28] systemów informatycznych, powodując tym samym zwiększoną zwartość tej cyberpodprzestrzeni. Optymalizacja szybkości i szczelności łączy sieciowych oraz aplikacje o dużej przepustowości, to już niczym wyścig Formuły 1 w świecie cybernetycznym. Liczy się tutaj przede wszystkim krótki czas dostępu do przetwarzanych danych zabezpieczonych przed nieautoryzowanym dostępem.
W Polsce szkieletem nośnym policyjnej cyberpodprzestrzeń jest Policyjna Sieć Transmisji Danych (PSTD). Ochrona przetwarzanych informacji i bezpieczeństwo sieci[29] to największy priorytet jej sprawnego funkcjonowania. PSTD łączy się z innymi sieciami i udostępnia połączenia, ale na bardzo restrykcyjnych zasadach. Jednym z systemów funkcjonujących w tym obszarze jest automatyczny system identyfikacji daktyloskopijnej AFIS (Kot, Tomaszycki, 2015, s. 333). To na jego przykładzie pokazany zostanie rozwój policyjnej cyberpodprzestrzeni obserwowany w ostatnich latach, a zwłaszcza jej rozrastanie się w globalnej cyberprzestrzeni.

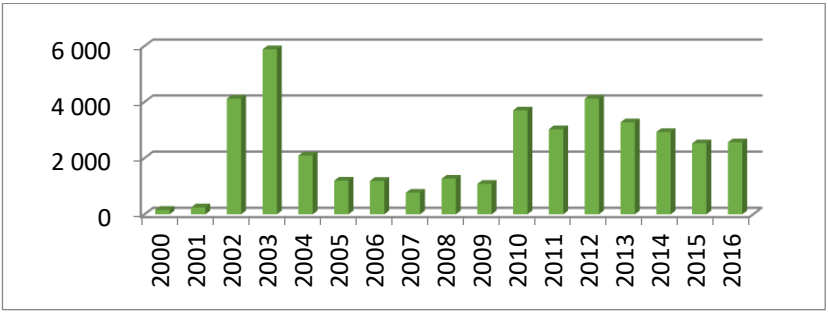
Wpływ AFIS na rozwój policyjnej cyberpodprzestrzeni

Pierwsza instalacja systemu AFIS (ang. *Automated Fingerprint Identification System*) w Polskiej Policji miała miejsce w 2000 roku. Przez cały okres jego funkcjonowania został on poddany wielu modernizacjom, tworząc w konsekwencji system rozproszony, ze zdalnymi klastrami zainstalowanymi na terenie całej Polski, pracującymi w architekturze klient-serwer. Początkowo był to tylko system centralny, ale już wówczas posiadał on budowę modułową pozwalającą na wdrażanie kolejnych rozwiązań, bez konieczności

[28] *ang. interoperability* - http://mkuliczkowski.pl/static/pdf/slownik.pdf, s. 56.
[29] *ang. network security* – http://mkuliczkowski.pl/static/pdf/slownik.pdf, s. 19.

zatrzymywania bieżącej jego pracy. Dwa lata później pozwoliło to na płynne wdrożenie osobnych klastrów systemowych z własną tymczasową bazą danych i zainstalowanie zdalnych stacji roboczych we wszystkich Laboratoriach Kryminalistycznych KWP/KSP. Od początku transmisja danych pomiędzy nimi odbywa się po dedykowanej policyjnej sieci PSTD, dając tym samym gwarancję nienaruszalności i integracyjności przetwarzanych danych daktyloskopijnych.
Pomimo, że technologie porównywania obrazów linii papilarnych nie były jeszcze tak zaawansowane jak obecnie, to już wówczas przynosiły wymierne efekty w identyfikacji sprawców. Rysunek 6. przedstawia liczbę śladów daktyloskopijnych wykrytych w drodze przeszukań ślad/karta (Hit), gdzie ślad oznacza obraz linii papilarnych palców lub dłoni zabezpieczonych na miejscu zdarzenia, zaś karta zestaw obrazów linii papilarnych palców pobranych od osoby (*ang. template* – wzorce odniesienia) i zapisanych w bazach danych.

Rysunek 6.Trafienie (HIT) dla przeszukań ślad/karta daktyloskopijna



Źródło: Opracowanie własne na podstawie danych z AFIS (rok, liczba Hit)

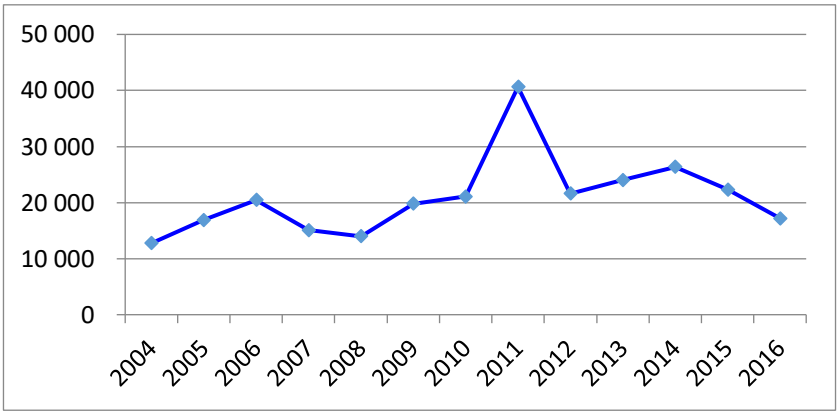
Co prawda w pierwszych latach wykrywczość nie była imponująca, gdyż uzależnione to było od rozmiaru bazy danych kart daktyloskopijnych. Na koniec 2000 r. liczyła ona zaledwie 1 013 137 kart, gdzie do końca 2003 r. liczba ta wzrosła do 1 929 581, a na koniec 2016 r. wynosiła już 3 873 939. Do roku 2003 dokonano identyfikacji większości zabezpieczonych śladów, dlatego w latach następnych obserwuje się już stały średni poziom wykrywczości. Nieznaczny przełom następuje w 2010 r., kiedy w systemie AFIS silnik porównywania obrazów daktyloskopijnych zostaje zmodernizowany

do najnowszego wówczas MetaMatcher'a wer. 4.0. Trwały przyrost kart daktyloskopijnych w połączeniu z tym zdarzenie wpływa na zwiększenie liczby pozytywnych identyfikacji śladów i ten wyższy poziom utrzymuje się do chwili obecnej. Takie rezultaty spowodowały, że od 2003 r. zaczęto sukcesywne instalować w kolejnych jednostkach policyjnych urządzenia do szybkiego ustalania lub potwierdzania tożsamości osób. Początkowo były to MorphoTouch'e (MT), a następnie MorphoRapId'y (MRiD) i czytniki L1 (Kot, Tomaszycki, 2015, s. 344), które komunikowały się bezpośrednio z jednostką centralną po sieci PSTD. Restrykcyjne wymogi bezpieczeństwa nie pozwoliły na wykorzystanie wszystkich ich możliwości. Ówczesny rynek informatyczny oferował technologie słabo zabezpieczające zdalną transmisje danych, dlatego zrezygnowano z komunikacji typu GSM/GPRS, Wi-Fi, czy Bluetooth. MT są urządzeniami stacjonarnymi i ich użytkowanie możliwe jest tylko w budynku. Mobilność MRiD polega na tym, że mają możliwość zbierania zeskanowanych obrazów linii papilarnych palców i zapisywania w lokalnej, zainstalowanej w urządzeniu bazie danych, a inicjalizowanie przeszukań następuje dopiero po dotarciu do jednostki Policji i podłączeniu się do komputera funkcjonującego w PSTD. Natomiast czytniki L1 służą tylko do skanowania opuszków palców i są podłączone do sprzętu posiadającego niezbędne oprogramowanie do ich obsługi, które gwarantuje bezpieczną transmisję danych. Na Rysunku 7. widać jak zmieniała się liczba potwierdzeń lub ustaleń tożsamości za pomocą tych urządzeń. W 2011 r. zauważalna jest znaczna tendencja wzrostowa. Na wynik ten wpłynęły dwa zdarzenia. Po pierwsze w roku poprzedzającym jednostki Policji zostały doposażone w 400 czytników L1. Dodatkowo zbiegło się to z zainstalowaniem nowej technologii porównywania danych daktyloskopijnych.

W tym samym czasie, co w Policji MT i MRiD instalowane były one również w Straży Granicznej. Zapytania z tych urządzeń również były wysyłane bezpośrednio do systemu AFIS, ale prze specjalny „punkt styku" z siecią PSTD. W ten sposób policyjna „cyberpodprzestrzeń" powiększyła się o kolejne obiekty, tym razem z obszaru pozapolicyjnego, ale zakres jej działania pozostawał jeszcze w granicach Polski.

1.5. Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni"

Rysunek 7.Potwierdzone tożsamości na urządzeniach MT, MRiD i L1



Źródło: Opracowanie własne na podstawie danych z AFIS (rok, liczba Hit)

1 maja 2004 r. kojarzony jest z kolejnymi zmianami w aplikacji AFIS, kiedy Polska przystępuje do Unii Europejskiej (UE). Wspólna unijna polityka azylowa, a tym samym wspólny europejski system azylowy nałożył na nasz kraj obowiązek połączenia się z Jednostką Centralną Eurodac (JC Eurodac – obecnie obowiązujący akt prawny: Rozporządzenie Parlamentu Europejskiego i Rady (UE) NR 603/2013 z dnia 26 czerwca 2013 r.). Podjęto decyzję, że połączenie to będzie realizowane „z i do" systemu AFIS. Zatem zainstalowano w nim nowe, niezbędne na te potrzeby funkcjonalności. Prace wdrożeniowe zaczęły się już wcześniej. W pierwszej kolejności wprowadzono do użytku urządzenia LiveScaner, a następnie pełnofunkcyjne stanowiska do rejestracji danych identyfikacyjnych osób (Kot, Tomaszycki, 2015, s. 345), które dawały możliwość wykonania elektronicznej karty daktyloskopijnej i szybką jej transmisję do AFIS po PSTD. Komunikacja ta odbywa się za pośrednictwem serwera FP (*FingerPrint*), nie tylko ze względów bezpieczeństwa, ale również z uwagi na konieczność prowadzenia kontroli jakości (formalnej i merytorycznej) przesyłanych danych. Następnie zaimplementowano w AFIS moduł Eurodac (Kot, Tomaszycki, 2015, s. 346-347) pozwalający na wymianę informacji z centralną bazą danych daktyloskopijnych Eurodac znajdującą się

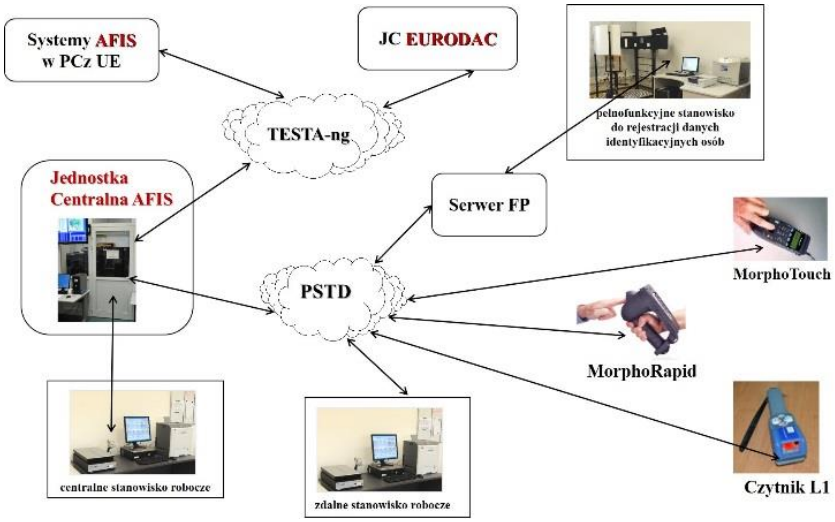
obecnie w Strasburgu (wówczas w Luksemburgu). Transmisja ta prowadzona jest po specjalnej sieci TESTA-ng (wtedy s-TESTA – bezpiecznej sieć ogólnoeuropejskich usług teleinformatycznych między organami administracji). Tym sposobem pierwszy dzień wejścia Polski do UE stał się kolejnym etapem rozwoju policyjnej cyberpodprzestrzeni, która tym razem zaczęła rozszerzać się poza fizyczne granice Polski.

Następny przełom datowany jest na roku 2015, gdy AFIS rozpoczyna automatyczną międzynarodową wymianę danych daktyloskopijnych z tego typu systemami umiejscowionymi w Państwach Członkowski Unii Europejskiej (PCz UE) w ramach tzw. Decyzji Pruem (Decyzja Rady 2008/615/WSiSW i 2008/616/WSiSW z dnia 23 czerwca 2008 r.) (Krzemińska, 2009, s. 198-213). Wymiana ta jest prowadzona między aplikacjami pracującymi w różnych środowiskach, o odmiennych konfiguracjach i zasadach gromadzenia danych, a jest możliwa dzięki wspólnemu uniwersalnemu plikowi wymiany (Krzemińska, 2008, s. 37). Oczywiście współpraca ta nie jest nawiązywana *ad hoc*, tylko połączenia z kolejnymi PC UE zestawianie są sukcesywnie, powodując tym samym postępujący rozrost policyjnej cyberpodprzestrzeni. Na dzień dzisiejszy w tym obszarze współpracujemy już z szesnastoma PC UE, a testy prowadzimy z kolejnymi trzema. Przewiduje się, że najpóźniej w 2018 r. działania te zostaną zakończone. Uzależnione to jest w dużej mierze od tempa przygotowywania do wymiany systemów AFIS w innych PC UE, gdyż niestety nie wszystkie posiadają zaimplementowane mechanizmy niezbędne do prowadzenia tej współpracy.

Architektura obecnego systemu AFIS została przedstawiona na Rysunku 8. Godnym uwagi jest połączenie z JC Eurodac. Odbywa się ono w topologii gwiazdy (*ang. star network*) oznaczając, że wszystkie systemy PC UE łączą się z jednym centralnym systemem. Komunikacja ta realizowana jest przez oddzielny serwer pocztowy dedykowany na te potrzeby. Międzynarodowa wymiana danych daktyloskopijnych w ramach Decyzji Pruem realizowana jest w topologii pełnej siatki (*ang. full mesh*), gdzie każdy system wymienia dane z każdym. Komunikacja ta jest prowadzona poprzez sieć TEST-ng, a pośredniczy w tym oddzielny serwer pocztowy przeznaczony do realizacji tego

rodzaju zapytań. Rozdzielenie tych połączeń było bardzo istotnym działaniem, gdyż w każdym z tych kanałów realizowany jest inny rodzaj kryptografii.

Rysunek 8.AFIS - Architektura



Źródło: Opracowanie własne na podstawie materiałów Zakładu Daktyloskopii CLKP.

System AFIS jest jednym z wielu funkcjonujących w policyjnej cyberpodprzestrzeni, ale już na jego przykładzie można zaobserwować jak zmieniała się ona w ostatnich 17 latach, coraz bardziej globalizując się, tym samym tworząc w Unii Europejskiej wspólną przestrzeń ochrony bezpieczeństwa i porządku publicznego. Widać również panującą tendencję do integracji i interoperacyjności systemów informatycznych w niej funkcjonujących, a wszystko w imię walki z terroryzmem oraz zwalczania przestępczości transgranicznej.

Zasady bezpieczeństwa stosowane w AFIS

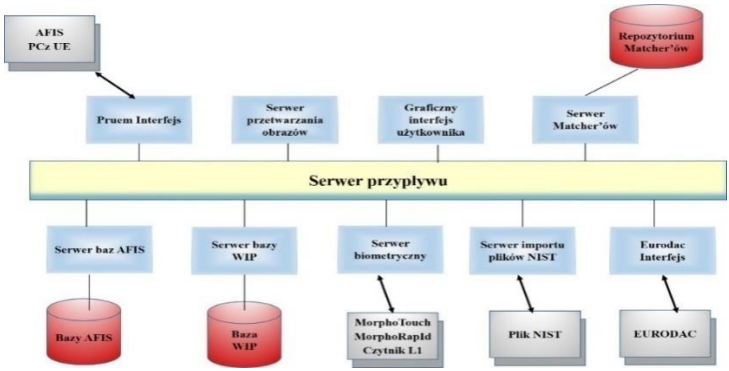
Umiejscowienie systemu AFIS w policyjnej cyberpodprzestrzeni spowodowało, że od samego początku jego funkcjonowania przyjęto restrykcyjne zasady gromadzenia, przechowywania, przetwarzania oraz transmisji danych

daktyloskopijnych. Pierwsze, podstawowe założenie dotyczy sposobu komunikacji wszystkich urządzeń współpracujących z systemem AFIS. Wszelkie połączenia z jego jednostką centralną odbywają się po wydzielonych zabezpieczonych sieciach (PSTD lub TESTA-ng) bez możliwości styku z publicznym internetem. Daje to większą gwarancję na ochronę przed kradzieżą danych, możliwością wprowadzenia zewnętrznych zakłóceń i zniekształcania przesyłanych informacji. W ramach tej komunikacji wymieniane są jedynie obrazy linii papilarnych wraz z oznaczeniami referencyjnymi, bez konkretnego wskazania na osobę. Jednemu zestawowi danych daktyloskopijnych pochodzących od określonej osoby przyporządkowany jest niepowtarzalny, unikatowy numer ID AFIS, który jest łącznikiem do danych osobowych gromadzonych w systemie KSIP (*Krajowy System Informacji Policyjnej*). Zaimplementowane mechanizmy kontrolujące jakość i integralność transmitowanych danych (Kasprzk, Maj, Tarapata, 2015, s. 528) zapobiegają zniszczeniu przekazywanych obrazów i danych referencyjnych, gwarantując tym samym ich nienaruszalność i odporność na manipulacje. W przypadku jakichkolwiek niezgodności status transportowanego rekordu zmienia się na błędny (*in-error*) i nie jest przetwarzany przez aplikację, aż do momentu ustalenia i wyjaśnienia przyczyny przez administratora systemu.

AFIS jest systemem skalowalnym, czyli posiada zdolność do sprawnego działania w warunkach rosnącej liczby użytkowników lub zwiększonej ilości przetwarzanych danych. Co prawda jest zaprojektowany na z góry określoną wydajność i zdolność przetwarzania danych. Przy zwiększonej w danym momencie ilości transakcji (ponad zaprojektowane limity) zadania są kolejkowane i wykonywane zgodnie z ich priorytetami. Dodatkowo, administrator systemu ma możliwość „ręcznego" sterowania kolejkami poprzez zmianę priorytetów przetwarzanych transakcji lub stopowanie wybranych usług (zwłaszcza tych spowalniających pracę). Taka możliwość ręcznego regulowania „ruchu" pozwala odciążyć mocno zajęte obszary systemowe i zaktywować te „śpiące", bez wpływu na stabilność pracy aplikacji.

1.5. Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni"

Rysunek 9.Jednostka Centralna AFIS



Źródło: Opracowanie własne Zakład Daktyloskopii CLKP.

Bezpieczeństwo danych to również bezawaryjna praca systemu, którą zapewnia jego modułowa budowa (patrz rysunek 9) oraz instalacja serwisów i usług systemowych na zestawie niezależnych maszyn wzajemnie współpracujących, połączonych w jedną, spójną logicznie całość. Dla użytkownika końcowego ta rozproszona architektura jest przezroczysta (ang. *transparency*) i postrzega on ją, jako jeden zintegrowany system. Dodatkowo niektóre kluczowe dla systemu moduły są redundantne, gwarantując tym samym ciągłość pracy aplikacji i dostęp do danych w przypadku awarii jednego z powielonych elementów (Tołpa, Protasiewicz, Kozłowski, Bułkszas, 2015, s. 549), a także ochronę przed cyberatakami. Dla przykładu serwer przepływu pokazany na Rysunku 7. składa się z trzech stacji Workflow. Każdy z tych stacji posiada własną konfigurację i indywidualne zabezpieczenia. Komputery te uzupełniają się wzajemnie. Kiedy jeden z nich ulega awarii, to zadania jego przejmują pozostałe dwa. Co prawda wykonują one zwiększoną ilość operacji, ale dla użytkownika końcowego nie ma to większego znaczenia, może jedynie zaobserwować nieznaczne spowolnienie pracy. Taka architektura sprawia też, że dużo sprawniej można wykonać modernizację systemu, czy nawet jego rozbudowę. Wymiana danego modułu na kolejny o większej sprawności może być przeprowadzona *on-line*, bez konieczności przerywania pracy użytkowników.

1.5. Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni”

AFIS to także system heterogeniczny (różnorodne systemy operacyjne). Bazy danych zainstalowane są na systemie AIX, zaś usługi porównujące i kodujące obrazy funkcjonują w środowisku Linux. Powszechnie uważa się, że właśnie takie system operacyjne gwarantują dużo wyższy poziom zabezpieczenia przed oprogramowaniem złośliwym (*ang. malware*, Maj, Tarapata, 2015, s. 531).

Interfejsy końcowe użytkownika udostępnione są na komputerach wyposażonych w system Windows i oprogramowanie Microsoft, czyli środowiska z rozwiniętą grafiką niezbędną do pracy z obrazami daktyloskopijnymi (do ich obróbki jakościowej i wizualizacyjnej). Stacje te wyposażone są w oprogramowanie antywirusowe z aktualizowanymi w czasie rzeczywistym centralnymi bibliotekami, umiejscowionymi na serwerze antywirusowym.

Niestety nawet najlepsze zabezpieczenia nie chronią w stu procentach przed możliwością utraty danych. Dlatego w AFIS wdrożono procedury archiwizacyjne. Wykonane kopie zapasowe zainstalowanych systemów operacyjnych aktualizowane są po każdej modyfikacji systemu. Codziennie wykonywane są pełne backupy wszystkich aktywnych baz danych (na poziomie level 0). Następnie kopiowane są one na taśmy w systemie cyklicznym, z okresem przechowywania jeden tydzień. W przypadku tzw. wypełnienia bazy jej status zmienia się na pasywny, zaś w jej miejsce aktywowana jest nowa. Bazę pasywną kopiuje się na taśmę, którą przekazuje się do archiwum. Raz w roku dokonuje się przeglądu taśm, połączonego z ich aktualizacją.

Prowadzona jest także stała obserwacja pracy systemu AFIS (ang. *monitoring system*) dzięki zaimplementowanym programom, które nie tylko wyświetlają na bieżąco stan usług i serwisów, ale również udostępniają wiele narzędzi niezbędnych do zarządzania nimi. Ponadto na każdym etapie obróbki informacji, zapisywana jest historia przetwarzanych transakcji, w tzw. plikach *trace,* generowanych dla wszystkich usług aplikacyjnych. System posiada również bazę logów, w której gromadzi się zapisy o tym, kto łączył się z aplikacją (użytkownik, urządzenie) i jakie wykonywał on czynności, a jakie system. Także zapisywane są wszystkie akcje podejmowane automatycznie przez system. Dzięki temu można prześledzić historię przetwarzania określonego rekordu począwszy od początku zaistnienia jego w systemie do czasu wykonania na nim

ostatniej operacji. Bez problemu można ustalić przyczynę odrzucenia danej transakcji (zarówno przez system jak i użytkownika). Innymi słowy w systemie zapisywane są wszystkie rezultaty z porównań, działania wykonane przez użytkownika i system oraz podejmowane decyzje na każdym etapie przetwarzania danego rekordu.

AFIS posiada mechanizmy autoryzacji i uwierzytelniania użytkowników[30] pozwalające na kontrolę dostępu do określonych obszarów systemu. Oznacza to, że nawet biegły z dziedziny daktyloskopii nie może zalogować się do systemu, jeśli nie posiada stosownych uprawnień. Musi on wcześniej poddać się niezbędnym szkoleniom i zdać egzamin kwalifikacyjny. Odbywa się to wieloetapowo i jest ściśle związane z przypisaną jemu rolą. Odmienne szkolenia przechodzą osoby wprowadzające dane z kart daktyloskopijnych, a inne biegli pracujący ze śladami linii papilarnych. Po zdanym egzaminie poszczególni użytkownicy uzyskują dostęp tylko do z góry określonych funkcji i zakresu danych, zgodnych z ich kwalifikacjami. Dodatkowym ograniczeniem jest brak możliwości zalogowania się osoby z innej stacji roboczej, niż została jej przypisana (zgodnej z miejscem zatrudnienia). Oznacza to, że np. biegły posiadający uprawnienia do pracy z systemem AFIS w Szczecinie, nie tylko nie będzie mógł wykonywać tych samych czynności na stanowiskach centralnych lub w innym województwie, ale nawet nie będzie mógł się zalogować z nich do systemu.

Zbiory danych daktyloskopijnych chronione są także w sposób fizyczny. Pokoje, w których wprowadza się, przetwarza i gromadzi te dane przynależą do różnych stref dostępu. Każdy z pracowników posiada indywidualną kartę dostępową, która pozwala na dostęp do pomieszczeń zgodnie z posiadanymi uprawnieniami. Na bieżąco prowadzona jest kontrola wejść i wyjść (ang. *access control*) oraz przebywania poszczególnych osób we wszystkich nadzorowanych obszarach, dzięki specjalnym czytnikom zainstalowanym na drzwiach wejściowych. Zapewnione zostały także optymalne warunki pracy dla sprzętu elektronicznego począwszy od instalacji klimatyzacji, poprzez zapewnienie gwarantowanego zasilania awaryjnego.

[30] *ang. identification* – http://mkuliczkowski.pl/static/pdf/slownik.pdf, s. 51.

Podsumowanie

W dzisiejszym świecie mało kto potrafi żyć bez urządzeń korzystających z cyfrowego przekazu. Cyberprzestrzeń, to drugi świat, równoległy do tego rzeczywistego. Któż nie zna powiedzenia: „*Jeśli nie ma cię w sieci, to nie istniejesz*"? Z pewnością jest to nieliczne grono osób, które nie zaznało w życiu przyjemności korzystania z komputera i możliwości komunikowania się ze światem, zwłaszcza tym wirtualnym. Co więcej do tych osób nie można z założenia zaliczyć żadnej z grup społecznych, gdyż nawet osoby, które swoje pierwsze kroki w tej dziedzinie stawiały będąc już np. w wieku starszym, uzależniają się od tych technologii.

Jednak cyberświat, to nie tylko same zalety, ale również liczne zagrożenia, których zwalczaniem zajmuje się Policja. Aby móc sprawnie realizować powierzone jej zadania w obu obszarach (rzeczywistym i cybernetycznym), buduje ona swoją własną policyjną cyberpodprzestrzeń, czyli wyizolowaną strefę, w której gromadzi i przetwarza dane pozostające w jej zainteresowaniu. Skuteczność jej działania zależy w dużej mierze od zapewnienia bezpieczeństwa wykorzystywanej infrastruktury teleinformatycznej, a także od zdolności do zapobiegania i zwalczania zagrożeń ze strony globalnej cyberprzestrzeni (Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej, str. 6-7). Wyzwanie to jest tym większe, że powstające zasoby bazodanowe stale się rozrastają, powstają nowe aplikacje i przybywa urządzeń z nimi współpracujących, komunikując się niejednokrotnie po sieciach rozległych.

Do wymienionych systemów informatycznych w niej funkcjonujących zalicza się Automatyczny System Identyfikacji Daktyloskopijnej (AFIS). Dynamiczny rozwój technologii gromadzenia danych daktyloskopijnych pozwalających na bezpieczne ich przetwarzanie oraz nowe wyzwania stawiane tej aplikacji spowodowały, że poddawana była on wielokrotnym modernizacjom. Do kamieni milowych jej rozwoju można zaliczyć instalację zdalnych stanowisk roboczych, podłączenie urządzeń do ustalania i potwierdzania tożsamości osób, podłączenie do JC Eurodac oraz podjęcie automatycznej międzynarodowej wymiany danych daktyloskopijnych z PC UE. Każdy z tych etapów wpłynął bezpośrednio na logistyczne rozrastanie się policyjnej cyberpodprzestrzeni. W efekcie

końcowym można powiedzieć, że wyszła ona poza granice Polski i rozprzestrzeniła się na niemal całą Unię Europejską. Wszystkie te działania prowadzone są w kierunku lepszej integracji i interoperacyjności z innymi systemami funkcjonującymi w UE w celu zapobiegania i zwalczania terroryzmu oraz przestępczości transgranicznej.

Podsumowując, na przykładzie systemu AFIS został pokazany dynamiczny rozwój policyjnej cyberpodprzestrzeni. Zaprezentowano również sposoby ochrony informacji w niej przetwarzanych. Należy jednak podkreślić, że kluczowym obiektem funkcjonującym w tej przestrzeni jest człowiek, i to od jego dyscypliny zależy czy będzie ona spełniać swoje zadanie, a dane w niej przetwarzane będą należycie chronione.

1.6. Outsourcing cyberbezpieczeństwa w świetle problematyki współczesnych zagrożeń w cyberprzestrzeni

Wstęp

Sieci komputerowe i telekomunikacyjne, w szczególności sieć internet, stały się nieodłącznym elementem codzienności. Wg danych Głównego Urzędu Statystycznego (GUS, 2016, s. 1), dostęp do internetu w 2016 r. posiadało 80,4% gospodarstw domowych oraz 93,7% przedsiębiorstw. Z usług e-administracji korzystało 30,2% osób w wieku 16-74 lat, a 67% przedsiębiorstw posiadało własne strony internetowe. Pole zastosowań Internetu jest oczywiście znacznie szersze:

- wymiana informacji – z portali społecznościowych korzysta w Polsce 14 mln aktywnych użytkowników (Gwóźdź 2016), większość użytkowników internetu posiada przynajmniej jedną skrzynkę e-mail,
- korzystanie z rozrywki elektronicznej i usług multimedialnych na żądanie,
- zarządzanie finansami – w Polsce jest ponad 31 mln internetowych kont bankowych (Boczoń, 2017),
- zakupy internetowe,
- dostęp do informacji,
- kreowanie wizerunku.

Internet stał się narzędziem komunikacyjnym do realizacji biznesu, jak również kreowania nowych usług biznesowych (w chmurze), które z założenia powinny być otwarte, powszechne i łatwe w użyciu. Nie ułatwia to tym samym ich zabezpieczenia. Nasycenie rynku usługami telekomunikacyjnymi powoduje, że z zaawansowanych technologii korzystają osoby z minimalnym przygotowaniem informatycznym. Zmienia się też spektrum wiekowe użytkowników – wzrasta odsetek dzieci i niepełnoletniej młodzieży, która to grupa osób powinna być szczególnie chroniona, także przed samym dostępem do niektórych treści.

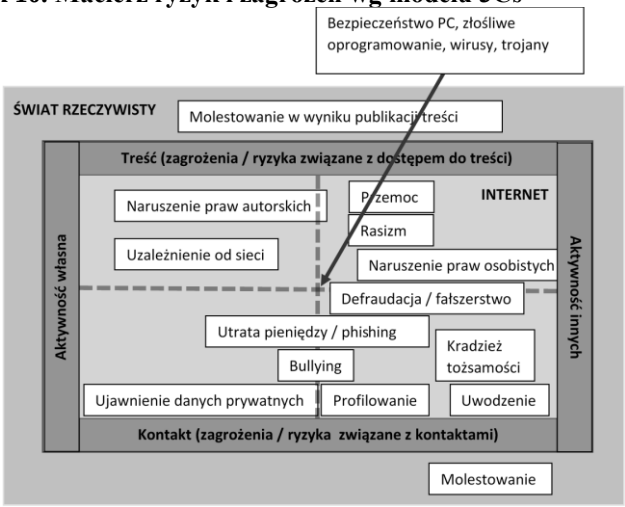
Zagrożenia w cyberprzestrzeni możemy w uproszczeniu podzielić na te związane z zakłóceniami pracy systemów składowych cyberprzestrzeni (infrastruktury),

w tym infrastruktury krytycznej, oraz powiązane z kontaktami nawiązywanymi w sieci. Warto podkreślić rosnące sprzężenie cyberprzestrzeni ze światem rzeczywistym – akcje podejmowane w przestrzeni wirtualnej mają często wymierne efekty w faktycznym otoczeniu.

Etiologia zagrożeń w cyberprzestrzeni

W ramach projektu "EU Kids Online" podjęto próbę systematyzacji aspektów związanych z analizą ryzyk oraz zagrożeń związanych z aktywnością dzieci w Internecie i w efekcie zaproponowano w 2007 roku model tzw. 3Cs – od angielskich słów *content, contact* oraz *conduct* (Hasebrink et al. 2009)**Błąd! ie można odnaleźć źródła odwołania.**. Kluczowym elementem modelu jest rozpoznanie trzech podstawowych aktywności dzieci w Internecie: konsumpcji treści (*content*), nawiązywania kontaktów nieinicjowanych bezpośrednio przez dziecko (*contact*), inicjowania relacji (*conduct*). Model został spopularyzowany w: (Byron 2008) i zaprezentowany w zmodyfikowanej formie, jako macierz zagrożeń, w: (Berson 2010). Jest na tyle uniwersalny, że z powodzeniem można go zastosować również do klasyfikacji szerszego spektrum e-zagrożeń.

Rysunek 10. Macierz ryzyk i zagrożeń wg modelu 3Cs



Źródło: Berson, I., Berson, M.,J., eds. "High-tech tots: Childhood in a digital world". IAP, 2010

Rysunek 1010 ilustruje wybrane przykłady zagrożeń występujących w internecie. Odległość od czynnika ryzyka (Treści, Kontaktu, Aktywności) określa znaczenie elementu dla danego typu zagrożenia. Publikując treści w Internecie, narażamy się dla przykładu na ryzyko ujawnienia danych prywatnych (np. adresu), co może doprowadzić do stania się ofiarą przestępstwa w świecie rzeczywistym.

Podstawowym powodem działalności cyberprzestępców jest chęć zysku. Tego rodzaju motywacja występuje w przypadku 64,5% znanych ataków. Do tego dodać należy 22,4% przypadków szpiegostwa przemysłowego, 5,3% - wojen cybernetycznych i tylko 7,9% tzw. aktywizmu (Passeri, 2017). W przypadku ataków wymierzonych w użytkowników najczęstsze powody to chęć zaspokojenia dewiacji seksualnych, skłonność do przemocy, chęć wyładowania agresji, żalu czy frustracji ze świata rzeczywistego.

Internet (często pozornie) kojarzy się z anonimowością, przez co w wirtualnym świecie ludzie często dokonują aktów, których w normalnych okolicznościach by się nie podjęli z obawy przed konsekwencjami. Częstym działaniem jest krytyka osób publicznych lub znajomych w mało parlamentarny sposób, niejednokrotnie formułuje się groźby karalne. Część młodzieży wykorzystuje media komunikacyjne do wyrządzania szkód emocjonalnych poprzez różne formy nękania (*cyberbullying)*, czy nawoływania do samobójstw. Pedofile, udając osoby nieletnie, poszukują ofiar i za pomocą manipulacji nakłaniają do czynności o naturze seksualnej.

Główne cyberataki jako zagrożenia dla funkcjonowania cyberprzestrzeni

Obecnie jednym z największych zagrożeń dla cyberprzestrzeni są wolumetryczne ataki DDoS (Distributed Denial of Service). Całkowite sparaliżowanie funkcjonowania internetu nie leży w niczyim interesie – sieć jest dla cyberprzestępców narzędziem pracy, dla służb źródłem informacji, dla terrorystów – narzędziem szybkiej komunikacji i werbunku. Należy się zatem spodziewać raczej ataków ukierunkowanych na konkretnych operatorów sieci, usługodawców lub dostarczycieli treści. Niemniej produktem ubocznym takich celowanych ataków mogą być zaburzenia funkcjonowania całej sieci – *vide* atak

DDoS wymierzony *w Spamhaus* (Arthur, 2013). Infrastrukturę do ataku DDoS można kupić na czarnym rynku już od 5 USD za godzinę (Incapsula.com).
W przypadku cyberwojny najbardziej prawdopodobne są ataki zmierzające do zakłócenia funkcjonowania elementów sterowania infrastrukturą krytyczną, np. systemów SCADA (*Supervisory Control And Data Acquisition*). Nie wszystkie takie systemy posiadają punkty styku z internetem, ale jak pokazał przykład Stuxneta (atakującego irańskie instalacje nuklearne), nawet one są zagrożone, jeśli można podłączyć do nich nośniki zewnętrzne.
Masowo występują względnie mniej groźne ataki, zmierzające do przełamania zabezpieczeń sieci korporacyjnych, publicznie dostępnych serwisów internetowych i serwerów. W ich przypadku wykorzystuje się metody typu *brute force* lub bardziej wysublimowane, także wykorzystujące nieznane powszechnie podatności w aplikacjach i systemach (*0-day exploits*).

Problemy zarządzania cyberbezpieczeństwem
Nie można mówić o szczegółowym modelu zarządzania cyberbezpieczeństwem optymalnym dla wszystkich organizacji. Zależy on od wielu czynników (struktura i status prawny organizacji, jej wielkość, koszt posiadanych aktywów, specyfika infrastruktury IT czy możliwość utworzenia własnej komórki ds. cyberbezpieczeństwa). Sektor publiczny boryka się tu ze specyficznymi problemami. Przetwarza newralgiczne dane osobowe i często dane wrażliwe, a jego zakres odpowiedzialności jest bardzo szeroki. Przy tym cechuje się brakami w standaryzacji, długim czasem oczekiwania na modernizację rozwiązań IT i niekiedy niewystarczającym poziomem świadomości, przejawiającym się np. w braku niezbędnych aktualizacji oprogramowania (Waszczuk, 2015, s. 48).
Jednym z najbardziej istotnych czynników mających wpływ na poziom zabezpieczeń przed cyberatakami jest brak na rynku wystarczającej liczby specjalistów. W Polsce brakuje ok. 50 tysięcy wykwalifikowanych specjalistów IT, a w Unii Europejskiej – ok. 270 tysięcy, przy czym do roku 2020 liczba ta wzrośnie do 800 tys. – 1 mln. specjalistów (Wolany 2016). Przy tym polski rynek w obszarze zabezpieczeń IT rozwija się dwukrotnie szybciej (7% rocznie) niż cały sektor – 3-4% rocznie (Teamquest.pl 2016). Powoduje to, że problem

braku specjalistów bezpieczeństwa staje się jeszcze bardziej palący, a koszt pracy tych, którzy na rynku już są obecni – zwiększy się.
Częściowym rozwiązaniem tego problemu jest użycie zaawansowanych systemów bezpieczeństwa, które – właściwie dobrane i zarządzane – mogą ograniczyć nakład pracy niezbędnej do utrzymania bezpieczeństwa systemów ICT na pożądanym poziomie. Innym wyjściem, zwłaszcza dla instytucji, które nie są w stanie utworzyć dedykowanej komórki bezpieczeństwa IT, może być zastosowanie w tym zakresie modelu outsourcingowego.

Ekonomia bezpieczeństwa IT
Oczekiwany zysk napastnika zależy od przychodu z ataku. Pełne dane karty kredytowej obywatela UE warte są na czarnym rynku ok. 45 USD, a dostęp do konta płatności online – ok. 5-10% wysokości zgromadzonych środków (McFarland et al. 2015, s. 6-8). Z kolei przeciętny koszt stania się ofiarą cyberataku dla małych przedsiębiorstw w USA to 38 tys. USD, a dla dużych firm 551 tys. USD (Kaspersky Lab 2015, s. 2). Ponemon Institute szacuje, że ataki phishingowe kosztują firmę zatrudniającą 10 tys. osób średnio 4 mln USD rocznie (Balley 2016).
Z drugiej strony, cyberprzestępca ponosi określone koszty, planując i przeprowadzając atak. Jeżeli uda się odpowiednio je podwyższyć, istnieje szansa, że napastnik zrezygnuje. Koszt ataku można podnieść np. poprzez wdrożenie ulepszonego oprogramowania. Napastnicy nie mogą już wtedy korzystać z dotychczasowych technik i muszą, często przez długi czas, wynajdywać nowe (Miller et al. 2011, s. 4). Innym rozwiązaniem jest wdrożenie dedykowanego systemu zabezpieczeń, potrafiącego radzić sobie z większością znanych ataków. W praktyce należy dostosować koszt zabezpieczeń do wartości aktywów.

Strategia ochrony w głąb
Strategia ochrony w głąb (ang. *defence in-depth*) minimalizuje ryzyko za pomocą zróżnicowanych strategii ochronnych, tak aby po przełamaniu części zabezpieczeń pozostałe nadal chroniły system i dane (Viega et al. 2002, s. 96-97). Wydłuża to czas ataku, a więc podwyższa jego koszt. Strategia nie obejmuje przy

tym tylko logicznych poziomów infrastruktury IT (komputer osobisty, aplikacja, serwer, sieć), ale także polityki, procedury i wreszcie świadomość użytkowników. Szczegółowy dobór niezbędnych rozwiązań i sposób ich wdrożenia zależy, jak wiemy, od specyfiki organizacji. Poniżej krótko opiszemy jedynie przykładowe rozwiązanie – firewall nowej generacji.

Warstwa zabezpieczeń technicznych

Różnorodność infrastruktur teleinformatycznych i możliwych technik ataków uniemożliwia zabezpieczenie systemów za pomocą jednego idealnego rozwiązania. Powoduje też, że ręczna praca administratora bezpieczeństwa jest skrajnie nieefektywna. Nieodzowne jest zatem użycie zestawu rozwiązań sprzętowych i programowych służących do ochrony aktywów IT.

Jeżeli wszystkie takie rozwiązania pochodzą od różnych dostawców, mocno utrudnia to zarządzanie bezpieczeństwem – należy choćby poświęcić dodatkowy czas na integrację poszczególnych rozwiązań. Z tej perspektywy pojedyncze rozwiązanie, które jednak potrafi wykonywać różne zadania, ułatwi ochronę przynajmniej na jednej warstwie w rozumieniu strategii ochrony w głąb.

Idea firewalla nowej generacji (ang. *Next Generation FireWall* – NGFW) nie jest nowa. Już w 2009 r. zespół badawczy Gartnera określił takie urządzenie jako niezbędny wynik ewolucji idei firewalla, reagującej na zmiany zarówno w sposobach, w jaki procesy biznesowe korzystają z usług IT, jak i w metodologiach ataków (Pescatore et al., 2009). Ideą NGFW jest możliwość zaawansowanej kontroli ruchu sieciowego na podstawie głębokiej analizy pakietów, a więc sprawdzania także tego, co w tym ruchu tak naprawdę jest przesyłane. Ponadto najczęściej proponowane funkcje bezpieczeństwa NGFW to: system IDS/IPS (ang. *Intrusion Detection/Prevention System*), filtrowanie treści, antyspam, rozpoznawanie złośliwego oprogramowania (antymalware), tworzenia sieci VPN (*Virtual Private Network*) i kształtowanie ruchu (*traffic shaping*) (Abdel-Aziz et al. 2009, s.6-7).

Realizując projekt MAN-HA „Realizacja w MAN-ach usług krytycznych o wysokim poziomie niezawodności”[31] w zakresie wdrożenia w 20 polskich

[31]http://man-ha.pionier.net.pl/pl/

jednostkach MAN[32] zaawansowanych rozwiązań NGFW, przekonaliśmy się, jak różne są wymagania organizacji nawet o podobnym profilu. Nie można więc podać ogólnej recepty na idealny NGFW. Dobierając urządzenie, należy uwzględnić cenę, pozycję w rankingach czy ogólną opinią, ale przede wszystkim przeprowadzić analizę możliwości względem pożądanych funkcji i wpasować je w ogólną koncepcję przyjętego modelu bezpieczeństwa. Bazując na rezultatach prac, chcielibyśmy przekazać kilka wskazówek, mogących pomóc w doborze sprzętu. Oprzemy się głównie na podanej wyżej liście funkcjonalności:

- system wykrywania włamań (IDS/IPS) jest cennym narzędziem w zabezpieczaniu infrastruktury. Może działać tylko na zasadzie sygnaturowej lub mieć moduł behawioralny i wykrywać anomalie. Tylko drugie podejście umożliwi detekcję nowych, nieznanych zagrożeń.
- Podobną charakterystykę ma moduł antymalware. Najlepiej, jeżeli jest wyposażony w tzw. mechanizm „sandbox" (piaskownicę), odizolowane od reszty systemu środowisko, symulujące prawdziwy komputer, w którym bada się zachowanie podejrzanego oprogramowania
- system antywirusowy – niemogący zastąpić systemów tradycyjnie działających na klientach, lecz uzupełniający je i wspierający jako dodatkowy mechanizm filtracji, wkomponowujący się w ideę ochrony w głąb
- mechanizm filtrowania treści, szczególnie przydatny tam, gdzie dostęp do pewnych stron WWW dla celów służbowych jest niezbędny. Bazując na listach reputacyjnych, a także na samodzielnie zdefiniowanych zbiorach stron złośliwych i zaufanych, administrator może dostosować politykę ruchu www do zapotrzebowania organizacji
- moduł antyspamowy proponujemy osobno zintegrować z serwerem poczty elektronicznej, oszczędzając cenne zasoby NGFW
- VPN – moduł umożliwiający tworzenie bezpiecznych, szyfrowanych kanałów komunikacyjnych na zewnątrz i do wewnątrz organizacji. Należy

[32] MAN –Metropolitan Area Network – sieć miejska; jednostki MAN oznaczają operatorów ww. sieci – por. http://www.pionier.net.pl/online/pl/jednostki/

zwrócić uwagę na zestaw obsługiwanych protokołów oraz algorytmów szyfrujących
- kształtowanie ruchu – pozwala na definicję polityki przetwarzania ruchu sieciowego zgodnie ze zdefiniowanymi priorytetami i ograniczeniami dla poszczególnych, mniej lub bardziej krytycznych, usług

Aktywując poszczególne funkcje systemu NGFW (często wymagających dodatkowych licencji), trzeba pamiętać, że każda z nich zużywa zasoby urządzenia. Producenci rozwiązań zwykle podają wartości parametrów (liczba obsługiwanych sesji, przepustowość itp.) przy braku uaktywnienia pełnego zestawu funkcji. Po ich włączeniu parametry mogą ulec pogorszeniu nawet o kilka rzędów wielkości.

Inną istotną kategorią rozwiązań bezpieczeństwa mogą stać się systemy wykrywania włamań oparte na detekcji anomalii. Są na razie jedyną, choć niepełną, odpowiedzią na zaawansowane ataki ukierunkowane (*Advanced Persistent Threats*), oparte na wykorzystaniu nieznanych publicznie podatności (zatem nie istnieją dla nich sygnatury). Wykrycie takiego ataku wymaga zdolności detekcji zachowania anomalnego, wdrożenia mechanizmu korelacji informacji z wielu systemów, możliwości zidentyfikowania zagrożenia i wdrożenia odpowiedniej reakcji (Kliarsky et al. 2011, s. 7-8). W dużej organizacji wąskim gardłem jest liczba zdarzeń do przechowania i przetworzenia, niekiedy rzędu miliardów, a nawet bilionów dziennie (Bhatt et al. 2014, s.35-41). Tworzone są prototypowe systemy, oparte na algorytmach uczenia maszynowego, stosujące podejście CEP (ang. *Complex Event Processing* – zaawansowane przetwarzanie zdarzeń), umożliwiające składowanie i przetwarzanie tylko istotnej części informacji o zdarzeniach (Frankowski et al. 2015, s. 351-372). Systemy takie, po odpowiednim wdrożeniu i skonfigurowaniu, mogą być cennym uzupełnieniem zestawu „obowiązkowych" zabezpieczeń.

Warstwa prawno-organizacyjna

Ramy działalności organizacji wyznaczają również ogólne i branżowe regulacje prawne. Do ustaw, które obowiązują wszystkie organizacje bez wyjątku, należy Ustawa o Ochronie Danych Osobowych z dn. 29 sierpnia 1997. W tym kontekście przywołać należy gruntowne zmiany, jakie wejdą w życie 25 maja

2018 r. (tzw. RODO). Instytucje publiczne muszą osiągnąć (i regularnie weryfikować) zgodność z Krajowymi Ramami Interoperacyjności a przykładem regulacji branżowych dla sektora finansowego są: Ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe czy tzw. rekomendacja D Komisji Nadzoru Finansowego, bezpośrednio związana z obszarem bezpieczeństwa teleinformatycznego.

Poza koniecznością wypełniania obowiązków wynikających z przepisów prawa, należy wspomnieć, że co do zasady zabezpieczenia techniczne muszą współgrać z organizacyjnymi. Same polityki i procedury, pozostaną tylko zestawem dokumentów. Z kolei tylko wdrożenie zabezpieczeń, niepoparte otoczeniem proceduralnym, szybko zdezaktualizuje się, a jeśli wiedza o zarządzaniu zabezpieczeniami znajduje się tylko w głowie administratorów, spowoduje to poważny problem w przypadku zmiany ich miejsca zatrudnienia.

Outsourcing w centrach zarządzania bezpieczeństwem

Bezpieczeństwo IT stało się pierwszoplanowym aspektem działania każdej większej organizacji. Inwestuję one często w rozwój własnych centrów zarządzania bezpieczeństwem (*SOC, Security Operations Center*). Celem działania SOC jest zapewnienie zwiększonego poziomu bezpieczeństwa i gwarancja szybkiej obsługi incydentów (zdarzeń) bezpieczeństwa, jakie zostaną wykryte w sieci organizacji (McAfee 2015, s. 3).

Niestety, założenie SOC jest bardzo ambitnym zadaniem. Wymaga pracy planistycznej, opracowania szeregu procedur, inwestycji w zakup, konfigurację i utrzymanie specjalizowanego oprogramowania oraz zapewnienia odpowiedniej liczby specjalistów. Organizacja ENISA ocenia, że działające w pełnym trybie ciągłym SOC wymaga zatrudnienia 12 specjalistów (ENISA 2006, s. 24). Nie każda organizacja, która SOC-a potrzebuje, jest w stanie tego rodzaju zasoby zapewnić.

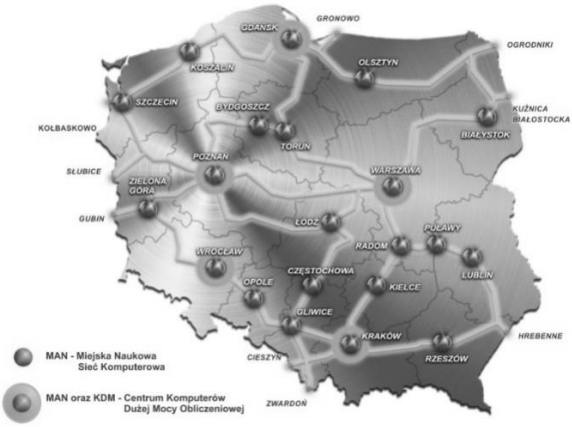
Norma ISO 31000:2009, stanowiąca jeden ze standardów zarządzania ryzykiem, zawiera zbiór ogólnych metod w zakresie postępowania z ryzykiem. Jedną z nich jest podzielenie się ryzykiem z inną organizacją (Purdy, 2010, s. 881-886). W przypadku cyberbezpieczeństwa oznacza to oddanie części lub całości zarządzania nim w outsourcing, co pozwoli na zapewnienie wyższego poziomu

bezpieczeństwa IT, często przy niższych kosztach i własnym wysiłku organizacyjnym (np. na pozyskanie i utrzymanie zespołu).
W Polsce istnieją podmioty komercyjne, świadczące usługi typu SOC. Jeden z nich opublikował w kwietniu 2016 r. informację o zrealizowaniu koncepcji SOC dla dużej jednostki administracji państwowej (ComCERT 2016). Brak jednak dostawcy podobnej usługi, który sam byłby jednostką sektora publicznego. Trudno też o konkretne szacunki oszczędności na outsourcingu bezpieczeństwa. Obliczenia dla modelowego przedsiębiorstwa działającego na rynku światowym (12 lokalizacji, 2 centra danych w USA i Wielkiej Brytanii) dały wynik ponad 1 mln USD rocznych oszczędności (Foresite.com 2015). Inwestycje we własne zasoby IT istotnie często nie znajdą uzasadnienia ekonomicznego, zważywszy że dostawcy usług mogą od razu dostarczyć właściwych kompetencji oraz rozbudowującej się infrastruktury, łącznie z centrami danych oraz ich zapleczem (Integrated Solutions 2015).

Działalność PCSS w sferze bezpieczeństwa publicznego
Poznańskie Centrum Superkomputerowo - Sieciowe jest jednostką Polskiej Akademii Nauk i działa w sektorze akademickim od 1993 roku, dostarczając usług komunikacyjnych (sieć miejska POZMAN i sieć krajowa PIONIER), obliczeniowych, składowania danych oraz usług w chmurze.

Sieć PIONIER
PCSS jest operatorem ogólnopolskiej szerokopasmowej sieci optycznej dla nauki PIONIER, która łączy 5 centrów superkomputerowych (Gdańsk, Kraków, Poznań, Warszawa, Wrocław) i 22 operatorów sieci miejskich MAN. PIONIER powstał na bazie sieci POL-34 w latach 2001-2003. Obejmuje ponad 6500 km własnych łączy światłowodowych w kraju oraz 700 km w Europie, bazuje na technologiach DWDM, MPLS, VPLS i IPv4/IPv6. Sieć stanowi podstawę do tworzenia zaawansowanych usług dla nauki i posiada bezpośrednie połączenia z sieciami naukowymi krajów sąsiednich, a za ich pośrednictwem – paneuropejską siecią dla nauki GÉANT (Stroiński et al. 2008, s. 57-94).

Rysunek 11. Struktura topologiczna sieci PIONIER



Źródło: materiały własne

Przykładem nowoczesnych usług dla nauki bazujących na sieci PIONIER są opracowane w ramach projektu PLATON[33] usługi: wideokonferencji, Eduroam, kampusowe, powszechnej archiwizacji oraz naukowej interaktywnej telewizji HD.

Cyberbezpieczeństwo w PCSS

Oprócz ochrony własnej infrastruktury, PCSS prowadzi badania nad zabezpieczeniami sieci i systemów ICT, a także aktywnie uczestniczy w krajowych i międzynarodowych projektach B+R związanych z cyberbezpieczeństwem. Prowadzi zespół CERT dla sieci PIONIER. Eksperci realizują szkolenia, występują na konferencjach branżowych. PCSS zrealizował wiele zewnętrznych audytów bezpieczeństwa, m.in. na potrzeby konferencji

[33]http://www.platon.pionier.net.pl/online/.

klimatycznych ONZ UNFCCC COP, dla banków, elektrowni, instytucji publicznych i służby zdrowia itd.
W ramach nowo otwartego Centrum Badawczego Polskiego Internetu Optycznego (CBPIO), wśród ponad 20 laboratoriów umożliwiających oferowanie innowacyjnych usług B+R, powstało Laboratorium Bezpieczeństwa Cyberprzestrzeni i Ochrony Infrastruktur Krytycznych. Do podstawowych jego zadań należą m.in.: analiza bezpieczeństwa oprogramowania, budowa nowatorskich zaawansowanych systemów bezpieczeństwa czy rozwój metodologii oceny poziomu zabezpieczeń.

PCSS a bezpieczeństwo publiczne

PCSS jest współzałożycielem Polskiej Platformy Bezpieczeństwa Wewnętrznego[34] (PPBW), forum dialogu pomiędzy użytkownikami końcowymi, światem naukowo-badawczym i administracją. PPBW stała się też platformą do budowania konsorcjów realizujących działania na rzecz tworzenia dedykowanych rozwiązań technologicznych i informatycznych, wspomagających działania podmiotów odpowiedzialnych za bezpieczeństwo publiczne **Błąd! Nie można odnaleźć źródła odwołania.**).
PCSS zrealizował dla potrzeb Policji projekty „Zarządzanie informacją i wiedzą w usługach o podwyższonym poziomie bezpieczeństwa" oraz "Zintegrowana Platforma Teleinformatyczna o podwyższonym poziomie bezpieczeństwa", koncentrujące się na dostarczeniu bezpiecznej, skalowalnej i niezawodnej architektury sieciowej z dodatkowymi elementami bezpieczeństwa, m.in. dedykowanym systemem Meta-IDS (Frankowski et al. 2012, s. 107-117). Realizowane były i są projekty oparte na tworzeniu systemów eksperckich do detekcji zagrożeń oraz rozwiązań wspierających zarządzanie incydentami: SECOR – „Moduł korelacji danych sensorycznych dla potrzeb wykrywania działań nieuprawnionych oraz wspomagania procesu podejmowania decyzji" oraz projekt europejski H2020 PROTECTIVE – „Proactive Risk Management through Improved Situational Awareness".

[34]http://www.ppbw.pl.

PCSS jest jednym z członków-założycieli Klastra „Obszar Zaawansowanych Technologii Bezpieczeństwa i Obronności", powołanego w roku 2014 na Politechnice Śląskiej.

Cel: działać dla pożytku publicznego

Od wielu lat PCSS, wraz z konsorcjum PIONIER, buduje innowacyjne i bezpieczne usługi dla nauki, ale także dla administracji publicznej czy placówek edukacyjnych. W ostatnich miesiącach, wspólnie z partnerami zrzeszonymi w Wielkopolskim Klastrze Teleinformatycznym, idąc za wskazówkami Strategii na Rzecz Odpowiedzialnego Rozwoju[35], opracowano w PCSS koncepcję CYBERDOG – konglomeratu systemów i usług, opartych na dostępie do e-infrastruktury, umożliwiającej podniesienie poziomu zabezpieczeń systemów ICT, IoT (Internetu Rzeczy) i SCADA m.in. przy zastosowaniu analityki HPC, systemów detekcji anomalii czy platform treningowych. Wyniki działania planowanych projektów B+R mają być skierowane w dużej mierze w stronę sektora nauki, a także administracji publicznej.

W ostatnim okresie miesiącach zainicjowano w Polsce wiele działań zmierzających do stworzenia spójnej strategii bezpieczeństwa cyberprzestrzeni polskiej, powstała „Strategia Cyberbezpieczeństwa RP na lata 2017-2022[36]. Do celów szczegółowych Strategii należą m.in. zwiększenie bezpieczeństwa teleinformatycznego dla usług cyfrowych, opracowanie i wdrożenie standardów bezpieczeństwa sieci i systemów (w szczególności dla organizacji pełniących zadania publiczne), a także zbudowanie mechanizmów współpracy między sektorem publicznym a prywatnym. Zapewnienie bezpieczeństwa w cyberprzestrzeni wymaga współpracy sektora publicznego, prywatnego i obywateli, jako jedno z kluczowych źródeł kompetencji np. w zakresie tworzenia norm i standardów wymienia się ekspertów z ośrodków naukowych, akademickich i instytucji badawczych (Ministerstwo Cyfryzacji, 2017, s. 13).

[35]https://www.mr.gov.pl/media/36848/SOR_2017_maly_internet_03_2017_aa.pdf.
[36]https://mc.gov.pl/files/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf.

Możliwość wykorzystania doświadczenia i kompetencji istniejącej grupy specjalistów bezpieczeństwa jest zatem zbieżna z założeniami Strategii. Specyfika Konsorcjum PIONIER oraz PCSS jako operatora sieci, jest przy tym w kilku aspektach szczególnie korzystna:

- Konsorcjum dysponuje nowoczesną i bezpieczną infrastrukturą przetwarzania, składowania oraz przesyłania danych, oraz zespołami doświadczonych specjalistów,
- Poszczególne jednostki Konsorcjum są rozproszone geograficznie mniej więcej równomiernie w całym kraju, a sieci metropolitalne działają w każdym mieście wojewódzkim, co ułatwi współpracę na poziomie organizacji o różnym zasięgu terytorialnym. Żadna część infrastruktury, która mogłaby być przeznaczona dla celów takiej współpracy, nie znajduje się poza granicami Polski.
- Jednostki prowadzą działalność B+R, dzięki czemu mogą wytwarzać innowacyjne systemy zabezpieczeń, które mogą być łatwo dostępne i wykorzystywane *pro publico bono* w ochronie usług publicznych.
- Konsorcjum jest neutralne technologicznie.

Podsumowanie

W powyższym opracowaniu staraliśmy się nakreślić, jak wieloaspektowe jest bezpieczeństwo IT. Trygve Gulbranssen powiedział, że pieniądz rządzi światem – i ma to zastosowanie również do cyberbezpieczeństwa. Straty zadawane przez cyberprzestępców mogą być bardzo wysokie, wiele kosztuje również zapewnienie odpowiedniej ochrony. Nieustanny wyścig między „czarnymi" a „białymi" kapeluszami[37] będzie dla tych drugich jeszcze trudniejszy w perspektywie aktualnych zmian technologicznych.

Nie wszystkie organizacje potrzebują centrum bezpieczeństwa SOC, ale wszystkie muszą podejmować stały wysiłek w celu obrony przed zagrożeniami z internetu. Na poziomie koncepcyjnym optymalną strategią postępowania jest ochrona w głąb, polegająca na mnożeniu systemów zabezpieczeń

[37] Ang. *White hat* – haker, który dąży do zapewnienia bezpieczeństwa infrastruktury, *black hat* – cyberprzestępca.

na poszczególnych warstwach. Muszą obejmować one i środki techniczne, i organizacyjne.

W większych organizacjach występuje dążenie do tworzenia specjalizowanych centrów SOC – co jest trudne, czasochłonne i drogie, dlatego część predestynowanych do tego instytucji nie jest w stanie takiego procesu przeprowadzić. Wtedy warto zastanowić się nad oddaniem opieki nad bezpieczeństwem zasobów w outsourcing. Tworzone są rozwiązania prawne i organizacyjne, które ułatwią instytucjom publicznym współpracę w tym zakresie. Umożliwi to nie tylko bardziej efektywne wykorzystanie zasobów instytucji publicznych, ale i wzrost w nich poziomu cyberbezpieczeństwa.

1.6. Outsourcing cyberbezpieczeństwa w świetle problematyki współczesnych zagrożeń w cyberprzestrzeni

1.7. Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych

Złośliwe oprogramowanie ransomware jako nowa forma cyberprzestępczości w kontekście rozwoju bankowości internetowej

Rozwój i globalizacja przyniosły nowe wyzwania dla ochrony informacji w systemach teleinformatycznych. Problematyka doskonalenia systemów bezpieczeństwa bankowości elektronicznej jest obecnie kluczowym czynnikiem procesów zarządzania ryzykiem systemów informatycznych w instytucjach finansowych i innych podmiotach (Gwoździewicz, Prokopowicz 2015, s. 209). Z przeprowadzonych przez technologiczne firmy badawcze Trend Micro (*Raport Trend Micro: wzrost liczby ataków ransomware w 2016*) oraz Cisco analiz, wynika, że procedury i systemy bezpieczeństwa infrastruktury i oprogramowania informatycznego wielu firm, banków i urzędów nadal wymagają zmodernizowania i dostosowania, celem znacznego zmniejszenia ryzyka ingerencji cyberprzestępców oraz zastosowania nowoczesnych rozwiązań technologii teleinformatycznej na miarę standardów XXI wieku (Goździewicz, Prokopowicz 2016a, s. 397).

Z rozwojem internetowej bankowości elektronicznej wiąże się wiele udogodnień dla klientów i kontrahentów banków oraz redukcja kosztów transakcyjnych w instytucjach finansowych. Z drugiej strony rozwój bankowości internetowej generuje wiele zagrożeń związanych z włamywaniem się na elektroniczne konta bankowe i kradzież pieniędzy oraz danych osobowych. W odpowiedzi na te zagrożenia banki rozbudowują systemy bezpieczeństwa transakcji realizowanych za pośrednictwem internetu (Prokopowicz, Dmowski, 2010, s. 341). W analiz przeprowadzonych przez technologiczne firmy badawcze wynika, że w ostatnich latach odnotowano wzrost powstawania nowych form zagrożeń hakerskich, w tym nowych rodzajów złośliwego oprogramowania tworzonego przez cyberprzestępców celem przejęcia kontroli nad komputerami

użytkowników bankowości internetowej i innych usług (Górka, red. 2014, s. 49). W odpowiedzi na te rosnące zagrożenia w instytucjach sektora finansowego, publicznego oraz w korporacjach bezustannie doskonalone są procedury bezpieczeństwa systemów informatycznych, usuwane są luki w systemach bezpieczeństwa oprogramowania za pomocą którego bank, firma czy urząd połączony jest z globalną siecią internet (Prokopowicz, Dmowski, Sarnowski, 2005, s. 73). W 2016 roku zaobserwowano silny wzrost aktywności w internecie złośliwego oprogramowania typu ransomware, za pomocą którego cyberprzestępcy blokują działanie komputera, smartfona lub innego urządzenia podłączonego do globalnej sieci aby następnie wyłudzić od ofiary cyberataku zapłacenie okupu za przywrócenie prawidłowego działania zainfekowanego w ten sposób urządzenia. Obecnie wzrasta potrzeba doskonalenia procesów zarządzania ryzykiem systemów informatycznych funkcjonujących w instytucjach finansowych, przedsiębiorstwach oraz podmiotach sektora publicznego. Szczególnie istotnym czynnikiem, który powinien być w większym stopniu zastosowany w budowaniu strategii rozwoju bezpieczeństwa systemów teleinformatycznych jest innowacyjność (Matosek 2009, s. 34) w zakresie przeprowadzania testów symulowanych ataków hakerskich celem zdiagnozowania przez zatrudnionych informatyków luk w zabezpieczeniach (*Billion-DollarScams ...,* 2016).

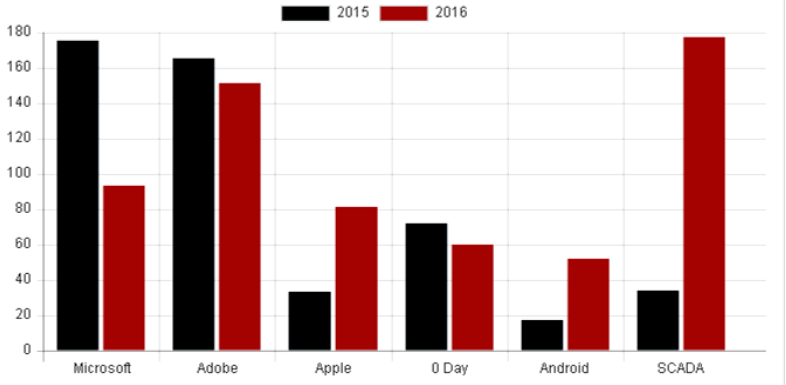
W artykule, w oparciu o źródła literatury fachowej oraz analizę raportów opracowanych przez technologiczne firmy badawcze Trend Micro oraz Cisco, przedstawiono problematykę zagrożeń i bezpieczeństwa bankowości elektronicznej oraz połączonych z internetem systemów informatycznych firm, instytucji finansowych i podmiotów sektora publicznego. W szczególności zwrócono uwagę na wzrost ryzyka aktywności złośliwego oprogramowania w wewnętrznych systemach informatycznych, kradzieży danych osobowych i informacji niejawnych oraz ich ujawniania przez osoby niepowołane, oraz przejęcia kontroli przez cyberprzestępców nad systemami operacyjnymi i infrastrukturą informatyczną zaatakowanych elektronicznie banków, korporacji i instytucji publicznych. Istotną kwestią prewencyjnego zwalczania cyberprzestępczości jest tworzenie scentralizowanych rozwiązań instytucjonalnych jak np. niedawno utworzone w Polsce instytucje Narodowego

Centrum Cyberbezpieczeństwa i Bankowego Centrum Cyberbezpieczeństwa, które będą koordynowały i rozwijały systemowo aktywizację procesów doskonalenia procedur i systemów bezpieczeństwa banków, instytucji sektora publicznego oraz przedsiębiorstw (Domańska-Szaruga, 2013, s. 263).

Oprogramowanie firm Adobe i Microsoft szczególnie podatne na ataki cyberprzestępców

Większość wykrytych przez firmy Trend Micro i Zero Day Initiative (ZDI wraz z TippingPoint) luk w zabezpieczeniach wykryta została w aplikacjach Adobe® Acrobat® Reader DC i WebAccess SCADA firmy Advantech. Oprogramowanie sieciowe WebAccess i inne systemy informatyczne klasy SCADA stosowane są obecnie powszechnie w podmiotach sektora publicznego oraz w przedsiębiorstwach i instytucjach sektora finansowego do zdalnej obsługi systemów informatycznych i automatyzacji procesów przemysłowych przedsiębiorstw jak również usług podmiotów użyteczności publicznej (*TrendLabs 2016 Annual Security Roundup…,* 2017).

Rysunek 12. Luki w zabezpieczeniach wykryte w latach 2016-2015 przez firmy analityczne Trend Micro i ZDI (wspólnie z TippingPoint).



Źródło: *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raportfirmyanalitycznej Trend Micro, 28.02.2017,(www.trendmicro.com/vinfo /us/security/research-and-analysis/threat-reports/roundup).

Wśród aplikacji, w których w 2016 roku wykryto najwięcej luk w zabezpieczeniach nie znalazł się program Adobe Flash (Leopando, 2016), ponieważ w tym rankingu w innych programach wykryto odpowiednio więcej luk, co może być związane z tym, że w ostatnim czasie więcej przeglądarek korzysta z języka HTML5. Jednak aplikacja Adobe Flash była także wykorzystywana w 2016 roku jako „nośnik" dla programów ransomware. Złośliwe oprogramowanie zawarte w aplikacji Adobe Flash umożliwiało cyberprzestępcom przeprowadzenie kampanii phishingowej skierowanej przeciwko rządom i ambasadom na całym świecie. Podobnie jak w poprzednich latach nadal najwięcej luk w zabezpieczeniach wykrywanych jest w systemie operacyjnym Windows i aplikacjach globalnego dostawcy oprogramowania firmy Microsoft. Jednak porównując rok 2016 do poprzedniego to zauważono wyraźny spadek liczby luk w zabezpieczeniach oprogramowania produkowanego przez Microsoft. Natomiast w tym samym czasie odnotowano wzrost zwiększających ryzyko ingerencji cyberprzestępców w aplikacje firmy Apple. Wzrost ten dotyczy zarówno zdiagnozowanych luk w zabezpieczeniach dla komputerów stacjonarnych, laptopów jak i urządzeń mobilnych typu smartfonów (*TrendLabs 2016 Annual Security Roundup ...,* 2017).

Z przeprowadzonych badań wynika, że w systemach operacyjnych i aplikacjach firmy Microsoft odnotowano 47-procentowy spadek luk w zabezpieczeniach w 2016 roku wobec roku poprzedniego. W produktach koncernu Microsoft zdiagnozowano łącznie już tylko 93 rodzajów luk w zabezpieczeniach. Spośród produktów koncernu Microsoft najwięcej luk w zabezpieczeniach zdiagnozowano w przeglądarce internetowej Internet Explorer. Jednak także w przypadku i tej aplikacji odnotowano duży spadek tych luk tj. znacząco poprawiono kwestię bezpieczeństwa korzystania z tej przeglądarki. W 2015 roku odnaleziono w tej przeglądarce aż 121 luk podczas gdy w 2016 r. już znacznie mniej ponieważ już „tylko" 33, co oznacza spadek aż o 73 proc. Analitycy firm technologicznych, które zdiagnozowały te luki wskazują, że istnieje kilka determinantów tego znacznego spadku. Producent tej przeglądarki, tj. firma Microsoft cyklicznie opracowywała i wdrażała poprawki zabezpieczeń. Proces usuwania luk w zabezpieczeniach polegał na cyklicznej, comiesięcznej

aktualizacji zabezpieczeń m.in. poprzez bieżące łatanie wykrytych luk w zabezpieczeniach.

Permanentne, dostosowane do bieżącej sytuacji łatanie zdiagnozowanych luk i umieszczanie w systemach informatycznych dodatkowych interfejsów zabezpieczających i ostrzegających przed zagrożeniami to nadal najlepsze metody ochrony przed atakami typu zero-day i potencjalnymi atakami malware i ransomware.

Tabela 1. Aplikacje w których wykryto najwięcej luk w zabezpieczeniach w 2016 roku.

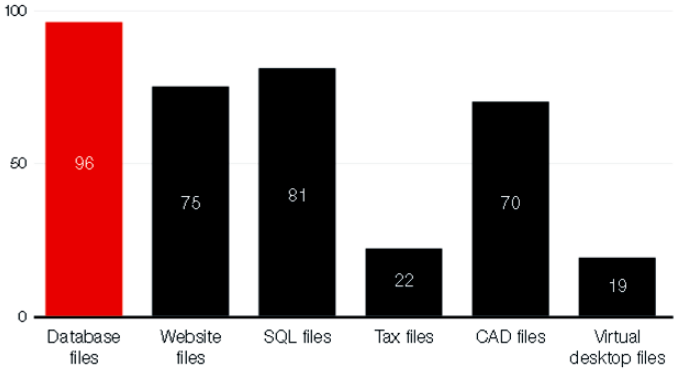
Aplikacja	Liczba luk w zabezpieczeniach
Advantech WebAccess	109
Adobe® Acrobat® Reader DC	89
Apple® OS X®	52
Android	52
Foxit® Reader	49
Adobe Flash®	38
Microsoft Internet Explorer®	33
Microsoft Windows® OS	26
Solar Winds®	25
Microsoft Edge	22

Źródło: *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raport,firmy,analitycznej Trend Micro, luty 2017, s. 10,(https://documents. trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf).

Z raportu „*TrendLabs 2016 Annual Security Roundup: A RecordYear for Enterprise Threats*" wynika, że w 2016 roku najwięcej rodzajów rodzin złośliwego oprogramowania ransomware jakie stworzyli cyberprzestępcy to były ukryte w spamie i rozsyłanych metodą BEC w mailach programy szyfrujące bazy danych firm i instytucji finansowych. Z przeprowadzonych badań wynika, że w 2016 roku jednym z głównych celów działalności cyberprzestępców było przeprowadzenie ataków z użyciem oprogramowania ransomware, za pomocą

którego dokonywano ataków polegających na szyfrowaniu plików bazodanowych w zainfekowanych systemach informatycznych firm zawierających w swych strukturach bazy danych z kluczowymi dla zaatakowanych podmiotów informacjami (Malak, 2017, s. 49). Kwestię tę przedstawia Rysunek 13.

Rysunek 13. Liczba głównych rodzin złośliwego oprogramowania ransomware szyfrujących wyszczególnione rodzaje plików związanych z działalnością firmy w 2016 roku.



Źródło:,*TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raport,firmy,analitycznej Trend Micro, luty 2017, s. 5,(https://documents. trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf).

Różne rodzaje załączników mailowych i technik rozsyłania spamu zawierającego ukryte złośliwe oprogramowanie ransomware

Obecnie wśród kierowników wydziałów bezpieczeństwa systemów informatycznych banków dominuje opinia, że ataki typu ransomware należą obecnie do największych zagrożeń dla instytucji finansowych, podmiotów sektora publicznego i przedsiębiorstw. Z danych raportu firmy badawczej Trend Micro „*TrendLabs 2016 Annual Security Roundup: A RecordYear for Enterprise Threats*" wynika, że liczba nowych odmian złośliwego oprogramowania infekującego komputery kodem ransomware w niedługim czasie wrosła ostatnio

o prawie 750% a wyłudzone okupy za zdjęcie założonych przez uprzednie infekcje ransomware z systemów informatycznych i określonych aplikacji blokad w skali globalnej szacuje się na ok. 1 mld dolarów. Taką kwotę od instytucji i przedsiębiorstw udało się wyłudzić przez cyberprzestępców mimo coraz powszechniej organizowanych w mediach kampanii informacyjnych, w których przestrzega się przed tymi zagrożeniami. Szacuje się, że statystycznie od każdej firmy, która zapłaciła okup za zdjęcie nałożonej na system informatyczny blokady, cyberprzestępcy wyłudzili po ok. 140 tys. dolarów (Król, 2017, s. 46).

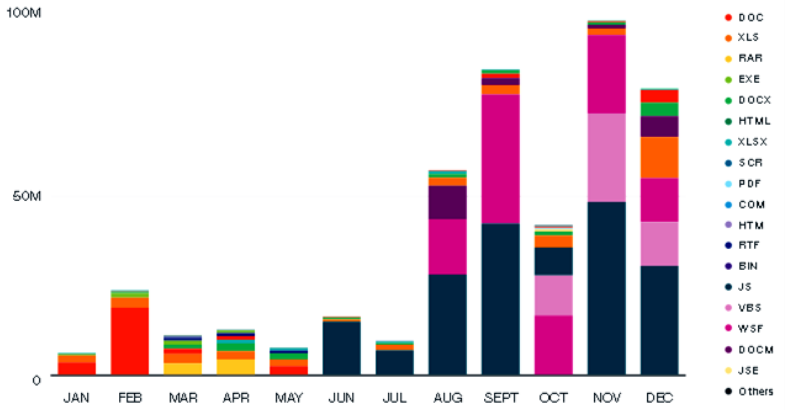
W ostatnich kwartałach cyberprzestępcy rozsyłali zainfekowany kodem ransomware spam doskonaląc swe hakerskie techniki poprzez zabiegi socjotechniczne do których zalicza się (Krebs 2016):

- kierowanie spamu do kierowników niższego szczebla lub pracowników operacyjnych w wybranych zwykle większych firmach, tj. osoby charakteryzujące się zwykle niższą świadomością potencjalnych zagrożeń wobec systemów, w których pracują, a firma jest na tyle duża, że stać ją na zapłacenie okupu,
- rozsyłanym mailom typu spam nadawana jest forma pism urzędowych znanych instytucji, ostatnio także wyspecjalizowanych firm handlowych lub kurierskich oraz dodawany atrybut wysokiego priorytetu,
- komputer infekowany jest poprzez złośliwe oprogramowanie ukryte w załączniku maila rozsyłanego jako spam, jednak aby uaktywnić infekcję w niektórych wersjach spamingu nie trzeba już nawet otwierać załącznika, wystarczy otwarcie zainfekowanego maila lub najechanie kursorem wskaźnika myszki komputerowej na plik załącznika bez jego otwierania,
- cyberprzestępcy konstruują sieci botnet wielu zainfekowanych komputerów, które rozsyłają kopie maili typu spam w milionach sztuk dziennie; zainfekowane komputery użytkowników mogą stać się nowym centrum rozsyłania zainfekowanego spamu dzięki czemu jeden zainfekowany komputer w firmie może rozesłać kopie złośliwego oprogramowania w spamie do setek innych komputerów w danej firmie,
- hakerzy tworzący złośliwe oprogramowanie celem przejęcia kontroli nad komputerem czy także np. internetowym kontem bankowości elektronicznej

określonego użytkownika wykorzystują wszelkie luki systemowe i produktowe, jakie się tylko pojawiają; odnotowane liczne w 2016 roku ataki DDoS generowane przez botnetMirai wycelowane były w znajdujące się w sprzedaży wytwarzane w Chinach urządzenia, w których w protokole telnet zakodowane było bardzo proste do „rozszyfrowania" a w zasadzie to do odgadnięcia hasło typu: „123456" (Goodin, 2014).

Poza tym od czerwca 2016 roku odnotowano silny wzrost rozsyłanego przez cyberprzestępców spamu zawierającego złośliwe oprogramowanie ransomware ukryte w plikach załączników JavaScript. Znaczący wzrost załączników JavaScript w listopadzie 2016 roku był spowodowany przez złośliwy program NEMUCOD, za pomocą którego cyberprzestępcy żądali okup od firm i banków, których komputery zostały zainfekowane tym programem typu ransomware. Poza tym w tym okresie także odnotowano wzrost rozsyłania za pośrednictwem poczty elektronicznej programów ransomware LOCKY.

Rysunek 14. Najpopularniejsze rodzaje plików w załącznikach zawierających złośliwe oprogramowanie ransomware rozsyłanych w spamie w 2016 r.



Źródło: *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raport firmy analitycznej Trend Micro, luty 2017, s. 23,(https://documents. trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf).

1.7. Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych

Na rysunku 14 przedstawiono najpopularniejsze rodzaje plików z 2016 roku, które rozsyłane w załącznikach wiadomości mailowych i w spamie zawierały ukryte złośliwe oprogramowanie ransomware infekujące komputery i urządzenia mobilne użytkowników.

Atak z botnetu Mirai

Atak z botnetu Mirai dodatkowo przyczynił się do zwiększenia presji na doskonalenie procedur bezpieczeństwa i poprawę zabezpieczeń systemów informatycznych. Serwer botnetowy Mirai złożony był z około 100 000 zagrożonych urządzeń internetowych (IoT) i za pośrednictwem tak zbudowanego serwera dokonano ataków typu DDoS (Distributed Denial-of-Service) przeprowadzonych na dużą skalę przy użyciu urządzeń dostawcy usług DNS, zakłócając dostęp do wielu witryn internetowych określonych firm i instytucji (Pauli 2016). Przeprowadzony w ten sposób atak zmusił wiele firm, w tym technologicznych i internetowych do wyłączenia na kilka godzin prowadzonych stron internetowych oraz oferowanych za pomocą tych stron usług, tj. do wymuszonego przejścia do trybu offline (York 2016).

Według tego schematu przeprowadzono atak na urządzenia technologii Dyn, z których korzystają takie firmy świadczące komunikacyjne usługi internetowe jak Twitter, Reddit i Spotify. Pod koniec 2016 roku pojawiły się również inne doniesienia w mediach dotyczące przeprowadzonych przez cyberprzestępców włamań z wykorzystaniem urządzeń technologii IoT. Przy pomocy złośliwego oprogramowania ransomware FLOCKER cyberprzestępcy dokonali ataku na systemy informatyczne różnych podmiotów za pośrednictwem Telewizorów wyposażonych w technologię smart (Duan, 2016). Udany atak spowodował u zaatakowanego użytkownika wyświetlenie komunikatu, który sugerował w treści, że wygenerowany jest przez organy ścigania i informował użytkowników o dokonanie rzekomych przestępstw. Ofiary tych ataków z wyświetlonego komunikatu dowiadywali się, że zostali zidentyfikowani przez określone organy ścigania, instytucje prewencji jako przestępcy i zostali oskarżenia o popełnienie przestępstw, których nie popełnili. Po wyświetleniu tego komunikatu, pełniącego rolę ostrzeżenia złośliwy program ransomware

FLOCKER blokował określone urządzenie i sugerowano dokonanie wpłaty na wskazaną kartę podarunkową w wysokości 200 USD poprzez aplikację iTunes® jako warunek odblokowania podłączonego do internetu urządzenia. Inny atak przeprowadzony w podobnym modelu wyłączył w zimie systemy kontroli środowiska w tym temperatury mieszkańców dwóch budynków w Finlandii.

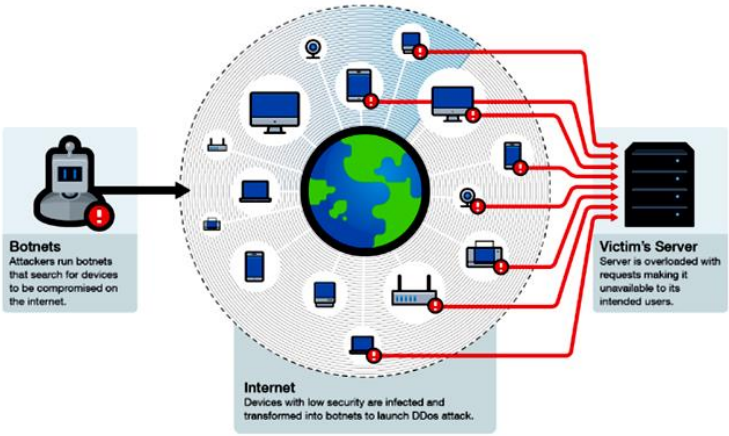
Tego typu ataki są poważnym ostrzeżeniem dla wielu innych firm i instytucji, które jeszcze nie stały się przeprowadzanych w ten sposób celem ataków. Z przeprowadzonych badań wynika, że cyberprzestępcy mogą tego typu ataków dokonywać zarówno z wewnątrz jak i z zewnątrz danej instytucji. Zaatakowane, zainfekowane złośliwym oprogramowaniem ransomware urządzenia i systemy IoT mogą stać się w sieci internet kolejnymi nośnikami ransomware infekującymi inne podłączone do internetu urządzenia. W związku z tym zainfekowane w ten sposób urządzenia mogą być wykorzystane jako kolejne przekaźniki oprogramowania ransomware wykorzystywane do przeprowadzania następnych ataków. Przeprowadzony w ten sposób zmasowany atak może istotnie zakłócić funkcjonowanie podmiotu, który stał się celem ataku. Konsekwencją skutecznego ataku ze strony cyberprzestępców może być wstrzymanie efektywnie prowadzonej działalności gospodarczej przez daną zaatakowaną firmę bądź instytucję finansową lub publiczną.

Zdarzenia tego typu potwierdzają tezę, że ataki tego typu stać się mogą także niezwykle poważnym zagrożeniem polegającym na zakłóceniu prowadzenia bieżącej komunikacji poprzez internet określonej firmy z innymi podmiotami.

Celem zmniejszenia ryzyka pojawienia się tego typu zagrożeń w wydziałach zarządzania bezpieczeństwem wielu firm i instytucji podjęto już szereg działań zabezpieczających systemy informatyczne i udoskonalane są procedury bezpieczeństwa (Bisson, 2016). W ramach poprawy procedur systemów bezpieczeństwa zaleca się regularne przeprowadzanie analizy ryzyka ingerencji cyberprzestępców w systemy informatyczne, usuwanie na bieżąco wykrytych luk w zabezpieczeniach celem utrzymania wysokiego poziomu bezpieczeństwa protokołów komunikacyjnych aplikacji za pomocą, których firma jest podłączona do globalnej sieci internet. Poza tym zaleca się także częste zmiany haseł urządzeń komunikacyjnych i teleinformatycznych oraz przechowywanie

danych o wysokim priorytecie poufności w pamięci wewnętrznej w trybie up-to-data w trybie bez dostępu do internetu (*TrendLabs 2016 Annual Security Roundup…,* 2017).

Rysunek 15. Mechanizm ataku typu DDoS z botnetu Mirai.



Źródło: *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raportfirmyanalitycznej Trend Micro, 28.02.2017,(www.trendmicro.com/vinfo /us/security/research-and-analysis/threat-reports/roundup).

Kradzież danych osobowych - największe naruszenie danych w historii

Wykryte w raportach firm analitycznych dokonywane przez hakerów naruszenia danych w systemach informatycznych, do których się włamali nie są już obecnie nowym zjawiskiem. Natomiast dyskusyjną kwestią pozostaje ujawnianie tego typu zdarzeń do mediów przez firmy i instytucje, które padły ofiarą ataków cyberprzestępców. Ataki, które kwalifikowane są do pojęcia naruszenia danych sprowadzają się zwykle do zmiany danych, szyfrowania, blokowania dostępu do informacji oraz do wykradania danych z systemów informatycznych, baz danych zaatakowanej firmy. Tego typu hakerskie ingerencje ze strony nie powołanych do tego podmiotów wykrywano wśród różnego rodzaju firm i instytucji reprezentujących różne sektory i gałęzie gospodarki, w tym

podmiotów sektora publicznego, także sektora edukacji, szkolnictwa wyższego (*Michigan State University Confirms Data ...,* 2016) oraz opieki zdrowotnej (Young, 2016).

Dylemat odnośnie kwestii ujawniać czy nie ujawniać zdarzenia ataku i naruszenia danych przez cyberprzestępców rozważano ostatnio na przykładzie kradzieży danych osobowych z portalu Yahoo. Tego typu zdarzenia i ich ujawnienie do mediów może mieć duży wpływ na funkcjonowanie firmy. Ujawnienie zdarzenia dokonanego na dużą skalę naruszenia danych może spowodować odpływ klientów, usługobiorców i spadek zainteresowania ofertą usług ze strony potencjalnych, nowych nabywców. W przypadku portalu Yahoo może to oznaczać drastyczny spadek portfela kont użytkowników korzystających z usług tej firmy internetowej, czyli zmniejszenia ilości kont mailowych i klientów korzystających z wyszukiwarek i informacji zawartych na tym portalu. W konsekwencji może to doprowadzić do spadku wpływów z wyświetlanych na banerach internetowych reklam i problemy finansowe.

Kwestia naruszenia danych, a konkretnie kradzieży danych osobowych z portalu Yahoo jest dobrym przykładem na prowadzenia badań nad rozstrzygnięciem wymienionego powyżej dylematu. Wynika to ze skali kradzieży danych osobowych jaką dokonali cyberprzestępcy w sierpniu 2013 roku. Wówczas cyberprzestępcy wykradli z portalu Yahoo ogromną ilość niejawnych danych osobowych, ponieważ łupem internetowych rabusiów padł ponad 1 miliard kont użytkowników. Wraz z wykradzionymi informacjami dotyczącymi poszczególnych kont hakerzy ukradli imiona i nazwiska użytkowników kont, daty ich urodzenia, adresy e-mail, hasła dostępu do konta mailowego oraz numery telefoniczne (*Yahoo Discloses 2013 BreachthatExposed ...,* 2016).

Obecnie jest to największe naruszenia danych w historii cyber kradzieży danych osobowych. Informacja o tej spektakularnej kradzieży trafiła do mediów dopiero w grudniu 2016 roku czyli ponad 3 lata po jej dokonaniu. Być może firmie prowadzącej portal Yahoo udawałoby się zachowywać nadal w tajemnicy tę największą internetową kradzież. Jednak we wrześniu 2016 roku z portalu Yahoo znów wykradzione zostały dane osobowe z 500 milionów kont użytkowników. Przy okazji tych informacji trafiających w grudniu 2016 roku do mediów świat dowiedział się także o tej jeszcze bardziej spektakularnej

kradzieży dokonanej w 2013 roku. Tego typu zdarzenia po ich ujawnieniu w mediach znacząco podważają dotychczasową reputację firmy i stawiają znak zapytania w kwestii bezpieczeństwa danych osobowych gromadzonych na internetowych portalach mailowych i społecznościowych. Kwestią kluczową dla efektywnego funkcjonowania i rozwoju tego typu firmy świadczącej informacyjne usługi internetowe jest odpowiedzialność firmy za bezpieczeństwo gromadzonych danych niejawnych, w tym osobowych (*TrendLabs 2016 Annual Security Roundup …,* 2017, s. 15).

Włamania cyberprzestępców do oprogramowania ATM w bankomatach

W 2016 roku zaobserwowano również rozwój złośliwego oprogramowania oraz skanowania kart bankowych poprzez skimming w związku z czym rosły zyski cyberprzestępców elektronicznie włamujących się do systemów informatycznych banków powiązanych z obsługą bankomatów. Od wielu już lat bankowi hakerzy doskonalą swe techniki włamywania się do bankomatowego oprogramowania ATM poprzez stworzone złośliwe oprogramowanie znane jako tzw. SKIMER. Z raportu *TrendLabs 2016 Annual Security Roundup: A RecordYear for Enterprise Threats*(*TrendLabs 2016 Annual Security Roundup: …,* 2017, s. 21) wynika, że w 2016 roku wspomniany Skimer został niedawno zaktualizowany, celem przejęcia kontroli nad bankomatami przez cyberprzestępców.

Jednym z głównych czynników tworzenia przez cyberprzestępców złośliwego oprogramowania dedykowanego do systemów bankomatowych ATM jest nadal stosowane w części urządzeń bankomatowych przestarzałych wersji systemów operacyjnych. W niektórych bankach nadal jest wiele urządzeń, w których funkcjonują nieaktualne systemy operacyjne, takie jak Windows® XP. Obecnie przyjmuje się, że ten system operacyjny jest szczególnie narażony na skuteczne ataki hakerskie i wynikające z tego niebezpieczeństwo relatywnie łatwego włamania się do bankowego systemu ATM. Powodem jest brak aktualizowania systemu Windows® XP przez firmę Microsoft, która zakończyła wsparcie w tym zakresie w 2016 roku, a niektórych wersji tego systemu to nawet znacznie wcześniej (Massy 2014).

1.7. Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych

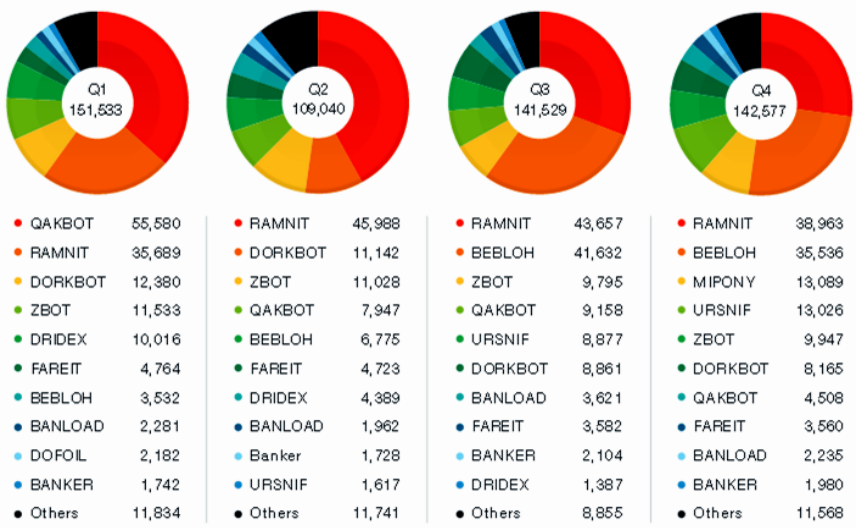
Rysunek 16. Rodziny złośliwego oprogramowania ATM i ich geograficzne pochodzenie.

Źródło: *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raport firmy analitycznej Trend Micro, luty 2017, s. 21,(https://documents. trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf).

Z testów przeprowadzanych przez analityków systemów informatycznych wynika, że wszystkie urządzenia wyposażone w system Windows XP mogą być mogą być obecnie celem ataków, ponieważ producent wycofał się z aktualizowania wykrywanych luk w zabezpieczeniach. Celem zdywersyfikowania sposobów przeprowadzanych ataków, cyberprzestępcy stosują różne warianty złośliwego oprogramowania dedykowanego dla systemów bankomatowych ATM. Niedawno wykryto nową wersję złośliwego oprogramowania zwanego ALICE, które stworzone zostało w październiku 2014 celem włamywania się do oprogramowania ATM. Z pomocą tego programu

cyberprzestępcy uzyskiwali możliwość podłączania się do klawiatury numerycznej zainfekowanego urządzenia bankomatu (Gwoździewicz, 2016). Program ALICE charakteryzuje się prostotą w zakresie instalacji lub odinstalowania i działa na tyle szybko, że cyberprzestępca uruchamia plik wykonywalny bezpośrednio w docelowym środowisku. Aby zainfekować bankomat programem ALICE cyberprzestępca musi zwykle fizycznie otworzyć bankomat i zarazić maszynę przy użyciu dysku CD-ROM lub USB.

Rysunek 17. Najpowszechniejsze rodziny złośliwego oprogramowania bankowego w 2016 roku.



Źródło:*TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats* [in] portal internetowy "Trend Micro", Raportfirmyanalitycznej Trend Micro, luty 2017, s. 22,(https://documents. trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf).

W związku z nadal funkcjonującym procederem rozprzestrzeniania się złośliwego oprogramowania bankowego i trojanów bankowych, to przede wszystkim banki i inne atakowane przez cyberprzestępców instytucje finansowe powinny stale doskonalić swe procedury bezpieczeństwa transferu danych w systemach teleinformatycznych. Powszechnie dominuje opinia,

że za utrzymanie wysokiego poziomu bezpieczeństwa bankowych systemów informatycznych i aplikacji podłączonych do internetu odpowiedzialne są instytucje bankowe i to one powinny ponosić koszty zarządzania ryzykiem systemów informatycznych. Koszty te nie powinny być przerzucane na klientów. Banki w swych materiałach marketingowych kierowanych do klientów informują o wysokim poziomie bezpieczeństwa systemów informatycznych. Banki w swym przekazie marketingowym gwarantują bezpieczeństwo swoich systemów, zapewniają o wysokim poziomie bezpieczeństwa swoich bankomatów. Utrzymanie tego wysokiego poziomu bezpieczeństwa systemów oprogramowania ATM zdeterminowane jest głównie cyklicznym i częstym przeprowadzaniem aktualizacji systemów operacyjnych, regularnym prowadzeniem kontroli. W ten sposób usuwane zostają na bieżąco wykrywane luki w zabezpieczeniach oprogramowania bankomatów i innych urządzeń bankowych (*TrendLabs 2016 Annual Security Roundup: ...,* 2017, s. 22).
Z drugiej strony, biorąc pod uwagę kwestię odpowiedzialności za zabezpieczanie transakcji dokonywanych online, również klienci banków pełnią w tym zakresie istotną rolę. Konsumenci usług bankowych powinni być na bieżąco informowani o nowych rodzajach zagrożeń jakie pojawiają się w sytuacji przeprowadzania transakcji w ramach bankowości internetowej. Nie wszyscy jeszcze użytkownicy systemów elektronicznej bankowości wiedzą, że np. cyberprzestępcy z wykorzystaniem złośliwego oprogramowania bankowego mogą uzyskać dostęp do kodu PIN i poświadczenia przeprowadzanej elektronicznie przez użytkownika transakcji. Użytkownicy systemów elektronicznej bankowości powinni regularnie zmieniać hasła dostępu do internetowego konta i powinni zachowywać szczególną ostrożność w sytuacji przeprowadzania transakcji online. Poza tym zaleca się, aby użytkownicy bankowości internetowej mogli niezależnie zabezpieczać różne technologie transferu danych w elektronicznej bankowości takie jak: witryny internetowe, wiadomości przesyłane poprzez e-mail oraz pliki w załącznikach.

1.7. Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych

Doskonalenie procedur bezpieczeństwa w systemach teleinformatycznych firm i instytucji finansowych

Jedną z czołowych instytucji analitycznych badających cyberzagrożenia transferu danych w internecie i wdrażających techniki oraz procedury bezpieczeństwa jest notowana na rynku giełdowym NASDAQ pod akronimem CSCO technologiczna firma Cisco.

Zgodnie z treścią opublikowanego raportu „Annual Cybersecurity Report" (*Cisco 2017 AnnualCybersecurity Report ...,* 2017) firma Cisco na podstawie przeprowadzonych badań wykazała, że w ostatnich kwartałach do najpowszechniej stosowanych technik przejmowania kontroli nad komputerem użytkownika, było wcześniejsze zainfekowanie złośliwym oprogramowaniem typu adware lub rozsyłanego w ogromnej ilości spamu. W związku z tym wiele firm i instytucji, które stały się obiektem ataków cyberprzestępców stara się informacje o tego typu negatywnych zdarzeniach zachować w tajemnicy z obawy o potencjalny spadek reputacji marki, przychodów i dochodów. Z drugiej strony rosnąca ilość infekcji nie jest wynikiem jedynie nikłej świadomości potencjalnych zagrożeń części kadry pracowników niższego szczebla wielu firm (Król 2017, s. 46). Do źródeł rosnącej liczby odnotowanych infekcji kodem ransomware komputerów kolejnych firm oraz innych form ataków hakerskich zalicza się:

- bezustanne doskonalenie technik hakerskich przez cyberprzestępców; np. do rozsyłania zainfekowanych plików nie tylko wykorzystywane są maile typu spam, ostatnio także wykryto nowe wersje TorrentLockera, który do infekowania komputerów złośliwym oprogramowaniem innych podmiotów, firm, instytucji stosuje w tym celu usługę Dropbox,
- generowanie przez cyberprzestępców wielu nowych odmian złośliwego oprogramowania, np. w 2016 roku liczba tworzonych różnych nowych wersji kodu ransomware wzrosła 10-cio krotnie,
- wiele firm i instytucji przystępuje do doskonalenia systemów bezpieczeństwa i zwiększania na ten cel wydatków dopiero gdy same staną się obiektem skutecznych bądź nieskutecznych ataków hakerskich (Grzywak, Widenka 2015, s. 81),

- problemy z kompatybilnością systemów oraz sukcesywnie rosnący pozim złożoności systemów bezpieczeństwa; z raportu „Cisco 2017 Annual Cybersecurity Report" wynika, że w 65 proc. tj. większości ankietowanych firm funkcjonujące na różnych poziomach organizacji systemy bezpieczeństwa zbudowane są z wielu różnych, nie zawsze w pełni kompatybilnych produktów, przy czym liczba podawanych tych produktów – składowych systemów bezpieczeństwa mieści się w zakresie od 6 do aż ponad 50 (*Cisco 2017 AnnualCybersecurity Report* …, 2017),
- w wielu firmach korespondencja przesyłana mailem nie zawsze jest zaszyfrowana z użyciem protokołów wysokiego priorytetu, z zastosowaniem zaawansowanych algorytmów szyfrujących.

Z badań przeprowadzonych przez analityków firmy informatycznej Cisco wynika, że większość firm, które padły ofiarą ataków hakerskich podjęły określone działania zmierzające w kierunku poprawy efektywności działania stosowanych systemów bezpieczeństwa. Do tych działań doskonalenia systemów bezpieczeństwa należały głównie (Król 2017, s. 48):

- przeważająca większość ponieważ aż 90 proc. firm zaatakowanych przez cyberprzestępców postanowiła zmodernizować stosowane procesy biznesowe celem znaczącego zwiększenia bezpieczeństwa,
- 38 proc. z tych firm zdecydowało się rozdzielić funkcje związane z utrzymywaniem infrastruktury i systemu IT od składowych systemu odpowiedzialnych za bezpieczeństwo,
- również 38 proc. z tych firm zwiększyło budżet działalności szkoleniowej i realizowały znacznie więcej szkoleń dla zatrudnionej kadry z zakresu różnych aspektów utrzymania i poprawy bezpieczeństwa w firmie,
- poza tym 37 proc. firm udoskonaliło i wdrożyło nowe rozwiązania technologiczne z zakresu zarządzania ryzykiem systemów informatycznych i znacząco ograniczyły skalę działania tego ryzyka.

W obliczu narastających zagrożeń ataków hakerskich, w tym rozsyłania spamu zawierającego złośliwe oprogramowanie typu ransomware coraz więcej firm tworzy dodatkowe zabezpieczenia systemów informatycznych i stale udoskonala pod tym względem działające w firmie oprogramowanie i infrastrukturę informatyczną. Proces ten nigdy nie zakończy się, przynajmniej dopóki realizuje

się postęp technologiczny, powstają nowe aplikacje i platformy internetowe, nowe wersje systemów operacyjnych oraz urządzenia infrastruktury informatycznej powszechnie wykorzystywane przez użytkowników. Każda niedoskonałość systemów informatycznych, teleinformatycznych sieci internetowych, wewnętrznych procedur bezpieczeństwa zostanie wcześniej lub później wykryta i wykorzystana przez internetowych włamywaczy, hakerów, cyberprzestępców. Kolejnym incydentem hakerskim potwierdzającym wspomniana tezę był niedawny atak na witrynę internetową Komisji Nadzoru Finansowego. Z analizy tej próby ataku hakerskiego banki i firmy wyciągają wnioski sugerujące, że nie wystarczy doskonalić firewalle, aplikacje odfiltrowujące spam, analizujące proceder fishingu, bramki bezpieczeństwa na hostach. Nie wystarczy zakładać dodatkowe aplikacje analizujące ruch mailowy i precyzyjnej odfiltrowujące spam zawierający złośliwe oprogramowanie. Równie istotne jest doskonalenie wewnętrznych procedur bezpieczeństwa, doskonalenie systemów elektronicznej transmisji danych wewnątrz struktury organizacyjnej firmy, tworzenie rozwiązań wymuszających na pracownikach stosowanie szyfrowania przesyłanych wiadomości i np. niekorzystania z poczty i witryn internetowych, w tym portali społecznościowych na komputerach firmowych. W związku z tym tylko tworzenie wielowarstwowych systemów bezpieczeństwa łączących wewnątrz firmowe procedury i infrastrukturę z aplikacjami pełniącymi rolę elektronicznego kontaktu firmy ze światem pozwoli na podnoszenie skuteczności systemów bezpieczeństwa (Kosiński 2015, s. 131).

Podsumowanie

Dokonujące się coraz dynamiczniej procesy globalizacyjne stanowiące istotny czynnik postępu technologicznego przyniosły nowe wyzwania dla ochrony elektronicznego przesyłania i przetwarzania danych, w tym archiwizowania danych niejawnych. Rozwój technik udostępniania informacji poprzez internet zdeterminowany jest przede wszystkim wieloma udogodnieniami dla beneficjentów, klientów i osób korzystających z usług informacyjnych oferowanych przez firmy, instytucje finansowe i publiczne. Z kolei dla podmiotów udostępniających elektronicznie informacje poprzez internet pojawia

się możliwość znaczącej redukcji kosztów transakcyjnych przeprowadzanych operacji finansowych oraz elektronicznego transferu danych. Proces udostępniania informacji poprzez internet generuje jednocześnie wiele zagrożeń związanych z przestępstwami kradzieży tożsamości, elektronicznego przechwytywania przez hakerów danych niejawnych oraz dokonywania malwersacji środków pieniężnych w systemach elektronicznej bankowości (Prokopowicz, Dmowski 2010, s. 326). W celu ograniczenia ryzyka utraty danych oraz innych zagrożeń elektronicznego transferu danych niejawnych poszczególne podmioty, w tym instytucje sektora publicznego, rozbudowują systemy bezpieczeństwa zdalnego udostępniania informacji oraz dokonywanych transakcji realizowanych za pośrednictwem globalnej sieci internet (Gąsiorowski, Podsiedlik, 2015, s. 93).

Dynamiczny rozwój tej sfery bankowości zdeterminowany jest postępem technicznym, który dokonuje się bezustannie w wielu różnych obszarach, zarówno w zakresie wykorzystywanego przez użytkowników internetu sprzętu komputerowego i innych urządzeń umożliwiających kontakt z globalna siecią jak również w zakresie rozwoju technik i sieci teleinformatycznych udostępnianych klientom przez banki. Z jednej strony klienci banków coraz chętniej korzystają z powstających w ten sposób udogodnień, a z drugiej strony banki odnotowują spadek kosztów operacyjnych i wzrost rentowności wygenerowanej poprzez wzrost liczby rachunków internetowych przy jednoczesnym spadku korzystania z tradycyjnej bankowości fizycznego oddziału banku (Grzywacz, 2016, s. 47). Jednak dla banku ja i dla jego klientów są to nie tylko same korzyści. W ostatnich latach rośnie ilość przypadków cyberprzestępstw. Dlatego też zapewnienie prawnej ochrony danych osobowych w cyberprzestrzeni powinno stanowić kluczowy aspekt w dobie ciągłego rozwoju społeczeństwa informacyjnego.

Problematyka bezpieczeństwa danych osobowych i informacji niejawnych coraz częściej uznawana jest za determinant rozwoju usług bankowości elektronicznej i przekłada się na zaufanie klientów korzystających z e-usług. W związku z tym powszechnie dominuje już opinia, że poprawa bezpieczeństwa w zakresie ochrony danych osobowych w cyberprzestrzeni powinna być koordynowana przez centralne instytucje państwa i systemu finansowego. Jeżeli te instytucje

będą sprawnie wypełniały postawione im cele w zakresie doskonalenia regulacji normujących bezpieczeństwo elektronicznego transferu danych to powinno się to przełożyć na szybszy rozwój e-usług czym zainteresowane są przede wszystkim międzynarodowe instytucje rozliczeniowe i banki.

Z przeprowadzonych badań i z analizy wyżej wymienionych raportów wynika, że mało prawdopodobne jest przy obecnym poziomie technologicznym zapewnienie pełnego poziomu bezpieczeństwa dokonywanych operacji w zakresie bankowości elektronicznej, obsługi e-usług i całkowite uniemożliwienie hakerom potencjalnego dostępu do informacji niejawnych. Instytucjonalne organy państwa, które odpowiadają za tworzenie, doskonalenie i uaktualnianie normatywów prawnych adekwatnie do dokonującego się postępu technologicznego powinny starać się możliwie najefektywniej wypełniać stosownie tę swoją rolę (Gwoździewicz, Prokopowicz, 2016b, s. 85). Aby jednak móc określić jaki to powinien być zakres tej interwencji, kontroli i uregulowania procesów elektronicznego transferu danych ze strony państwa to niezbędnym jest zweryfikowanie źródeł wzrostu liczby skutecznych włamań osób trzecich do systemów elektronicznego transferu danych. Na bieżąco powinna być prowadzona weryfikacja determinantów kwestii bezpieczeństwa transferu danych niejawnych (Goździewicz, Prokopowicz 2016a, s. 394). Niezbędnym jest permanentne precyzyjne identyfikowanie czynników ryzyka i odpowiadanie na pytanie czy te ryzyka są generowane głównie przez techniczne niedoskonałości systemów informatycznych czy raczej niedopracowane procedury bezpieczeństwa lub ignorowane umyślnie lub nieświadomie przez klientów zasady bezpiecznego korzystania z urządzeń służących do elektronicznego składowania i transferu danych, w tym także danych osobowych.

W związku z powyższym celem pełnej identyfikacji czynników ryzyka i wdrożenia stosownych regulacji bezpieczeństwa niezbędna jest pełna współpraca centralnych organów państwa zajmujących się m.in. kwestiami bezpieczeństwa elektronicznego transferu danych, w tym Policji, Ministerstwa Cyfryzacji, ABW, CBŚ, centralnych i nadzorczych instytucji sektora finansowego tj. NBP i KNF, także banków komercyjnych i innych podmiotów partycypujących w procesie elektronicznego transferu danych. Dopiero

w wyniku tej pełnej współpracy możliwe jest wypracowanie skutecznych rozwiązań systemowych i stosownego do danej sytuacji doskonalenia regulacji prawnych przez państwo.

1.8. System dozoru elektronicznego w Polsce

Dozór elektroniczny jako jeden ze sposobów na rozwiązanie problemów więziennictwa.

Przestępczość towarzyszy ludziom od zarania dziejów. Z uwagi na to, iż jest to zjawisko społecznie niepożądane, bezustannie poszukuje się skutecznych form temu zapobiegających oraz sposobów reakcji - w momencie, gdy dana jednostka naruszy porządek prawny. Jak zauważa Paweł Moczydłowski, do XVIII wieku często stosowaną karą była tzw. banicja, czyli wygnanie poza dany obszar osoby naruszającej zasady współżycia społecznego. Kiedy zorientowano się, że w rzeczywistości jednostki te są przerzucane między danymi państwami, rozpoczęto izolację przestępców w specjalnie do tego przeznaczonych miejscach. Początkowo były to wieże zamkowe i piwnice, a następnie więzienia. Wraz z rozwojem więziennictwa, kara izolacyjna stała się dominującą, a kara śmierci przestawała obowiązywać (Moczydłowski, 2006, s. 124-125).

Celem kary pozbawienia wolności jest prewencja generalna (ogólna) – czyli w skrócie ochrona społeczeństwa przed daną jednostką i odstraszenie od naruszania porządku prawnego – oraz prewencja indywidualna (szczególna), której zadaniem jest zindywidualizowane oddziaływanie resocjalizacyjne na osobę odbywającą tę karę w celu zmiany jej postaw i zachowań oraz przygotowanie do życia na wolności. W praktyce, resocjalizacja sprawcy niejednokrotnie nie przynosi oczekiwanych rezultatów (Moczydłowski, 2006, s. 125-126).

Jedną z przyczyn tego stanu rzeczy może być przeludnienie więzień. Wielokrotnie zdarzało się tak, iż skazani na karę pozbawienia wolności musieli oczekiwać na jej wykonanie, gdyż nie było miejsc w jednostkach penitencjarnych. Działo się tak zazwyczaj w przypadkach drobnej przestępczości. Społeczeństwo postrzegało to jako bezkarność sprawców (Kotowski, 2009, s. 13, 17-18). Aby poradzić sobie z problemem przeludnienia, bardzo często stosowano instytucję warunkowego zawieszenia wykonania kary pozbawienia wolności lub – rzadziej – warunkowe umorzenie postępowania.

W takich przypadkach, społeczne przekonanie o niesprawiedliwości zwiększało się. Innymi problemami, które towarzyszyły wykonywaniu kary pozbawienia wolności w warunkach izolacji były: brak możliwości zapewnienia wszystkim osadzonym wystarczająco dobrych warunków socjalno-bytowych w jednostkach penitencjarnych oraz wysokie koszty utrzymania więźniów (Moczydłowski, 2006, s. 87, 96-98).

Rozwiązania powyższych problemów upatrywano się w dozorze elektronicznym, który z powodzeniem funkcjonował m.in. w Anglii i Szwecji (Moczydłowski, 2006, s. 127). Na początku lat 90-tych nie było jednak możliwości wprowadzenia go w Polsce. Powodem był brak infrastruktury systemowej (ibidem, s. 123). W roku 1990, Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych, w Rezolucji 45/110 z dnia 14 grudnia 1990: *Wzorcowe reguły minimalne Narodów Zjednoczonych dotyczące środków o charakterze nieizolacyjnym* przyjęło, iż państwa członkowskie wprowadzą do swoich systemów prawnych środki nieizolacyjne i rozwiną je. (Kotowski 2009, s. 16-17). W podobnym tonie wypowiedział się Komitet Ministrów Rady Europy, który w roku 1999 zalecił wykorzystywanie monitoringu elektronicznego na każdym etapie postępowania karnego – *Rekomendacja nr <99> 22 dotycząca przepełnienia więzień i szybkiego wzrostu populacji więźniów* (Moczydłowski 2006, s. 116).

Wprowadzenie do polskiego systemu prawnego dozoru elektronicznego stało się faktem w dniu 18 października 2007 roku, kiedy ogłoszono Ustawę z dnia 7 września 2007 roku o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego. Ustawodawca zadecydował o tym, aby akt prawny obowiązywał wyłącznie przez 5-letni okres – od 1 września 2009 roku do 31 sierpnia 2014 roku. Intencją tej decyzji była możliwość oceny przyjętego rozwiązania systemowego i ewentualna rezygnacja z niego lub odpowiednia modyfikacja (Kotowski, 2009, s. 13-14).

Aktualnie, system dozoru elektronicznego unormowany jest w Ustawie z dnia 6 czerwca 1997 roku – Kodeks karny wykonawczy (Dz.U. 1997 nr 90 poz. 557 z późn. zm.) – dalej KKW. Regulacje prawne znajdują się w rozdziale VIIa, który został dodany przez art. 4 pkt 20 Ustawy z dnia 20 lutego 2015 roku o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw (Dz. U. poz. 396). Zmiany weszły w życie z dniem 1 lipca 2015 roku. Na podstawie Kodeksu karnego

wykonawczego sporządzone zostały ponadto następujące rozporządzenia wykonawcze:

- Rozporządzenie Ministra Sprawiedliwości z dnia 26 maja 2015 r. w sprawie określenia szczegółowych warunków technicznych i wymagań funkcjonalnych, jakie powinny spełniać środki techniczne służące do wykonywania dozoru elektronicznego, oraz sposobu funkcjonowania systemu komunikacyjno-monitorującego (Dz.U. 2015 poz. 797);
- Rozporządzenie Ministra Sprawiedliwości z dnia 28 maja 2015 r. w sprawie sposobu archiwizowania oraz sposobu i trybu usuwania danych osobowych i informacji zarejestrowanych w związku z wykonywaniem dozoru elektronicznego (Dz.U. 2015 poz. 800);
- Rozporządzenie Ministra Sprawiedliwości z dnia 3 czerwca 2015 r. w sprawie wysokości opłaty wyrównawczej dla nadajnika i rejestratora stacjonarnego lub przenośnego służących do wykonywania dozoru elektronicznego (Dz.U. 2015 poz. 813);
- Rozporządzenie Ministra Sprawiedliwości z dnia 10 października 2016 r. w sprawie wzoru pisemnego pouczenia o przysługujących skazanemu prawach i ciążących na nim obowiązkach związanych z dozorem elektronicznym, jak również o konsekwencjach naruszenia tych obowiązków (Dz.U. 2016 poz. 1692);
- Rozporządzenie Ministra Sprawiedliwości z dnia 10 października 2016 r. w sprawie sposobu oraz szczegółowych warunków wykonywania kar, środków karnych i środków zabezpieczających w systemie dozoru elektronicznego (Dz.U. 2016 poz. 1698);
- Rozporządzenie Ministra Sprawiedliwości z dnia 10 października 2016 r. w sprawie sposobu i trybu sprawowania nadzoru nad wykonywaniem dozoru elektronicznego (Dz.U. 2016 poz. 1700).

System dozoru elektronicznego – kwestie terminologiczne.

Definicja dozoru elektronicznego oraz systemu dozoru elektronicznego zawarta została w art. 43b. § 1 i 2 KKW. Dozór elektroniczny to monitorowanie zachowania osoby oddanej pod dozór przy wykorzystaniu środków technicznych. System dozoru elektronicznego (dalej SDE) natomiast, jest

ogółem sposobów postępowania oraz środków technicznych, które służą wykonywaniu dozoru elektronicznego.
Dozór elektroniczny można stosować jako:

- środek zabezpieczający – elektroniczna kontrola miejsca pobytu. Stanowi o tym art. 93a. § 1. pkt 1 Ustawy z dnia 6 czerwca 1997 roku - Kodeks karny (Dz.U. 1997 nr 88 poz. 553 z późn. zm.) – dalej KK,
- wybrany środek karny - zakaz zbliżania się do określonych osób (art. 41a. § 1 i 2 KK) oraz zakaz wstępu na imprezę masową za czyn popełniony w związku z masową imprezą sportową (art. 41a. § 3 KK),
- karę pozbawienia wolności.

W SDE kontrolować można przebywanie przez skazanego w określonym miejscu i czasie (dozór stacjonarny), bieżące miejsce pobytu skazanego (dozór mobilny) oraz przestrzeganie zakazu zbliżania się skazanego do określonej osoby na wyznaczoną minimalną odległość (dozór zbliżeniowy). Jako dozór stacjonarny wykonuje się karę pozbawienia wolności w SDE. Dozór mobilny lub zbliżeniowy natomiast stosuje się w przypadku środków karnych i zabezpieczających (KKW: art. 43b. § 3, art. 43c. § 1). Z uwagi na to, iż stosowanie dozoru elektronicznego jako środek zabezpieczający lub środek karny występuje rzadziej niż kara pozbawienia wolności w SDE, dalsze rozważania w tym zakresie zostaną pominięte.

Warunki i tryb orzekania o udzieleniu skazanemu zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego.
Wykonywanie kary pozbawienia wolności w systemie dozoru elektronicznego jest możliwe w przypadku, gdy:

- wobec skazanego orzeczono karę pozbawienia wolności (również zastępczą karę pozbawienia wolności), która nie przekracza 1 roku, a sprawca nie popełnił przestępstwa w warunkach recydywy,
- jest to dostateczna forma osiągnięcia celów kary,
- skazany dysponuje ustalonym miejscem stałego pobytu,
- wspólnie zamieszkujące ze skazanym pełnoletnie osoby wyraziły pisemną zgodę na tę formę kary oraz dokonywanie czynności kontrolnych przez upoważniony podmiot dozorujący,

- umożliwiają to warunki techniczne, które obejmują w szczególności liczbę i zasięg dostępnych rejestratorów oraz nadajników, a także organizacyjne możliwości ich obsługi.

Zezwolenia na odbycie kary pozbawienia wolności w systemie dozoru elektronicznego może udzielić skazanemu sąd penitencjarny, jeżeli spełnione zostały wszystkie wyżej wymienione warunki (KKW: art. 43la. § 1, art. 43lb.). Wniosek o zezwolenie na odbywanie kary pozbawienia wolności w SDE może złożyć skazany, jego obrońca, prokurator lub sądowy kurator zawodowy, a w przypadku skazanych osadzonych w jednostce penitencjarnej – również dyrektor zakładu karnego. Do wniosku należy dołączyć pisemną zgodę wszystkich pełnoletnich osób zamieszkujących we wskazanym miejscu, w którym kara ma być wykonywana (dalej zgoda). Chodzi o osoby, które fizycznie zamieszkują w danym miejscu, a nie osoby formalnie zameldowane. Po wydaniu postanowienia o udzieleniu zezwolenia na wykonywanie kary w SDE, cofnięcie zgody jest nieskuteczne. Sąd penitencjarny może – pomimo braku zgody – zezwolić na odbycie kary pozbawienia wolności w SDE, jeśli jej wykonanie w oczywisty sposób nie sprawia nadmiernych problemów dla osoby, która nie wyraziła tej zgody, a jej prywatność naruszana jest w stopniu nieznacznym. W przypadku, gdy wniosek składa dyrektor zakładu karnego, sąd penitencjarny zleca kuratorowi sądowemu przeprowadzenie wywiadu środowiskowego w miejscu stałego pobytu skazanego. Sądowy kurator zawodowy może zlecić wykonanie tej czynności sądowemu kuratorowi społecznemu. W trakcie wywiadu, kurator sądowy może odebrać oświadczenie o zgodzie na odbywanie przez skazanego kary pozbawienia wolności w systemie dozoru elektronicznego (KKW: art. 43h. § 3, 4, 5 i 8, art. 43la. § 4, art. 43lc., art. 43ld. § 3). W Kodeksie Karnym Wykonawczym brak jest przepisów, które odnosiłyby się do niektórych sytuacji, np. gdy właścicielem lokalu jest osoba niezamieszkująca ze skazanym. Z uwagi na to, iż zainstalowanie środków technicznych może wiązać się z koniecznością dokonania jakichś zmian w domu/mieszkaniu, sąd penitencjarny prosi o zgodę właściciela lokalu. Podobną, nieunormowaną kwestię stanowi zamieszkanie skazanego w placówce udzielającej zakwaterowania dla wielu osób, np. w schronisku dla bezdomnych. W takim przypadku uzyskanie pisemnej zgody od wszystkich osób pełnoletnich

wspólnie zamieszkujących często nie jest możliwe. Ze względu na to, w praktyce nie jest to wymagane, a zgodę udziela wyłącznie dyrektor placówki.
Zezwolenia na odbycie kary pozbawienia wolności w SDE można udzielić skazanemu, jeśli jego stopień demoralizacji, względy bezpieczeństwa i inne okoliczności nie wskazują na konieczność osadzenia go w zakładzie karnym. W przypadku osób już osadzonych bierze się pod uwagę jego dotychczasowa postawę i zachowanie. Przed wydaniem postanowienia, sąd penitencjarny żąda od upoważnionego podmiotu dozorującego nadesłania informacji w sprawie ewentualnego braku możliwości spełnienia wymaganych warunków technicznych. W przypadku wystąpienia barier technicznych, wniosek pozostawia się bez rozpoznania. (KKW: art. 43la. § 2 i 3, art. 43lf. § 1 i 2).
W postanowieniu o udzieleniu skazanemu zezwolenia na odbycie kary pozbawienia wolności w SDE, wskazuje się czas, miejsce, rodzaj lub sposób wykonywania orzeczonych obowiązków, a także rodzaj środków technicznych, które mają zostać zainstalowane. Skazanemu wyznacza się termin i sposób zgłoszenia upoważnionemu podmiotowi dozorującemu gotowości do zainstalowania wskazanych w postanowieniu środków, o czym zawiadamia się sądowego kuratora zawodowego (jeśli nie uczestniczył w posiedzeniu) oraz podmiot dozorujący doręczając im odpis postanowienia. Termin ten nie może być dłuższy niż 24 godziny i biegnie od momentu zwolnienia z zakładu karnego (jeżeli dotyczy osadzonego) lub ogłoszenia/doręczenia postanowienia (jeżeli dotyczy skazanych nieprzebywających w zakładzie karnym). Na postanowienie o udzieleniu lub odmowie udzielenia zezwolenia przysługuje zażalenie. W przypadku odmowy udzielenia zezwolenia, ponowne rozpatrzenie wniosku w tej samej sprawie jest możliwe wtedy, gdy skazany lub jego obrońca złoży wniosek po upływie 3 miesięcy od dnia wydania postanowienia (KKW: art. 43k. § 2 zdanie pierwsze, art. 43lh. § 1, 3 i 4, art. 43lj. § 1, art. 43lk., art. 43ll.). Ze względu na 3-miesięczny okres karencji ponownej możliwości wnioskowania o zezwolenie na odbycie kary pozbawienia wolności w SDE, zdarza się niejednokrotnie, iż wnioskodawca wycofuje wniosek i składa go ponownie w momencie, gdy – z uwagi na określone okoliczności – prawdopodobieństwo udzielenia zezwolenia jest większe.

1.8. System dozoru elektronicznego w Polsce

Organizowanie i kontrolowanie wykonywania kary pozbawienia wolności w systemie dozoru elektronicznego.

Nadzór nad wykonywaniem kary pozbawienia wolności w SDE sprawuje sąd penitencjarny, który kontroluje i ocenia:

- legalność oraz prawidłowość wykonywania kary,
- poprawność przeliczania okresów wykonywania kary,
- realizowanie działalności wychowawczej i zadań probacyjnych sądowego kuratora zawodowego oraz przebieg procesu resocjalizacji osoby skazanej,
- funkcjonowanie upoważnionego podmiotu dozorującego w obszarze realizowania obowiązków przez osobę skazaną,
- kolejność wykonywania orzeczeń, a także prawidłowość powiadamiania o warunkach technicznych umożliwiających niezwłoczne rozpoczęcie wykonania kary lub zawiadamiania o terminie, od którego będzie to możliwe (art. 43d. KKW).

Organizowaniem i kontrolowaniem wykonywania kary pozbawienia wolności w SDE oraz nałożonych w związku z tym obowiązków zajmuje się sądowy kurator zawodowy (art. 43d. KKW). Realizowanie nałożonych na skazanego obowiązków podlega dokładnej kontroli i ma na celu oddziaływanie wychowawcze i zapobieganie powrotności do przestępczości (Kotowski 2009, s. 20). Przy wykonywaniu czynności służbowych, sądowy kurator zawodowy – w celu zapewnienia sobie bezpieczeństwa – może żądać pomocy Policji (Art. 9 Ustawy z dnia 27 lipca 2001 r. o kuratorach sądowych - Dz.U. 2001 nr 98 poz. 1071 z późn. zm.; § 8 Rozporządzenia Ministra Sprawiedliwości z dnia 10 października 2016 r. w sprawie sposobu oraz szczegółowych warunków wykonywania kar, środków karnych i środków zabezpieczających w systemie dozoru elektronicznego – Dz.U. 2016 poz. 1698).

Merytoryczny i techniczny nadzór nad funkcjonowaniem SDE sprawuje Biuro Dozoru Elektronicznego (dalej BDE), którego siedziba znajduje się przy ul. Zwycięzców 34 w Warszawie. Dyrektorem biura jest gen. Paweł Nasiłowski, jeden z pomysłodawców i architektów systemu. BDE jest ponadto odpowiedzialne za administrowanie i obsługę centrali monitorowania, która stanowi element SDE. Zespół Obsługi Centrali Monitorowania (dalej Zespół) rejestruje, gromadzi, przetwarza, przechowuje, odtwarza i zabezpiecza dane

osobowe oraz inne informacje o przebiegu kary dotyczące skazanych objętych SDE. Dane te i informacje przekazywane są uprawnionym organom. Zespół współpracuje również z podmiotami odpowiedzialnymi za krajową infrastrukturę energetyczną i telekomunikacyjną oraz utrzymuje telefoniczny kontakt z osobami poddanymi monitorowaniu. BDE jest ponadto odpowiedzialne za opracowywanie projektów aktów prawnych dotyczących tego systemu, prowadzenie statystyk związanych z SDE, współpracę z sędziami penitencjarnymi, prokuratorami, adwokatami, sądowymi kuratorami zawodowymi i właściwymi jednostkami organizacyjnymi Ministerstwa Sprawiedliwości. Do zakresu działań BDE należy ponadto organizowanie szkoleń dotyczących SDE oraz prowadzenie działań informacyjnych i promujących stosowanie SDE[38]. Na stronie Biura Dozoru Elektronicznego[39] znajdują się liczne informacje systemie, dane statystyczne, akty prawne, wzór wniosku o zezwolenie zgody na wykonywanie kary pozbawienia wolności w SDE, oświadczenie-zgoda pełnoletnich osób wspólnie zamieszkujących ze skazanym. Ponadto, istnieje możliwość pobrania ulotki informacyjnej, a także informatora dla osoby oddanej pod dozór elektroniczny, który dostępny jest w języku polskim, angielskim, niemieckim, francuskim i rosyjskim.

Środkami technicznymi, które służą wykonywaniu dozoru elektronicznego są nadajniki, stacjonarne i przenośne rejestratory, centrala monitorowania i system teleinformatyczny (komunikacyjno-monitorujący) umożliwiający przetwarzanie informacji związanych z organizowaniem i kontrolowaniem wykonywania kary pozbawienia wolności w SDE. System teleinformatyczny stanowi środek komunikacji między podmiotem prowadzącym centralą monitorowania, upoważnionym podmiotem dozorującym, sądami, sądowymi kuratorami zawodowymi oraz innymi uprawnionymi podmiotami. Wewnątrz systemu przekazywane są często dane wrażliwe. Zagwarantowanie poprawnego funkcjonowania systemu dozoru elektronicznego jest konieczne dla ochrony danych personalnych i innych informacji przed ujawnieniem ich osobom do tego nieuprawnionym (art. 43f. § 1 i 2 KKW). System komunikacyjno-monitorujący opracowany został przez polskie konsorcjum IMPEL - ITM POLAND - SMT

[38] http://www.sw.gov.pl/jednostka/biuro-dozoru-elektronicznego - dostęp 16.06.2017.
[39] http://www.dozorelektroniczny.gov.pl/

SOFTWARE - EBS. Prawa własności posiada Ministerstwo Sprawiedliwości, co niewątpliwie podnosi bezpieczeństwo systemu, który nie jest zależny od podmiotów pośrednich.[40] Aby móc uzyskać dostęp do systemu teleinformatycznego należy posiadać certyfikat użytkownika w SDE, oprogramowanie obsługujące certyfikat i kartę kryptograficzną z kodem PIN. Certyfikat jest wydawany na okres 5 lat z możliwością jego przedłużenia lub wcześniejszego unieważnienia. Przy logowaniu do SDE, należy umieścić kartę w czytniku i wpisać kod PIN[41].

Rozporządzenie Ministra Sprawiedliwości z dnia 26 maja 2015 r. w sprawie określenia szczegółowych warunków technicznych i wymagań funkcjonalnych, jakie powinny spełniać środki techniczne służące do wykonywania dozoru elektronicznego, oraz sposobu funkcjonowania systemu komunikacyjno-monitorującego (Dz.U. 2015 poz. 797) – dalej Rozporządzenie MS z dnia 26 maja 2015 r. – to akt wykonawczy, w którym znajdują się wytyczne odnośnie m.in. rejestratora stacjonarnego, jak i nadajnika. Rejestrator stacjonarny to radiowe urządzenie, instalowane w miejscu wykonywania kary, które rejestruje wysyłane przez pozostający w zasięgu monitorowania nadajnik komunikaty. Informacje te przekazywane są do centrali monitorowania. Urządzenie wyposażone jest w dwa przyciski umożliwiające uzyskanie połączenia z centralą monitorowania oraz numerem alarmowym 112. Każdy rejestrator stacjonarny spełnia następujące funkcje:

- posiada możliwość regulacji zasięgu monitorowania w sposób, który dopasowuje zasięg ściśle do miejsca wykonywania kary,
- identyfikuje każdy – pozostający w jego zasięgu – nadajnik, a także rejestruje każdy przypadek manipulowania przy urządzeniu lub nadajniku. Urządzenie zapisuje wszystkie pozostałe zdarzenia, które podlegają rejestracji. Informacje dotyczące zarejestrowanych zdarzeń przechowywane są w pamięci rejestratora przez co najmniej 72 godziny (w przypadku awarii energetycznej lub sieci telekomunikacyjnej, po przywróceniu pełnej sprawności rejestrator przesyła wszystkie informacje do centrali monitorowania),

[40]Informacje uzyskane w rozmowie telefonicznej z pracownikiem Biura Dozoru Elektronicznego.
[41] http://sde24.pl/Repozytorium/PolitykaCertyfikacjiSDE.pdf - dostęp 16.06.2017.

- posiada interfejs zezwalający na odczytanie i przekazanie danych dotyczących zdarzeń, które podlegają rejestracji, jak również sygnałów o przeczytaniu wiadomości,
- przekazuje w czasie rzeczywistym do centrali monitorowania przy wykorzystaniu publicznej sieci telekomunikacyjnej (§ 1 pkt 7, § 4 pkt 2-6 Rozporządzenia MS z dnia 26 maja 2015 r.).

Rejestrator stacjonarny jest niezwykle czuły, dlatego przy instalowaniu środków technicznych, poucza się skazanych i inne osoby, iż nie należy przestawiać/przesuwać urządzenia. Umiejscowienie urządzenia w mieszkaniu pełni kluczową rolę. Zdarza się bowiem, iż rejestrator zainstalowany w bezpośredniej bliskości od źródła dźwięku, generuje zdarzenia i konieczna jest wtedy interwencja telefoniczna centrali monitorowania. Zaleca się, aby rejestrator nie był w ogóle dotykany – nawet w przypadku wystąpienia potrzeby wytarcia z kurzu.

Rysunek 18. System dozoru elektronicznego

Źródło:http://www.sw.gov.pl/assets/50/81/72/500fceb20eff749955ce608325c39467f9ec15d7.pdf

Zainstalowany w wodoodpornej i antyalergicznej opasce nadajnik mocowany jest zazwyczaj na nodze lub przegubie dłoni. Urządzenie wyglądem przypomina

zegarek. W razie nieobecności lub spóźnienia, urządzenie monitorujące – rejestrator stacjonarny – natychmiast przesyła informację o tym zdarzeniu do centrali monitorowania, która szczegółowo rejestruje przebieg kary. O każdej tego typu sytuacji, informowany jest także sędzia penitencjarny i zawodowy kurator sądowy[42]. Nadajnik musi wskazywać każdy przypadek manipulowania nim(§ 3 Rozporządzenia MS z dnia 26 maja 2015 r.).Dane osobowe skazanego (imię, nazwisko, numer PESEL – a w przypadku braku – numer paszportu lub innego dokumentu tożsamości oraz zarejestrowane informacje związane z wykonywaniem kary pozbawienia wolności w SDE) przechowuje i archiwizuje podmiot dozorujący. Odbywa się to w sposób, który gwarantuje ich bezpieczeństwo przez 2-letni okres od momentu ich uzyskania. Dane te mogą być przekazane Policji i przez nią przetwarzane jedynie w celu zapobiegania lub wykrywania przestępstw lub przestępstw skarbowych (art. 43x. KKW). Po upływie okresu 2 lat od momentu uzyskania danych, podmiot dozorujący przekazuje je do sądu, który wydał postanowienia o zezwoleniu na odbycie kary pozbawienia wolności w SDE. Jeżeli zapis danych jest prawidłowy, nośnik dołączany jest do akt sprawy, a wszelkie zgromadzone w systemie teleinformatycznym dane są trwale usuwane (§ 5 i 7 Rozporządzenie Ministra Sprawiedliwości z dnia 28 maja 2015 r. w sprawie sposobu archiwizowania oraz sposobu i trybu usuwania danych osobowych i informacji zarejestrowanych w związku z wykonywaniem dozoru elektronicznego – Dz.U. 2015 poz. 800).
Centralę monitorowania prowadzi podmiot dozorujący lub jednostka organizacyjna, która podlega Ministrowi Sprawiedliwości. Wyboru podmiotu dozorującego dokonuje Minister Sprawiedliwości. Czyni to w trybie określonym w Ustawie z dnia 29 stycznia 2004 roku – Prawo zamówień publicznych (Dz.U. z 2015 t. poz. 2164 z późn. zm,). Podmiotem tym może być instytucja państwowa, przedsiębiorca lub podmiot zagraniczny, który spełnia warunki do prowadzenia w Polsce działalności gospodarczej, a w rozumieniu prawa kraju rejestracji jest przedsiębiorcą (art. 43g. KKW). Czynności terenowe wykonują dwuosobowe patrole. Inspektorzy jeżdżą oznakowanymi pojazdami

[42] http://www.dozorelektroniczny.gov.pl/?page_id=18 – dostęp 16.06.2017.

służbowymi, są umundurowani i posiadają legitymacje służbowe, których wzór został zatwierdzony przez Ministerstwo Sprawiedliwości[43].

Obowiązki i prawa skazanego.

Skazany, któremu udzielono zezwolenia na odbycie kary pozbawienia wolności w SDE zostaje pouczony o obowiązkach, które z tego wynikają i przysługujących mu prawach. Kwestia ta uregulowana została w Oddziale 3 rozdziału VIIa KKW. Pierwszym z obowiązków, który ciąży na osobie skazanej jest konieczność zgłoszenia podmiotowi dozorującemu gotowości do zainstalowania środków technicznych. Należy tego dokonać w terminie i w sposób określony w postanowieniu. W przypadku, gdy skazany tego nie uczyni lub uchyla się od instalacji środka technicznego, podmiot dozorujący niezwłocznie powiadamia o tym fakcie sąd oraz sądowego kuratora zawodowego (art. 43m. § 1 i 3 KKW).

Kolejnymi istotnymi obowiązkami są:

- nieprzerwane noszenie nadajnika,
- dbanie o powierzone środki techniczne (ochrona przed zniszczeniem, uszkodzeniem, utratą lub uczynieniem niezdatnymi do użytku) oraz zapewnienie stałego zasilania energią elektryczną,
- udostępnianie podmiotowi dozorującemu środków technicznych do kontroli, wymiany lub naprawy. Kontrola techniczna dokonywana może być między godziną 6:00 a 22:00. W nagłych sytuacjach, kontrola może nastąpić poza tymi godzinami,
- udzielanie prezesowi sądu/upoważnionemu sędziemu, sądowemu kuratorowi zawodowemu, podmiotowi prowadzącemu centralę monitorowania, podmiotowi dozorującemu wyjaśnień odnośnie przebiegu odbywania kary oraz wykonywania nałożonych obowiązków, a także stawianie się na wezwania sędziego i kuratora,
- pozostawanie w wyznaczonym przez sąd miejscu w określonym czasie. Sąd penitencjarny ustala przedziały czasu, w których osoba skazana ma prawo oddalić się z miejsca wykonywania kary na okres maksymalnie 12 godzin dziennie, zwłaszcza w celu świadczenia pracy, wykonywania

[43] http://www.dozorelektroniczny.gov.pl/?page_id=54 – dostęp 16.06.2017.

praktyk religijnych, sprawowania opieki nad osobą małoletnią/niedołężną/chorą, kształcenia i samokształcenia, realizowania własnej twórczości, dokonania niezbędnych zakupów, komunikowania się z obrońcą, udziału w terapii lub korzystania z opieki medycznej,
- umożliwianie sądowemu kuratorowi zawodowemu wejścia do miejsca, gdzie został zainstalowany rejestrator (KKW: art. 43n., art. 43na., art. 43v. § 5).

Skazany jest nadto zobowiązany do odbierania połączeń przychodzących do rejestratora stacjonarnego. W czasie, gdy osoba skazana powinna przebywać w miejscu wykonywania kary, w sytuacji nieodebrania przez niego połączenia przychodzącego, do systemu teleinformatycznego wprowadza się informację o tym zdarzeniu. Stanowi o tym §4 pkt 3 Rozporządzenia Ministra Sprawiedliwości z dnia 10 października 2016 r. w sprawie sposobu oraz szczegółowych warunków wykonywania kar, środków karnych i środków zabezpieczających w systemie dozoru elektronicznego (Dz.U. 2016 poz. 1698).
Na skazanego, który odbywa karę pozbawienia wolności w SDE sąd penitencjarny może nałożyć obowiązki probacyjne wskazane w art. 72 KK. Wnioskować może o to prokurator lub sądowy kurator zawodowy. Obowiązki mogą być w każdym momencie rozszerzane lub modyfikowane. Istnieje ponadto możliwość zwolnienia od orzeczonych obowiązków, za wyjątkiem obowiązku przeproszenia pokrzywdzonego (art. 43nb. KKW).
W uzasadnionych przypadkach, istnieje możliwość zmiany miejsca wykonywania dozoru stacjonarnego oraz przedziałów czasu, w których skazany może pozostawać poza miejscem odbywania kary. Decyzję o tego typu zmianach podejmuje sąd penitencjarny. W sytuacji, gdy zachodzi konieczność szybkiego dokonania zmian, wyżej wymienione przedziały czasu mogą być zmodyfikowane przez sądowego kuratora zawodowego, który niezwłocznie powiadamia o tym sędziego penitencjarnego i zamieszcza informację w systemie teleinformatycznym. Sąd penitencjarny może uchylić te zmiany lub dokonać własnej modyfikacji (art. 43o. § 1, 3 i 4 KKW).
W szczególnie istotnych dla osoby skazanej sytuacjach, uzasadnionych względami osobistymi, zdrowotnymi lub rodzinnymi, sądowy kurator zawodowy może udzielić skazanemu zgody na opuszczenie miejsca odbywania

kary na czas, który nie przekracza jednorazowo 7 dni. Pożądanym (lecz niekoniecznym) jest, aby osobie skazanej asystowała osoba najbliższa lub osoba godna zaufania. Kurator, który podjął taką decyzję, niezwłocznie powiadamia o tym prezesa sadu, upoważnionego sędziego lub sędziego penitencjarnego i wprowadza informację do systemu teleinformatycznego. Jeżeli po udzieleniu zezwolenia wystąpiły okoliczności, które mogłyby wskazywać na zwiększone prawdopodobieństwo naruszenia przez skazanego porządku prawnego, zgoda na opuszczenie miejsca wykonywania kary może zostać cofnięta. W przypadku, gdy zezwolenie zostało cofnięte, osobie skazanej nie udziela się ponownie takiej zgody (art. 43p. KKW).

W sytuacji zagrożenia życia lub zdrowia ludzkiego, sądowy kurator zawodowy może podjąć decyzję o usunięciu nadajnika lub odinstalowaniu rejestratora stacjonarnego. W terminie 7 dni od tej decyzji, prezes sądu lub upoważniony sędzia zarządza ponowne założenie nadajnika lub zainstalowanie rejestratora albo występuje do sądu o zarządzenie przerwy w wykonaniu kary (art. 43r. KKW).

Jak wcześniej wspomniano, jednym z obowiązków skazanego jest dbanie o powierzone środki techniczne. W przypadku umyślnego uszkodzenia nadajnika i/lub rejestratora stacjonarnego, sąd może nałożyć na osobę skazaną opłatę wyrównawczą w wysokości 379 zł (dla nadajnika) i/lub 2164 zł (dla rejestratora stacjonarnego). Kwotę tę należy uiścić na rzecz podmiotu dozorującego. Opłaty nie orzeka się po upływie 6 miesięcy od momentu zdarzenia (art. 43s. § 1, 3 i 4 KKW).

Zakończenie dozoru elektronicznego.

Karę pozbawienia wolności wykonywaną w systemie dozoru elektronicznego uznaje się za wykonaną z chwilą zakończenia dozoru, chyba że zezwolenie na odbycie kary w SDE zostało uchylone (art. 43za. § 1 KKW). Odwołanie tej zgody następuje w przypadku, gdy:

- skazany nie zgłosi podmiotowi dozorującemu w wyznaczonym terminie gotowości do zainstalowania środków technicznych lub uchyla się od niezwłocznej instalacji rejestratora, bądź założenia nadajnika,
- w trakcie odbywania kary skazany naruszył porządek prawny, zwłaszcza gdy popełnił przestępstwo lub przestępstwo skarbowe, bądź uchyla się

od wykonania nałożonych obowiązków, orzeczonego środka karnego, kompensacyjnego lub przepadku,
- przerwa w wykonaniu kary została odwołana z innego powodu niż ustanie przyczyny, z uwagi na którą udzielono przerwy,
- w trakcie wykonywania kary skazany został tymczasowo aresztowany lub osadzony w zakładzie karnym w związku ze skazaniem w innej sprawie.

W wyjątkowych przypadkach, sąd penitencjarny może zrezygnować z uchylenia zezwolenia. W razie uchylenia zezwolenia na odbycie kary pozbawienia wolności w SDE, oblicza się pozostały do wykonania okres kary pozbawienia wolności i zawiadamia o tym skazanego. Sąd penitencjarny zarządza doprowadzenie skazanego do zakładu karnego. Ponowne udzielenie zezwolenia na odbycie kary w SDE w tej samej sprawie nie jest możliwe (KKW: art. 43zaa. § 1 i 2, art. 43zac., art. 43zad., art. 43zae.).

Powyżej wskazane przesłanki na uchylenie zezwolenia mają charakter obligatoryjny. Art. 43zab. KKW stanowi natomiast, iż jeśli skazany nie wrócił do miejsca wykonywania kary w wyznaczonym czasie, sąd penitencjarny może uchylić zezwolenie. W praktyce najczęściej dzieje się tak, iż sądowy kurator zawodowy przeprowadza ze skazanym rozmowę ostrzegawczą, poznaje powód naruszenia i przekazuje tę informację sędziemu penitencjarnemu, który podejmuje adekwatną decyzję w sprawie. Sądowy kurator zawodowy wprowadza do systemu teleinformatycznego informację o każdym naruszeniu porządku prawnego lub nałożonego obowiązku.[44] Obowiązkiem skazanego jest powiadamianie sądowego kuratora zawodowego i/lub centrali monitorowania w związku z każdą nieobecnością w miejscu wykonywania kary w wyznaczonym czasie. Pracownicy centrali monitorowania pełnią dyżury i w każdej chwili – całą dobę – osoba skazana może porozmawiać z osobą, sprawującą nadzór nad wykonaniem kary[45].

Wobec skazanych odbywających karę pozbawienia wolności w systemie dozoru elektronicznego (nie dotyczy zastępczej kary pozbawienia wolności za przestępstwo lub przestępstwo skarbowe), sąd penitencjarny może zastosować warunkowe przedterminowe zwolnienie. Wnioskować o to może

[44] http://www.dozorelektroniczny.gov.pl/?page_id=50).
[45] http://www.dozorelektroniczny.gov.pl/?page_id=18.

także sądowy kurator zawodowy. W sytuacji skorzystania z instytucji warunkowego przedterminowego zwolnienia, uchyla się zezwolenie na odbycie kary w SDE (art. 43 ln. KKW).
Kluczowym momentem czasowym w obliczaniu wykonania kary pozbawienia wolności w SDE jest instalacja środków technicznych (początek dozoru elektronicznego) i ich deinstalacja (zakończenie dozoru elektronicznego).

System dozoru elektronicznego w liczbach.
Z danych zamieszczonych na stronie BDE wynika, iż do dnia 30.04.2017 r. karę[46] w SDE odbyło 56179 skazanych. W tym czasie system objął łącznie 60845 osoby[47]. Aktualnie dostępna pojemność systemu wynosi 15000 miejsc. W dniu 31.05.2017 roku karę w SDE odbywało 4551 skazanych. Wolnych miejsc pozostawało wówczas 10449, co oznaczało wykorzystanie systemu w 30,3%[48]. Kara w systemie dozoru elektronicznego wykonywana jest w zdecydowanej większości wobec mężczyzn. W maju 2017 roku, udział procentowy kobiet w populacji skazanych w SDE wynosił 7.6%, podczas gdy w przypadku populacji osadzonych w ZK/AŚ[49] udział ten wyniósł 3,6%[50]. Na dzień 31.05.2017 do SDE liczba potencjalnych „kandydatów" do SDE wyniosła łącznie 30535 skazanych – w tym 9996 osadzonych w ZK/AŚ[51].

[46] Wszelkie dane statystyczne zgromadzone na stronie Biura Dozoru Elektronicznego, odnoszą się do osób, wobec których wykonywano karę pozbawienia wolności, środek karny lub środek zabezpieczający. Informacji tych udzielił pracownik BDE, odpowiedzialny za zbieranie i analizę danych statystycznych. Terminu „kara" nie można utożsamiać zatem w tym przypadku wyłącznie z karą pozbawienia wolności, a „skazany" może w tym przypadku również oznaczać podejrzanego lub oskarżonego.
[47] http://www.sw.gov.pl/assets/22/14/77/288103de1e84b021bbd946b0f0a063a650bbda89.pdf - dostęp 16.06.2017
[48] http://www.sw.gov.pl/assets/85/57/82/cb633cd8b291b9c58b80ddf40f7d597a7d91007f.pdf - dostęp 16.06.2017
[49] Zakład Karny/Areszt Śledczy.
[50] http://www.sw.gov.pl/assets/48/00/89/4da5d51548c25fb796040f4fc45b5e431bfa56f1.pdf - dostęp 16.06.2017
[51] http://www.sw.gov.pl/assets/37/63/62/bf088ac03b4beb5926f552752e690b9faaa0651f.pdf - dostęp 16.06.2017.

System dozoru elektronicznego – zalety jego stosowania.

Odbywanie kary w SDE opiera się na odpowiedzialności i samodyscyplinie skazanych oraz dokładnym respektowaniu harmonogramu określonego przez sąd. Wśród zalet wykonywania kary pozbawienia wolności w SDE wymienić można:

- brak rygoru panującego w izolacji więziennej,
- aktywność zawodowa – możliwość zarabiania na utrzymanie siebie i swoich bliskich,
- możliwość kształcenia/dokształcania się,
- utrzymywanie relacji z osobami bliskimi, sposobność czynnego uczestnictwa w ich życiu,
- brak skrępowania w korzystaniu z dostępu do informacji i dóbr kultury[52],
- mniejsza ingerencja w sferę prywatności (Kotowski 2009, s. 17),
- redukcja kosztów (Moczydłowski 2006, s. 164),
- zmniejszenie populacji więziennej.

Podsumowanie

Kara pozbawienia wolności stanowi najsurowszą reakcję prawną na naruszenie porządku prawnego. Powinna być stosowana w ostateczności – gdy orzeczenie innej kary nie jest możliwe z uwagi na przewidywaną niską skuteczność w zapobieganiu powrotności do przestępstwa. Jest to zgodne z zaleceniami podmiotów międzynarodowych odnośnie pierwszeństwa kar wolnościowych. Możliwość odbywania kary pozbawienia wolności w systemie dozoru elektronicznego sprawia, iż brak jest niekorzystnych efektów społecznych wynikających z izolacji. Osoba odbywająca tę karę w warunkach wolnościowych pozostaje w kontakcie z osobami bliskimi i nie jest zmuszona do przerwy w nauce lub pracy. Ryzyko demoralizacji skazanych oraz degradacji ekonomicznej jest tutaj mniejsze, niż gdyby kara była wykonywana w warunkach izolacji więziennej. Z drugiej strony, zapewnienie bezpieczeństwa dla ogółu społeczeństwa zdaje się być w takim przypadku trudniejsze.

[52] http://www.sw.gov.pl/assets/37/63/62/bf088ac03b4beb5926f552752e690b9faaa0651f.pdf - dostęp 16.06.2017.

Wprowadzenie do polskiego postępowania karnego wykonawczego możliwości odbywania kary pozbawienia wolności w systemie dozoru elektronicznego stanowiło odpowiedź na problem przeludnienia więzień. Niejednokrotnie zdarzało się tak, iż osoba skazana musiała czekać na osadzenie w jednostce penitencjarnej, w wyniku czego społeczeństwo mogło postrzegać to jako niesprawiedliwość. System dozoru elektronicznego odciążył w pewnym zakresie system więziennictwa i zwiększył skuteczność procesu resocjalizacji. W warunkach przeludnienia nie ma bowiem możliwości indywidualnego oddziaływania na osadzonych, gdyż należy zapewnić wtedy porządek wewnątrz jednostki i dopilnować, aby żaden ze skazanych nie zbiegł z zakładu karnego / aresztu śledczego. Pozytywnym aspektem jest również to, iż wykonanie kary pozbawienia wolności w SDE stanowi tańszą alternatywę dla kary stosowanej w warunkach pełnej izolacji.

Niewątpliwym atutem jest to, iż system komunikacyjno-monitorujący opracowany został przez polskie konsorcjum, a prawa własności posiada Ministerstwo Sprawiedliwości. Aktualna pojemność systemu wynosi 15000 miejsc, jednakże istnieje możliwość jej rozszerzenia. Fakt, iż system teleinformatyczny jest niezależny od wpływu zagranicznych podmiotów pośrednich podnosi znacząco jego bezpieczeństwo i ogranicza koszty związane z jego obsługą i utrzymaniem.

W niniejszym opracowaniu poruszono najważniejsze zagadnienia dotyczące wykonywania kary pozbawienia wolności w systemie dozoru elektronicznego. Z uwagi na klauzule tajności, część danych nie mogła zostać tu przedstawiona.

1.9. Wybrane problemy bezpieczeństwa systemów do zdalnej automatycznej identyfikacji opartej na RFID

Wstęp

Automatyczna zdalna identyfikacja pełni kluczową rolę w funkcjonowaniu większości organizmów żywych jak i systemów technicznych. Głównym założeniem tej techniki identyfikacji obiektów jest zdalne ich rozpoznawanie na podstawie unikalnych, charakterystyczny cech lub odczytanie cech, wartości dołączonych do nich „identyfikatorów". W celu realizacji takiego procesu, system rozpoznający musi być wyposażony w odpowiedni czytnik, do obserwacji na odległość oraz analizator z bazą danych, który na podstawie wartości parametrów identyfikacyjnych odnajduje w tej bazie właściwą pozycję. Istotne są tutaj ograniczenia w działaniu takiego „czytnika", cechy identyfikatora, skuteczność analizatora oraz zawartość bazy danych systemu do zdalnej identyfikacji.

Systemy automatycznej zdalnej identyfikacji, w odniesieniu do organizmów biologicznych, pełnią istotną rolę w ich przetrwaniu i stanowią często funkcjonalny wzorzec dla rozwiązań stosowanych w środowisku technicznym. Posiadają także niedoskonałości, związane z ograniczeniami działania ich komponentów, które często znacząco wpływają na bezpieczeństwo systemu korzystającego z takiego rozwiązania. W sferze biologicznej mogą to być na przykład systemy automatycznej identyfikacji osobników za pomocą znacznika zapachowego lub graficznego, które łatwo oszukać poprzez podstawienie własnego obiektu wyposażonego w kopię identyfikatora, np. użycie takiego samego zapachu jak znacznik biologicznego jest często stosowane przez myśliwych. W takim przypadku, system automatycznej zdalnej identyfikacji oparty na ograniczonej liczbie znaczników, bez możliwości bezpośredniej weryfikacji wyniku procesu identyfikacji zawodzi, dokonując niewłaściwego rozpoznania obiektu.

Właśnie dlatego, wprowadzając systemy automatycznej identyfikacji do rozwiązań technicznych bardziej należy koncentrować się na specyfice

i niedoskonałościach ich działania niż na oferowanych funkcjonalnościach. Z drugiej strony rozwiązań dotyczących wykorzystania słabości takich systemów, także można szukać w systemach biologicznych, które natura odpowiednio ukształtowała na drodze ewolucji.

Najciekawszymi i najdynamiczniej rozwijającymi się technicznymi systemami zdalnej automatycznej identyfikacji są obecnie systemy RFID (*ang. Radio Frequency IDentification*) stosowane w szerokim zakresie niemal we wszystkich dziedzinach życia. Bezkrytyczne wdrażanie tej technologii jest jednak coraz bardziej krytykowane przez specjalistów z zakresu bezpieczeństwa IT, co wynika bezpośrednio z badań nad podatnością nowych rozwiązań na zagrożenia oraz codziennej praktyki ochrony systemów teleinformatycznych. Praktyki te wskazują na wiele nieścisłości w zakresie własności kluczowych komponentów systemów RFID a także ich wpływ na obniżenie poziomu bezpieczeństwa wielu systemów, w których taka automatyczna identyfikacje zastosowano.

Podstawy technologii RFID

RFID jest techniką zdalnego rozpoznawania obiektów wyposażonych w miniaturowe radiowe systemy nadawczo-odbiorcze działające w trybie „hasło-odzew". W typowych realizacjach takich systemów ich czytniki rozsyłają sygnał radiowy, który odebrany przez układ elektroniczny, znacznik RFID, zwany czasami transponderem lub tagiem RFID, umieszczony na, lub wewnątrz identyfikowanego, wcześniej oznakowanego takim znacznikiem obiektu, powoduje jego odpowiedź, także w postaci sygnału radiowego (Szczurkowski, 2010, s. 16-23).

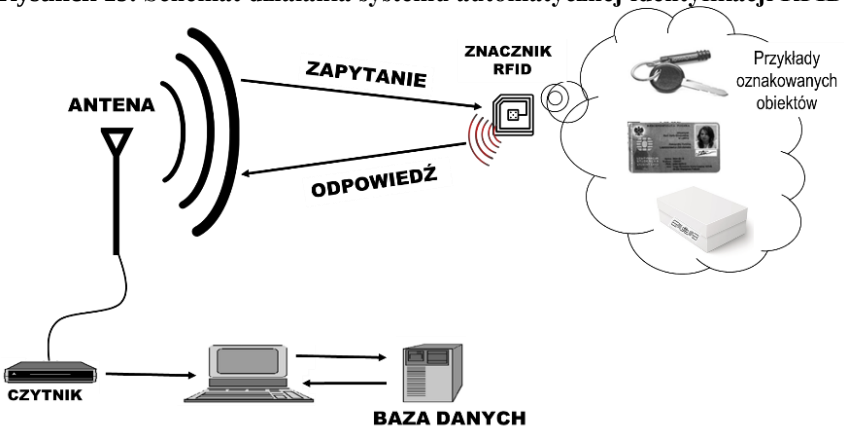
Sygnał ten zawiera zestaw danych identyfikacyjnych dotyczących obiektu oznakowanego obiektu. Odebrany sygnał jest analizowany a następnie porównywanych z wzorcem z bazy danych w celu jednoznaczniej identyfikacji obiektu (Rysunek 19).

Systemy takie stały się ostatnio tak rozpowszechnione, że właściwie trudno znaleźć obszar działalności, w którym nie występuje rozwiązanie tego typu. Znajdują one zastosowania w (Korczak, 2009):

- handlu i logistyce - do znakowania towarów,

- administracji - do znakowania dokumentów,
- finansach i bankowości - do identyfikacji stron operacji finansowej,
- ochronie - do monitorowania/lokalizacji kosztownych przedmiotów,
- systemach bezpieczeństwa pojazdów tzw. immobilizery – do identyfikacji właściciela pojazdu,
- ochronie zdrowia – do kontroli stanu zdrowia pacjenta,
- zarządzaniu personelem (identyfikatory pracownicze),
- ewidencjonowaniu zwierząt (np. mikrochipy do znakowania psów),
- i wielu, wielu innych.

Rysunek 19. Schemat działania systemu automatycznej identyfikacji RFID



Źródło: Opracowanie własne.

Zakres zastosowania układów RFID zależy w dużej mierze od zaimplementowanego w tych układach standardu komunikacyjnego, sposobu zasilania, sposobu przechowywania i przetwarzania danych identyfikacyjnych, możliwości miniaturyzacji i rozbudowy oraz oczywiście kosztów (Szczurkowski, 2010, s. 16-23).

Ze względu na sposób przechowywania i generowania danych identyfikacyjnych znaczniki RFID dzielimy je na kategorie:

- RO (*ang. Read Only*). Zapisane w układzie elektronicznym RFID dane identyfikacyjne zawierające jedynie numer seryjny identyfikatora

wbudowany na stałe w procesie produkcji, bez możliwości jego późniejszej modyfikacji,
- typu WORM (*ang. Write Once Read Many Times*). Zapisu wartości identyfikacyjnych można dokonać można dokonać po procesie produkcji, jest to jednak zapis jednorazowy i nie ma w nich możliwości zmiany numeru seryjnego,
- typu R/W (Read / Write). Znaczniki tego typu umożliwiają wielokrotny zapis danych identyfikacyjnych, bez możliwości zmiany numeru seryjnego.
- Biorąc pod uwagę źródło zasilania znaczniki RFID dzieli się na:
- aktywne, które wyposażone są we własne źródło zasilania, które wykorzystują zarówno do operacji związanych z przetwarzaniem danych identyfikacyjnych jak transmitowaniem odpowiedzi dla czytnika,
- pasywne, które nie posiadają własnego źródła zasilania, a do wszystkich operacji wewnątrz znacznika oraz zasilania transmisji wykorzystują sygnał otrzymany z czytnika,
- semi-pasywne czyli takie, które podobnie jak znaczniki pasywne do zasilenia transmisji zwrotnej używają sygnału z czytnika, jednak do wykonywania operacji na danych wewnątrz układu (np. aktywacja układu do pomiaru temperatury) wykorzystują dodatkowe źródło zasilania.

Najbardziej rozpowszechnione i jednocześnie spełniające najwięcej wymagań związanych z kryteriami kosztowo-technologicznymi oraz funkcjonalnymi są znaczniki pasywne.

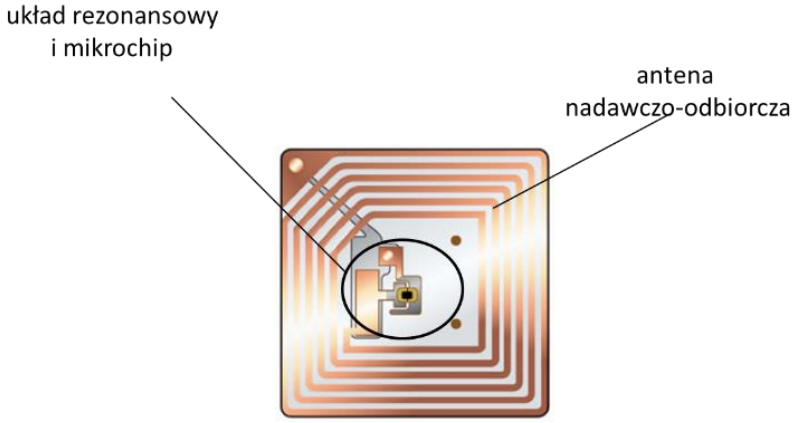
Pasywne transpondery RFID

Pasywne znaczniki RFID są najprostsze do realizacji, najtańsze w produkcji i dzięki temu najczęściej stosowane dzięki zastosowanej w nich technice generowania sygnału zwrotnego z wykorzystaniem sygnału otrzymanego z innego źródła, czyli bez wykorzystania własnego źródła zasilania.

W pasywnych układach RFID wykorzystuje się zjawisko sprzężenia elektromagnetycznego, które jest sposobem przenikania prądu elektrycznego pomiędzy obwodami, które nie są ze sobą bezpośrednio połączone. Zgodne z zasadą działania tego zjawiska, gdy znacznik znajdzie się w zasięgu transmisji sygnału z czytnika, sygnał ten wzbudza prąd w rezonansowym obwodzie

odbiorczym LC transpondera. Uzyskana energia jest gromadzona w układzie znacznika a następnie wykorzystana do wygenerowania prądu do odpowiedzi dla czytnika. Odpowiedź ta jest w postaci zmodulowanego sygnału radiowego zawierającego kilkunastocyfrowy identyfikator. Oczywiście moc sygnału odpowiedzi transpondera jest o wiele wielokrotnie mniejsza niż sygnału odebranego od czytnika, co ogranicza także zasięg (Ahson, Ilyas, 2008, s. 3-17). Wzbudzony w transponderze prąd jest rzędu miliamperów a czas potrzebny do wygenerowania odpowiedzi to ok. 25-50 ms. Taki sposób komunikacji, jest wystarczający do wypełnienia funkcji automatycznej identyfikacji w większości systemów czasu rzeczywistego. Ponadto, w niektórych zaawansowanych rozwiązaniach technicznych (z modułem do przetwarzania danych identyfikacyjnych), wzbudzony w obwodach prąd jest wykorzystywany także do zasilenia operacji wykonywanych w obwodach układu scalonego podłączonego do RFID. Operacje takie muszą jednak wymagać do działania prądu rzędu μA (np. czujniki temperatury).

Rysunek 20. Budowa pasywnego znacznika RFID



Źródło: scmwiki2012.wordpress.com/r-2/radio-frequency-identification-rfid/.

Sposób działania pasywnych znaczników RFID wyznacza także ich klasyfikację i ograniczenia. Podział ten określony jest przez zakres częstotliwości

komunikacyjnej transponderów, co warunkuje także skutecznych zasięg transmisji tych układów. Działają one w zakresach:

- niskich częstotliwości - 125 kHz - 134,2 kHz.
- wysokich częstotliwości - 13.56 MHz.
- ultra wysokich częstotliwości - 860 MHz - 960 MHz,
- super wysokich częstotliwości - 2.45 GHz.

Zasięg odpowiedzi pasywnych znaczników, zgodnie z przejętymi normami, jest od kilku centymetrów dla znaczników działających z zakresie niskich częstotliwości, poprzez kilkadziesiąt centymetrów dla układów działających na częstotliwości 13,56 MHz (niektóre źródła mówią o kilku metrach), do kilkunastu metrów zasięgu dla ultra wysokich częstotliwości i kilkudziesięciu dla działających w pasmach super wysokich częstotliwości.

Systemy zdalnej automatycznej identyfikacji wykorzystujące układy RFID konstruuje się i wdraża bazując na wartościach podanych parametrów i teoretycznych zależnościach opisujących zjawisko. Problem jednak w tym, że przedstawione normy i doświadczenia z tymi urządzeniami nie dają pełnego obrazu możliwości komunikacyjnych tych układów w różnych środowiskach użytkowania i przy różnych implementacjach ich układów. Trudno bowiem znaleźć precyzyjne dane umożliwiające skuteczne szacowanie ich sprawności energetycznej w różnych wariantach konfiguracyjnych, co pozwoliłoby na określić zasięg odpowiedzi przy różnych rozmieszczeniach elementów układu, środowiskach pracy i różnych poziomach sygnału nadawczego z czytnika.

Problemy bezpieczeństwa systemów z elementami RFID

Doświadczenia dotyczące stosowania elementów RFID w różnych systemach komunikacyjnych wskazują, że technologia ta podatna jest na typowe zagrożenia dotyczące większości urządzeń technologii IT (Miri 2013) (Juels 2005) (Heydt-Benjamin, Bailey, Fu, Juels, O'Hare, 2066) (8) (Karmakar, 2013, s.16-30) (Ahson, Ilyas, 2008). Wśród nich najważniejsze to:

- podsłuch – nieupoważnione uzyskiwanie informacji zawartych w transponderach RFID. Skoro w odpowiedzi na impuls magnetyczny pasywny Tag RFID wysyła informację identyfikująca go, to mogą to robić

także te czytniki którymi dysponują osoby spoza kręgu legalnych użytkowników systemu[53] (Kirschenbaum, Avishai, 2006) (Kannouf, Douzi, Benabdellah, 2015);

- podszywanie – można elektronicznie wytworzyć sekwencję identyfikacyjną będącą kopią tej, którą wysyła prawdziwy znacznik RFID lub używać transpondera RFID zdemontowanego z jednego obiektu i przytwierdzonego do innego;
- podrabianie, klonowanie – w sytuacji, gdy system działa wyłącznie w oparciu o zdalną identyfikację, czyli nie weryfikuje się związku obiektu materialnego z jego sekwencją identyfikującą, można odczytywać zdalnie zawartość i następnie wykonywać kopie znaczników RFID a także wykonywać własne, zawierające transpondera działające według ustalonych procedur komunikacyjnych ale przesyłających sekwencje identyfikacyjne nie odnoszące się do legalnych obiektów[54] (Yossi, 2006);
- DoS (odmowa wykonania usługi – Denial of Service) – w celu zablokowania możliwości zdalnej identyfikacji można zastosować fizyczne osłony blokujące sygnał radiowy, zagłuszać sygnał wytwarzając inny o tej samej częstotliwości lub zdalnie uszkodzić znacznik[55];
- śledzenie – ponieważ, każdy znacznik RFID posiada unikalny kod identyfikacyjny można przyjąć, że oznakowanie takim znacznikiem obiektu umożliwia jednocześnie wyróżnienie go spośród innych w dowolnym momencie jego życia, pod warunkiem że znajdzie się od w zasięgu czytnika (Miri, 2013,s. 241).
- rozpowszechnianie wirusów komputerowych – ta ciekawa możliwość ma związek ze zdalnym przesyłaniem sekwencji informacji do każdego urządzenia nadawczo-odbiorczego, które wyśle odpowiedni sygnał do znacznika RFID. Jeżeli sygnał taki wyśle urządzenie komputerowe to może się okazać, że w sekwencja identyfikacyjna otrzymana z transpondera będzie zawierała zestaw poleceń do wykonania przez komputer.

[53] www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20.
[54] www.youtube.com/watch?v=BR-JXDdzCko.
[55] www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20.

Przedstawione powyżej podatności na zagrożenia bezpieczeństwa informacji opisywanej technologii automatycznej identyfikacji, mogą posłużyć do wykreowania wielu scenariuszy związanych ze stosowaniem znaczników RFID w różnych dziedzinach życia. Scenariusze takie umożliwią mogą stanowić podstawę dogłębnej analizy kwestii bezpieczeństwa stosowania elementów tej technologii w różnych systemach informacyjnych.

Oto takie przykładowe scenariusze:

- pracownik konkurencji lub złodziej dokonuje nieautoryzowanej, zdalnej inwentaryzacji zasobów sklepu/magazynu określając precyzyjnie ilość i rodzaj zasobów. (podsłuch);
- atakujący zdalnie modyfikuje lub niszczy identyfikatory w tagach RFID obiektów w łańcuchu dostaw (np. w kontenerze). (niszczenie układów elektronicznych, DoS);
- atakujący w paczce z wieloma towarami umieszcza same tagi RFID, co daje wrażenie, że obiektów jest więcej niż w rzeczywistości;
- atakujący podmienia identyfikatory w etykietach RFID towarów droższych na identyfikatory towarów tańszych;
- atakujący umieszcza towar ze znacznikiem RFID w klatce Faradaya, co uniemożliwia transmisję sygnału identyfikującego;
- złodziej sklepowy po prosu usuwa etykietę RFID z opakowania towaru;
- złodziej sklepowy uszkadza czytnik etykiet RFID towarów w sklepie (DoS);
- terrorysta lub przestępca modyfikuje znacznik RFID w paszporcie/dowodzie tożsamości na identyfikator uczciwego obywatela lub w czasie odczytu zawartości zakłóca działanie czytnika albo wytwarza sygnał identyfikatora innej osoby (Juel, Molnar, Wagner, 2005);
- atakujący modyfikuje identyfikator RFID na taki, który posiada terrorysta, przestępca lub osoba z nimi powiązana (podrobienie) (Juel, Molnar, Wagner, 2005);
- atakujący skanuje zawartość bagaży na lotnisku (podsłuch);
- w bagażu terrorysty umieszcza się tag RFID, który rozsyła wirusa komputerowego;

- bomba w restauracji eksploduje, gdy skaner wykryje w pobliżu pięć lub więcej osób ze znacznikami RFID w amerykańskich paszportach;
- zamachowiec określa położenie potencjalnej ofiary przez zdalne odczytywanie personalnych identyfikatorów RFID;
- czytnik w obiekcie handlowym odczytuje identyfikator RFID oraz identyfikatory towarów, które ze sobą posiada, zapisuje je w bazie danych a następnie w odpowiednim momencie proponuje mu na ekranie inne, o tym samym profilu, ale np. droższe lub prowadzi indywidualny marketing w innej formie;
- atakujący trwale unieszkodliwia znacznik RFID kierunkowym impulsem elektromagnetycznym dużej mocy.

Oprócz wymienionych, teoretycznych scenariuszy, badania nad zastosowaniem technologii RFID ujawniły cały szereg innych mankamentów, dotyczących zaawansowanych konstrukcji znaczników, które stosuje się w kartach płatniczych lub którymi znakuje się dokumenty tożsamości:

- kryptolog Adi Shamir w 2006r udowodnił możliwość złamania haseł standardowych metek RFID za pomocą telefonu komórkowego[56],
- ekspert ds. bezpieczeństwa Chris Paget w 2010r opublikował film, w którym prezentuje sposób pozwalający na zdalne odczytanie i sklonowanie paszportów elektronicznych RFID w ciągu zaledwie 20 minut[57],
- Lukas Grunwald i Christiana Bottger opracowali darmowe oprogramowania, za pomocą którego można w ciągu 5 minut, nie mając fizycznego dostępu do niego, sklonować zawartość elektronicznego znacznika paszportu, dowodu osobistego itp.[58] (Miri, 2013, s.46-50),
- i wiele, wiele innych, w tym te, prezentowane na konferencjach Black Hat USA w 2013[59] i 2015 roku[60].

[56] www.rfidjournal.com/articles/view?2167.
[57] www.youtube.com/watch?v=BR-JXDdzCko.
[58] www.rfdump.org/.
[59] www.blackhat.com/us-13/briefings.html#Brown.
[60] www.blackhat.com/us-15/briefings.html#breaking-access-controls-with-blekey.

Podsumowanie

Niemal wszyscy eksperci ds. bezpieczeństwa IT wypowiadając się negatywnie na temat poziomu bezpieczeństwa systemów, z wbudowanymi systemami RFID. Jednak technologia ta rozszerza swój zasięg zastosowań gdyż przez wielu ludzi jest postrzegana jako idealne rozwiązanie wielu problemów z zakresu technologii informacyjnych, przy braku, według powszechnego mniemania, wad takich systemów. Oczywiście eksperci z dziedziny bezpieczeństwa IT nieustannie proponują modyfikacje operacji wewnątrz układów transponderów, nowe sposoby szyfrowania danych czy protokoły komunikacyjne do zastosowania w tych układach. Niestety, nie poprawia to generalnie sytuacji, w której technologia zawierająca wiele niejasności dla użytkowników i tak wiele słabych stron jest stosowana na każdym kroku, nie bacząc na potencjalnie negatywne skutki takich działań. Pewnym mylącym użytkowników symptomem działania tych systemów jest to, że większość ich sprzętowych, legalnych implementacji posiada parametry wymagające bliskości czytnika i znaczników, utwierdzając korzystających z tych systemów w mylnym przekonaniu, iż zdalna komunikacja z ich systemem jest niemożliwa.

Wstępne badania nad parametrami układów pasywnych RFID, prowadzone w pracowni RFID Wyższej Szkoły Oficerskiej Wojsk Lądowych im. Tadeusza Kościuszki we Wrocławiu ujawniły, że praktycznie wyniki odczytu tego typu znaczników znacznie odbiegają od przyjętych w standardach implementacyjnych norm dla tych urządzeń. Na przykład układy RFID wbudowane w karty standardu MIFARE, stosowane np. w kartach bankomatowych, działające w paśmie 13,56 MHz, z opisanym w normie zasięgiem odpowiedzi rzędu kilkudziesięciu centymetrów (nieoficjalnie do kilku metrów), bez problemu dało się odczytać z odległości kilkunastu metrów!

Obserwacje te potwierdza analiza parametrów najnowszego sprzętu do odczytywania pasywnych znaczników RFID tzw. Long Range RFID Readers[61],[62],[63]. Sprzęt tego typu, dostępny dla znaczników wszystkich zakresów częstotliwości, umożliwia znaczące zwiększenie odległości odczytu pasywnego

[61] www.aliexpress.com/price/long-range-rfid-reader_price.html.
[62] www.atlasrfidstore.com/active-rfid/.
[63] www.gaorfid.com/devices/readers-by-feature/long-range-rfid-readers.

znacznika RFID[64]. Jeśli do tego dodamy, że można go stosować jako kierunkowe nadajniki sygnału, to wiele spośród teoretycznych scenariuszy przedstawionych w rozdziale 3 niniejszego artykułu przestaje być teoretycznymi.
Dodatkowo, warto zauważyć, że nawet proste doświadczenia z przesyłaniem energii poprzez sprzężenie indukcyjne wyraźnie udowadnia nieścisłość niektórych założeń dotyczących działania systemów RFID[65].
W związku z prezentowanymi faktami wydaje się, że oficjalnie przyjmowane parametry działania pasywnych znaczników RFID powinny być zweryfikowane a wyniki tej weryfikacji upowszechnione. Dotyczy to zarówno praktycznych możliwości odległości odczytu ich wartości jak i zablokowania takiej operacji.

[64] www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20
[65] www.ely.pg.gda.pl/nkse/index.php/projekty/zrealizowane/60-bezprzewodowy-przesyl-energii-elektrycznej-poprzez-rezonansowe-sprzezenie-indukcyjne-model-demonstracyjny.

2. Społeczne aspekty cyberbezpieczeństwa

2.1. Kilka uwag na temat koncepcji cyberprzestrzeni

O *cyberprzestrzeni* mówi i pisze się ostatnio często w zawiązku nie tylko z jej znaczeniem w procesie globalizacji naszego świata, ale również ze względu na zagrożenia, jakie mogą się pojawić wtedy, jeśli stanie się ona kolejnym *polem walki* między poszczególnymi państwami w czasie ewentualnej np. wojny hybrydowej. Biorąc to pod uwagę wydaje się celowym zastanowienie się nad koncepcją *cyberprzestrzeni* oraz nad jej uwarunkowaniami zaistnienia we współczesnej cywilizacji, a także nad jej gospodarczym, społecznym, politycznym i militarnym wpływem na rozwój ludzkości.

Zauważmy na wstępie, że koncepcja *cyberprzestrzeni* nie pojawiła się z dnia na dzień, czyli nie zaistniała *deus ex machina* na skutek jakiegoś cudownego zdarzenia, lecz jest jednym z osobliwych artefaktów dokonanych przez ludzi w wyniku ich trwającego od wielu tysiącleci cywilizacyjnego i społecznego rozwoju. I w ciągu tego rozwoju ludzie starali się opanować i przekształcać swoje środowisko naturalne – najpierw w wymiarze lokalnym, czyli w *mikroskali* – a następnie wychodzić poza nią w coraz szerszym wymiarze, tzn. w danym kraju, na określonym kontynencie i poza nim, czyli w obrębie globu. Współcześnie podejmowane są usiłowania zmierzające nawet do podboju Kosmosu.
Szacuje się, że cywilizacyjny i społeczny rozwój gatunku *Homo sapiens* rozpoczął się około 20 tys. lat p.n.e., czyli od czasu, gdy wspomniany gatunek zaczyna wychodzić ze świata zwierzęcego zdobywając stopniowo przewagę nad nim, choć był jeszcze nieliczny, a zaliczane do niego istoty były znacznie mniejsze i słabsze w porównaniu z przedstawicielami niektórych gatunków zwierząt. Przewagę tą uzyskiwał sukcesywnie posługując się prymitywnymi narzędziami sporządzonymi z kamienia, drzewa i kości zwierząt, które w praktyce doskonalił, jak również swoją umiejętność posługiwania się nimi. Przewaga ta stała się zdecydowaną, gdy około 10 tys. lat p.n.e. – w okresie

neolitu – niektóre grupy tego gatunku przeszły do osiadłego trybu życia i zaczęły uprawiać ziemię, hodować zwierzęta i opanowały umiejętność korzystania z ognia.

Kolejnym istotnym wydarzeniem w rozwoju interesującego nas gatunku jest *pierwsza rewolucja trakcyjna*, która dokonała się około 3 600 lat p.n.e., gdy wynaleziono koło, co umożliwiło wytwarzanie pojazdów kołowych i wykorzystywanie do poruszania się nimi siły pociągowej wołów i koni. Umożliwiło to ludziom m.in. zwiększenie swojej przestrzeni życiowej poprzez przemieszczanie się na coraz bardziej odległe tereny.

Wspomnijmy także o tym, że już w XVI wieku p.n.e. rydwany są na szeroką skalę wykorzystywane m.in. w wielu ówczesnych armiach (Ziółkowski, 2009, s. 226 i 233). Oczywiście, ówcześni ludzie nie zdawali sobie sprawy z tego faktu, że wspomniana rewolucja była pierwszym krokiem w procesie zwiększania przestrzeni życiowej człowieka i, iż spowoduje następne, które doprowadzą go kiedyś do możliwości penetracji Kosmosu i do lądowania na Księżycu.
Przypomnijmy też o tym, że około 3000 tys. lat p.n.e. powstają na ziemiach Mezopotamii i Egiptu pierwsze *polis* – czyli państwa – miasta, m.in. bardziej znany, jakim był Babilon. A także o tym, że około 2500 lat p.n.e. rozpoczęto wydobywać i wytapiać miedź oraz inne metale i ludzkość weszła w epokę brązu, zaś około 1200 lat p.n.e. wykorzystywano żelazo. Odkrycie metali i żelaza spowodowało, że ludzkość weszła w kolejne fazy coraz bardziej rozwiniętej cywilizacji.

Osiągnięcia gatunku *Homo sapiens*, które były możliwe dzięki aktywnej postawie ludzi w stosunku do środowiska naturalnego przejawiało się zarówno w dążeniach do jego przeobrażeń – zgodnie z wzrastającymi ich potrzebami, jednak niestety konsekwencją tej postawy była także jego eksploatacja nie licząca się często z negatywnymi skutkami dla tego środowiska. Otóż postawa ludzi wobec środowiska naturalnego ma ambiwalentny charakter i powoduje nie tylko swego rodzaju współdziałanie z nim, np. przy uprawie ziemi lub hodowli zwierząt, ale także ich walkę, np. z gatunkami zwierząt lub roślin, które

są uznawane za szkodliwe. A wtedy dochodzi np. do wypalania lasów, aby pozyskać ziemię pod uprawę itp. działania negatywne, które dewastowały ekosystem.

Przypomnijmy również o tym, że ludzie od najdawniejszych czasów walczyli nie tylko z przyrodą, którą chcieli sobie podporządkować, ale też między sobą. I walki między nimi w miarę ich cywilizacyjnego i społecznego rozwoju stają się coraz bardziej zaciekłe i okrutne. Przez wiele wieków są one toczone na powierzchni Ziemi w mniej lub bardziej dogodnych miejscach. Ale w miarę rozwoju poszczególnych państw, które z małych *polis* rozrastają się pod względem terytorialnym w większe jednostki i specjalizacji istniejących w nich sił zbrojnych – polem walki stają się także powierzchnie wód, na których rozgrywają się bitwy morskie. Poprzez morza dokonywano także inwazji na przybrzeżne państwa już od czasów starożytnych po nasze czasy. I do I. wojny światowej walki są prowadzone na wspomnianych wcześniej polach, nazywanych niekiedy „polami chwały" i na powierzchni wód.

Dopiero na kolejnym etapie rewolucji przemysłowej, która dokonała się w XVIII wieku, związanym z odkryciem nowego źródła mineralnej energii, jaką stała się *ropa naftowa*, pojawiają się nowe rodzaje broni i powstają nowe pola walki. Otóż wynaleziony w 1897 roku silnik napędzany ropą naftową – którego konstruktorem był Rudolf Diesel – zostaje użyty w 1911 roku do poruszania samochodów, a następnie do ciężkich pojazdów mechanicznych, jakimi stały się czołgi oraz do budowy dwusilnikowych samolotów używanych już w 1914 roku.

Z kolei wynalezienie silnika napędzanego siłą energii elektrycznej umożliwiło budowę okrętów podwodnych, które zostały skutecznie użyte przez Niemcy już w 1914 roku. Używane przez państwa uczestniczące w wojnie samoloty bojowe wspierają nie tylko walczące wojska lądowe i niszczą znajdujące się na zapleczu przeciwnika rezerwy i środki walki, ale także zwalczają się nawzajem, dążąc do zapewnienia sobie przewagi w przestrzeni powietrznej, która staje się nowym polem walki. Natomiast okręty podwodne doprowadzają do rozszerzenia pola walki na wodach mórz i oceanów poniżej ich powierzchni.

2.1. Kilka uwag na temat koncepcji cyberprzestrzeni

Zauważmy, że już w pierwszej połowie XX wieku doszło więc do nieznanego dotąd w historii poszerzenia pola walki i w czasie II. wojny światowej prowadzono działania zbrojne na lądzie, na powierzchni mórz i oceanów, w ich głębiach oraz w przestworzach. A u schyłku tego wieku pojawia się koncepcja tzw. *wojen gwiezdnych*, których polem walki miał być Kosmos. Na razie została ona urzeczywistniona jedynie w filmowej wersji.

Jednak przestrzeń kosmiczna nie przestaje być przedmiotem zainteresowania środowisk wojskowych i od wielu lat poruszają się w niej satelity szpiegowskie, obok licznych satelitów telekomunikacyjnych, które stały się koniecznym elementem coraz bardziej rozbudowanego systemu internetowego.

Przypomnijmy również o tym, że około połowy XX wieku pojawia się *cybernetyka*, czyli nauka o sterowaniu oraz o przekazywaniu i przekształcaniu informacji w systemach technicznych, biologicznych i społecznych – jak ją określił Norbert Wiener – która umożliwiła budowę analogowych maszyn matematycznych, a następnie *komputerów*, czyli elektronicznych maszyn cyfrowych służących do automatycznego przetwarzania danych oraz projektowania i programowania rozmaitych działań. Możliwość wykorzystywania komputerów do wykonywania rozmaitych czynności zarówno z obsługą oprogramowania poszczególnych użytkowników, jak też rozmaitych instytucji działających w sferze publicznej i prywatnej, doprowadziła do pojawienia się *Internetu*, czyli globalnej sieci komputerowej obejmującej tysiące pojedynczych sieci istniejących w poszczególnych państwach. Sieć ta jest powszechnie wykorzystywana do przesyłania drogą elektroniczną poczty oraz do wyszukiwania i pozyskiwania rozmaitych informacji, a także różnych programów przez poszczególnych użytkowników, którymi są zarówno osoby prywatne, jak też rozmaite instytucje. Zaś globalny zasięg Internetu umożliwiają satelity komunikacyjne poruszające się w przestrzeni kosmicznej, które mogą odbierać i retransmitować przekazy informacji w skali całego globu.

Zwróćmy na to uwagę, że ludzie nigdy nie żyli w świecie wolnym od zagrożeń od czasu zaistnienia gatunku *Homo sapiens.* Jednak dopiero w XX wieku

dostrzegli, że zaistniałe zagrożenia przybrały apokaliptyczną postać, ponieważ mogą one doprowadzić do zagłady nie tylko ich gatunku. Bowiem w połowie tegoż wieku po raz pierwszy została użyta bomba atomowa o nieznanej dotąd sile rażenia i to nie tylko w momencie jej wybuchu, ale także przez wiele następnych lat na skutek promieniowania radioaktywnych cząstek, które zagrażają żywym organizmom. Zauważmy, że w dzisiejszych arsenałach są zgromadzone bomby termojądrowe o jeszcze większej mocy rażenia. I z tego względu wiek ten może zostać uznany w historii za początek nowej epoki nazwanej przez geologów *antropocenem* (Bendyk, 2016), czyli epoką, w której człowiek może decydować o dalszym losie Ziemi. Stało się to na skutek:

- kolejnych osiągnięć rewolucji naukowo-technicznych, które zmieniają i dewastują środowisko naturalne;
- niekorzystnych trendów demokratycznych zwłaszcza w przeludnionych krajach Trzeciego Świata;
- nierównomiernego rozwoju gospodarczego i cywilizacyjnego zacofania poszczególnych krajów;
- wzrastającego wyzysku krajów słabszych pod względem gospodarczym przez istniejące mocarstwa oraz
- bezwzględnej walki istniejących mocarstw o dominację w skali światowej, która stymuluje różne napięcia polityczne i powoduje lokalne konflikty zbrojne, jakie mogą przeobrazić się w zmagania wojenne w szerszym wymiarze, a nawet doprowadzić do kolejnej wojny światowej.

Otóż w świecie, w którym pojawiają się potężne ugrupowania polityczno-militarne, utrzymanie pokoju w skali światowej łączy się z prowadzeniem polityki wzajemnego odstraszania, pobudzającego nieustanny wyścig zbrojeń, mogący doprowadzić do tego, że w przyszłości polem zbrojnych zmagań stanie się już nie tylko Ziemia, ale i Kosmos. Współczesny świat staje więc przed nowymi zagrożeniami, nie znanymi społeczeństwom minionych wieków i wynikającymi z nich wyzwaniami zarówno militarnymi, jak i pozamilitarnymi. Zagrożenia te wymagają wnikliwych analiz związanych ze strategicznymi i taktycznymi problemami bezpieczeństwa w wymiarze globalnym, a także w wymiarze poszczególnych kontynentów i krajów, a w tej mierze także Polski.

2.1. Kilka uwag na temat koncepcji cyberprzestrzeni

Postępująca globalizacja spowodowała, że nawet lokalne konflikty zbrojne mogą spowodować negatywne skutki o trudnym do przewidzenia zasięgu. Z tego też względu bezpieczeństwo poszczególnych krajów trzeba postrzegać globalnie biorąc pod uwagę potencjalny wymiar zagrożeń. Obecnie nie ma takich zagrożeń i związanych z nim problemów bezpieczeństwa, które mogłyby być obojętne z militarnego punktu widzenia (Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, 2013).

Zaistnienie Internetu i problemy związane z jego funkcjonowaniem zainspirowały zapewne pojawienie się koncepcji *cyberprzestrzeni*, która stała się jedną z nowych ujęć przestrzeni w szerokim tego słowa znaczeniu. Otóż koncepcja ta skłania do refleksji nad tym, czym jest ta osobliwa przestrzeń poprzedzona dodatkiem „*cyber*".

Wiadomo, że słowem *przestrzeń* posługiwano się od dawna dla określenia rozmaitych doświadczeń człowieka związanych z jego przemieszczaniem się w środowisku naturalnym, w którym żył, a także poza nim, czyli na innym obszarze. Dotyczyło ono więc przestrzeni pojmowanej trójwymiarowo, o nieograniczonej rozciągłości, wolnej od przedmiotów, a w tej mierze także tworów przyrody. I być może pod wpływem żywiołowych doświadczeń ludzi utrwaliło się mniemanie, że przestrzeń – to ta część otaczającej ich rzeczywistości, która jest wolna od tworów przyrody lub wytworów człowieka, czyli stanowi *próżnię*, w której mogą się przemieszczać ludzie i rozmieszczać w niej dowolne przedmioty. I to mniemanie znalazło się także w niektórych koncepcjach filozoficznych, a nawet w teoriach naukowych. Jednym z pierwszych filozofów, który obok materii wyróżnił także istnienie przestrzeni – utożsamianej z „próżnią"- był żyjący na przełomie V-IV wieku p.n.e. Demokryt z Abdery. Uważał on, że atomy, które są cząstkami składowymi poszczególnych przedmiotów poruszają się właśnie i łączą w owej próżni (Tatarkiewicz, 1948, s. 52).

Przyjęcie hipotezy zakładającej istnienie materii – pod postacią różnych przedmiotów i *próżni* – czyli wolnej od przedmiotów przestrzeni, która według

Newtona – twórcy tzw. *mechanistycznej koncepcji przestrzeni* – była swoistym absolutnie pustym pojemnikiem bez ścian. I w tym osobliwie wyobrażanym pojemniku istnieją i poruszają się rozmaite przedmioty. Koncepcja ta uzasadniała utrzymujący się powszechnie błędny sposób myślenia o istnieniu przestrzeni, jako osobliwej nieograniczonej próżni.

Dopiero w świetle teorii względności Einsteina hipoteza ta okazała się bezpodstawna, ponieważ między materią a przestrzenią występuje nierozerwalny związek wzajemny wyrażający się w tym, że nie może istnieć przestrzeń bez „wypełniających" ją przedmiotów materialnych, zaś próżnia jest także postacią materii, jako np. ośrodek rozchodzenia się fal elektromagnetycznych. Nie ma również takich przedmiotów, które same sobą nie tworzyłyby przestrzeni lub nie zmieniałyby jej właściwości w zależności od sposobu, w jaki poruszają się one w niej. Ścisły związek materii oraz przestrzeni i czasu ze sobą został też dobitnie wyrażony przez Einsteina w zdaniu wypowiedzianym przez niego tuż po ogłoszeniu *ogólnej teorii względności: „Gdyby znikła materia, to znikłyby przestrzeń i czas"* (Einstein, 1958, s. 8).

Wskażmy także na to, że przestrzeń – to taka ogólna forma bycia przedmiotów i zjawisk materialnych, która będąc zasadniczym warunkiem współistnienia i wzajemnego ich oddziaływania, odzwierciedla w swej istocie i cechach porządek współistnienia przedmiotów i zjawisk, określonych za pomocą relacji metrycznych i topologicznych.

Do słowa *przestrzeń* można dołączyć różne przydawki modyfikujące, które nadadzą jemu specyficzne znaczenia, stając się terminami w poszczególnych naukach, np. w astronomii, fizyce i matematyce. Tytułem przykładu wymieńmy następujące terminy utworzone w ten sposób: „przestrzeń konfiguracyjna", „przestrzeń kosmiczna", „przestrzeń n-wymiarowa" itp. Co oznacza więc termin *cyberprzestrzeń*, będący w użyciu cybernetyki i informatyki? Otóż uważam, że jest to termin wskazujący na pewien fragment przestrzeni kosmicznej naszego Układu Słonecznego, w której funkcjonuje globalna sieć komputerowa obejmująca swoim zasięgiem tysiące pomniejszych sieci istniejących w poszczególnych państwach, będąca powszechnie dostępna i wykorzystywana

do wysyłania elektronicznej poczty, a także do wyszukiwania i pozyskiwania rozmaitych informacji oraz różnych programów przez użytkowników Internetu.

Cyberprzestrzeń jest zatem wirtualnym tworem intelektualnym, który jest tak realistycznie ukazany, że wydaje się istnieć jako rzeczywista przestrzeń, czyli jako swoisty byt w ontologicznym znaczeniu. Jednak nie można zapominać o różnicy między bytem wirtualnym a rzeczywiście istniejącym obiektywnie, czyli niezależnie od kogokolwiek, tzn. od postrzegania go przez ludzi.

Czy posługiwanie się wirtualną koncepcją *cyberprzestrzeni* jest celowe? Jest to oczywiście pytanie retoryczne w sytuacji, gdy koncepcja ta jest używana w informatyce. Podobne pytania można by postawić przecież także w przypadku innych koncepcji przestrzeni, np. „przestrzeni n-wymiarowej", która jest również intelektualnym tworem. Wydaje się zatem, że odkąd istnieje Internet, odtąd pojawiła się też potrzeba takiego określenia sfery jego funkcjonowania, jaką jest *cyberprzestrzeń.*

Wspomnijmy także o tym, że ponieważ Internet jest w coraz szerszym zakresie stosowany we wszystkich dziedzinach społeczno-gospodarczych i politycznych stał się on również przedmiotem zainteresowania rozmaitych grup przestępczych, czyli tzw. „hakerów". Dokonują oni włamań do systemów komputerowych w poszczególnych krajach, a w związku z tym pojawiła się również możliwość osiągania korzyści majątkowych np. poprzez włamania do kont bankowych oraz do uprawiania szpiegostwa lub działalności terrorystycznej. Na skutek tego *cyberprzestrzeń* stała się też areną nowej przestępczości i nowych zagrożeń zarówno w wymiarze indywidualnym, jak i publicznym. Nic więc dziwnego, że większość państw podejmuje zdecydowaną walkę z tego rodzaju przestępczością i stara się zapewnić sobie bezpieczeństwo w *cyberprzestrzeni* (Grzelak, 2011, s. 139-147).

Swoistym paradoksem w tej walce jest jednak to, że zacierają się w niej różnice między tym, co służy ofensywnym i defensywnym celom poszczególnych państw. Otóż paradoks ten będzie dopóty istniał – dopóki będę one wyznawały

zasadę, że włamanie do obcego systemu komputerowego i spenetrowanie jego zawartości jest działaniem defensywnym, co może wydawać się sprawą wątpliwą. Bowiem każde włamanie jest przecież w swej istocie działaniem ofensywnym. I jak długo zasada takiej podwójnej oceny działań ofensywnych i defensywnych będzie wyznawana, tak też długo trudno będzie osiągnąć solidarność wszystkich państw w walce z tymi rodzajami przestępczości popełnianymi w *cyberprzestrzeni*, które dotyczą spraw politycznych i militarnych. Stosowanie tej zasady podważa zatem wzajemną wiarygodność nawet między zaprzyjaźnionymi państwami.

2.1. Kilka uwag na temat koncepcji cyberprzestrzeni

2.2. Proces migracji - realne czy wirtualne zagrożenie?

Wprowadzenie

Proces migracji towarzyszy ludzkości od zarania dziejów. Przemieszczanie się jednostek, czy też całych grup zamieszkujących poszczególne terytoria spowodowane było koniecznością znalezienia lepszych „warunków bytowania". Historia migracji wskazuje, że potrzeba wędrówki powodowana była chęcią pozyskania korzystnych warunków do życia, pozwalających na wykorzystanie nowych zasobów środowiska, niezbędnych do zaspokojenia potrzeb bytowych człowieka, warunkujących możliwość przetrwania, które w aktualnym miejscu uległy wyczerpaniu. Nowe tereny dawały nowe możliwości zdobywania pożywienia lub bezpieczniejsze miejsce do osiedlenia się. Kierunki takich migracji uzależnione były od klimatu, zasobności środowiska w żywność oraz możliwości stworzenia siedlisk. Wraz z rozwojem i opanowaniem różnych dziedzin życia społecznego wzrastał zasięg migracji. Osiadły tryb życia powoli przekształcał się w koczowniczy, a migracja była spowodowana głównie poszukiwaniem pożywienia oraz nowych terenów pasterskich dostarczających lepszych „warunków bytowania". Stabilizacja osadnictwa przypada na okres późnego brązu. To właśnie wtedy powstają pierwsze cywilizacje, które skupiają ludzi chętnych do zmiany trybu życia na osiadły w powstających pierwszych dużych siedliskach. Takie ośrodki zaczęły przyciągać ludzi chcących się rozwijać i wykorzystywać budujące się struktury społeczne i ekonomiczne (Leciejewicz, 2006, s. 1718). Istotną rolę w przemieszczaniu się ludzi zaczął odgrywać transport za pośrednictwem udomowionych zwierząt (m.in. wielbłądy, osły, słonie, konie) oraz żegluga śródlądowa i morska. Tak postępujący rozwój cywilizacyjny z jednej strony dawał możliwości zamieszkania ludziom w tworzonych siedliskach – dynamicznie rozwijających się miastach, a z drugiej były celem ataku społeczności zamieszkujących tereny mniej zagospodarowane. Konsekwencją dążenia do zdobycia terenów zagospodarowanych, ich przywłaszczenia wraz z infrastrukturą, były zbrojne ataki powiązane z grabieżą wszelkich dóbr. Przejmowanie władzy, upadek wielkich cywilizacji, były czynnikami masowego przemieszczania całych ludów, zarówno tych, którzy

zwyciężyli, jak i tych, którzy byli zwyciężeni - represjonowani (wypędzenia). Innym czynnikiem, który powodował wzrost migracji był gwałtowny rozwój struktur społecznych, a w jego następstwie rozwój handlu i uprzemysłowienie. Jednym z głównych powodów przemieszczania ludzi była potrzeba zmiany statusu ekonomicznego i społecznego. Fale migracji przetoczyły się przez kontynenty z różną intensywnością, w sposób pokojowy, lub też z zaangażowaniem militarnym. W okresie podbojów kolonialnych kolonizatorzy wyzyskiwali lokalne społeczności przyczyniając się do tworzenia nierówności społecznych. Taki układ powodował konieczność opuszczenia „nieprzyjaznych" terenów przez osoby wyzyskiwane i udanie się do bardziej „przyjaznych" siedlisk. Kolejny duży ruch migracyjny powstał w okresie rewolucji przemysłowych. Kolejne etapy rozwoju cywilizacyjnego oraz społecznego i nierówność w zakresie dostępu do dóbr stanowią kamienie milowe w dziejach migracji oraz uwidaczniają złożoność tego procesu i problem z przystosowaniem się przez człowieka szukającego swojego miejsca na ziemi. Każdy taki okres stawał się przyczyną wielu nowych kierunków migracji, a w konsekwencji otwierał możliwości tworzenia innych struktur społecznych w „nowym świecie". Proces przemieszczania się ludzi można ogólnie podzielić na: (1) migrację ekonomiczną (zmiana miejsca zamieszkania ze względu na warunki ekonomiczne, z możliwością powrotu do miejsca zamieszkania w każdej chwili) i (2) uchodźców (zmiana zamieszkania ze względu na działania zagrażające życiu i zdrowiu ludzi, m.in. działania wojenne, prześladowania etniczne, rasowe, wyznaniowe, bez możliwości powrotu do miejsca zamieszkania). W każdym z tych procesów dominującą rolę odgrywało pozyskanie i wykorzystanie informacji w celu określenia miejsca oraz warunków przesiedlenia. To dzięki informacji o „lepszym świecie" ludzie podejmowali decyzje o podróży w „nieznane". W takim kontekście migracja wiąże się z rzeczywistym działaniem ludzi w ich konkretnym środowisku życia, ale także z ich wyobrażeniem o „nowym, lepszym domu". Czy te działania mogą przenosić się do cyberprzestrzeni i, czy mogą być elementami wpływającymi na cyberbezpieczeństwo? Na te i wiele innych pytań, związanych z tym intrygującym tematem, postaram się odpowiedzieć w dalszej części opracowania.

2.2. Proces migracji - realne czy wirtualne zagrożenie?

Oblicza współczesnej migracji ekonomicznej

Wprowadzając w zagadnienia współczesnej migracji należy przytoczyć tezę, że: międzynarodowe ruchy ludności przeobrażają państwa i społeczeństwa na całym świecie, wywierając wpływ na stosunki bilateralne i regionalne, bezpieczeństwo, tożsamość narodową i suwerenność (Castles, Miler, 2011, s. 12). Oczywiście tak postawiona teza podkreśla, że proces migracji jest procesem ciągłym, a jego wpływ jest wieloraki i ma zasięg globalny. W 2006 roku, podczas sześćdziesiątej pierwszej sesji Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych (ONZ), sekretarz generalny Kofii Annan podkreślił, że migracja w skali światowej jest zjawiskiem pozytywnym, zarówno z punktu widzenia krajów przyjmujących imigrantów, jak i państw, z których pochodzą[66].

W 2005 roku ogólna liczba migrantów na całym świecie obejmowała około 191 milionów, co stanowiło wzrost o 25% w stosunku do roku 1990. „Weszliśmy obecnie w nową erę migracji - zjawisko to stało się obecnie światowym fenomenem" - podkreślił w raporcie sekretarz generalny ONZ. Kofii Annan wskazał na takie kraje jak: Irlandia, kilka państw Europy Południowej, Koreę Południową czy Chile, gdzie obecność imigrantów zasadniczo przyczyniła się do dynamicznego rozwoju gospodarczego[67]. W 2013 roku liczba migrantów na świecie zwiększyła się do około 232 milionów.

Migracja jest potężnym narzędziem w walce z ubóstwem i szansą na polepszenie jakości życia - przekonuje ONZ w trakcie obchodów Międzynarodowego Dnia Migrantów w 2016 roku. Migranci ekonomiczni świadczą pracę w kraju docelowym, a zarobione pieniądze przesyłają rodzinom pozostawionym w ojczyźnie. „Jednak ta liczna populacja nadal pozostaje w dużej mierze niewidoczna i niewysłuchana" - czytamy w przesłaniu Sekretarza Generalnego ONZ Ban Ki Muna[68]. Obraz migracji kreowany przez sekretariat ONZ przedstawia migrację jako zjawisko pozytywne, oparte na przestrzeganiu Praw Człowieka, oraz z zachowaniem wszelkich konwencji dotyczących

[66] http://www.unic.un.org.pl/unic-activities/spotkanie-wysokiego-szczebla-na-forum-zgromadzenia-ogolnego-na-temat-migracji-miedzynarodowych-i-rozwoju/862.

[67] https://wiadomosci.wp.pl/migracja-w-skali-swiatowej-jest-zjawiskiem-pozytywnym-6036386656195713a.

[68] https://wiadomosci.wp.pl/onz-migracja-szansa-na-polepszenie-zycia-6078989422130305a.

przemieszczania się ludzi pomiędzy krajami, a nawet kontynentami. Oczywiście, biorąc pod uwagę migrację ekonomiczną, jest to jak najbardziej rzeczywiste przedstawienie skomplikowanych ruchów ludności oraz przepływu środków ekonomicznych. Na zakres migracji ekonomicznej ma wpływ: (1) wzrost liczby ludności, (2) popyt na pracę, (3) niski standard życia, (4) brak możliwości ekonomicznych w dotychczasowym miejscu zamieszkania, (5) dostępność dóbr materialnych, (6) rodzące się perspektywy ekonomiczne oraz (7) stabilna polityka gospodarcza w nowym miejscu zamieszkania. Migracja ekonomiczna staje się czynnikiem demograficzno-ekonomicznym, nie tylko w skali pojedynczego kraju, ale również w skali międzynarodowej, czy też globalnej. Ogólnie mówiąc kierunki migracji ekonomicznej przebiegają pomiędzy krajami biednymi a krajami bogatymi, wysokorozwiniętymi. Jednakże proces ten przebiega również pomiędzy krajami biednymi, sąsiadującymi w obrębie danego kontynentu, np. mieszkańcy Afryki. Przemieszczanie się ludzi pomiędzy kontynentami wiąże się z większymi odległościami, w rezultacie ze znacznymi nakładami na podróż. Innym bardzo istotnym czynnikiem migracji ekonomicznej jest polityka państw przyjmujących migrantów w stosunku do przesiedleńców. Mieszkańcy krajów rozwiniętych mają większą możliwość przemieszczania się i zamieszkania w kraju docelowym niż obywatele krajów rozwijających się (Thiollet, 2017, s. 13-14). Jednakże, biorąc pod uwagę, że mieszkańcy krajów o wysokim stopniu ubóstwa rzadko decydują się na migrację ekonomiczną do krajów najbogatszych, natomiast ich migracja odbywa się częściej do krajów średniozamożnych lub też niezamożnych, ale jednocześnie z dużym wzrostem gospodarczym. Do krajów najbogatszych migrują głównie mieszkańcy o średnim statusie społecznym, pochodzący z terenów objętych transformacją społeczną i ekonomiczną (Castles, Miler, 2011, s. 42). Migracja ekonomiczna oraz osiedlanie się przybyszy w określonych miejscach stwarza nowe warunki społeczne i kulturowe w danym społeczeństwie. Nie jest to obojętne dla kultury, religii, tradycji, obyczajów oraz ładu społeczno-politycznego. Oczywiście najlepszym wariantem byłoby, aby osiedleńcy asymilowali się z otoczeniem, a proces ten przebiegał bezkonfliktowo i doprowadził do pełnej integracji z rdzennymi mieszkańcami. Jednakże przybyli migranci nie zawsze przyjmują taki porządek, a ich postępowanie odbiega od asymilacyjnego podejścia do osiedlenia i współżycia

w nowych warunkach. Państwo przyjmujące napływającą ludność, w ramach przeciwdziałania takim przypadkom, zmienia swoje podejście do przybyszy akceptując ich odmienność kulturową i powolne dostosowywanie się migrantów do życia społecznego i kulturalnego w całkowicie odmiennych warunkach niż te, z którymi mieli do czynienia w kraju pochodzenia. Wielokulturowość opiera się na uznaniu kulturowej i tożsamościowej ekspresji mniejszości i włączeniu ich w obszar reprezentacji narodowych, które w ten sposób stają się pluralistyczne (Simon, 2017, s. 99-100). Zdarzenia aktów terrorystycznych, zapoczątkowane zamachami z 11 września 2001 roku, spowodowały w niektórych państwach przyjmujących migrantów ekonomicznych wycofanie się z polityki wielokulturowości. W społeczeństwach tych zrodził się nowy typ działania, polegający na wnikliwiej obserwacji „wszystkich obcych". Procesy asymilacji, które do tej pory przebiegały niemalże bezkonfliktowo zaczęły wyglądać inaczej, już bez wzajemnego współdziałania. Kraje wysoko uprzemysłowione, które w ostatnich latach borykają się z trudnościami ekonomicznymi, w których gospodarka przechodzi wielowymiarowy kryzys, w aspekcie społecznym zmagają się również z nowym podejściem rdzennych mieszkańców do ludności napływowej przekraczającej granice ze względu na bezrobocie w kraju, z którego pochodzą imigrantów ekonomicznych. Część społeczeństwa, która utraciła pracę, za ten fakt obwinia właśnie imigrantów. To w nich widzi wręcz przyczynę swojego położenia ekonomicznego i społecznego. W takich przypadkach na rynku pracy powstaje segmentacja w różnych dziedzinach i branżach. Wraz z segmentacją widoczne stają się zależności w dostępie do pracy przez osoby nisko i wysoko wykwalifikowane, osoby przynależne do różnych grup etnicznych, kobiety i mężczyzn oraz osoby z uregulowanym lub nie statusem prawnym na terenie danego kraju.

Migracja ekonomiczna odzwierciedla również dążenie nie tylko pojedynczych jednostek do poprawy swojego statusu ekonomicznego, społecznego i politycznego, ale odzwierciedla również dążenia całych rodzin czy nieformalnych grup lokalnych (wspólnot). To właśnie w takich grupach mogą być rozważane i podejmowane decyzje o emigracji zarobkowej jednej lub wielu osób poszukujących różnych źródeł dochodu. Zróżnicowane źródła dochodu pozwalają na planowanie działań ekonomiczno-gospodarczych danych społeczności, a „ich" człowiek na emigracji staje się siła napędową wielu

inwestycji na rynku lokalnym. Odnoszą bowiem w tym przypadku wymierne korzyści w wyniku transferu dóbr materialnych do kraju pochodzenia migrantów ekonomicznych. Profity pozwalają na wymianę ekonomiczną pomiędzy różnymi częściami świata, a więc migracja ekonomiczna ma zasięg globalny.
Możemy przytaczać wiele argumentów na temat korzyści płynących dla obu stron z migracji ekonomicznej, ale każdy z tych argumentów zostanie podważony w momencie reemigracji. Możliwość powrotu jest naturalnym elementem takiej migracji i prawem każdego migranta.

Oblicza współczesnego uchodźctwa

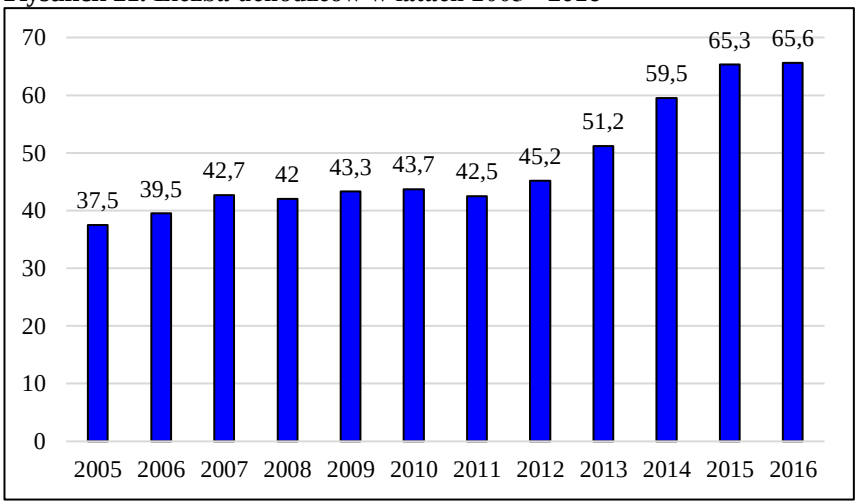
W prawie międzynarodowym status oraz prawa uchodźcy reguluje tzw. Konwencja Genewska - Konwencja Dotycząca Statusu Uchodźców, sporządzona w Genewie dnia 28 lipca 1951 r. (Dz. U. z 1991 r. Nr 119, poz. 515 i 517). Termin „uchodźca" stosuje się do osoby, która (...) *na skutek uzasadnionej obawy przed prześladowaniem z powodu swojej rasy, religii, narodowości, przynależności do określonej grupy społecznej lub z powodu przekonań politycznych przebywa poza granicami państwa, którego jest obywatelem, i nie może lub nie chce z powodu tych obaw korzystać z ochrony tego państwa, albo która nie ma żadnego obywatelstwa i znajdując się na skutek podobnych zdarzeń poza państwem swojego dawnego stałego zamieszkania, nie może lub nie chce z powodu tych obaw powrócić do tego państwa* (...) (Konwencja Genewska, 1951, art. 1). Początkowo zapisy Konwencji Genewskiej obejmowały swoim zakresem tylko uchodźców z Europy, którzy pojawili się po II wojnie światowej, natomiast wraz z podpisaniem Protokołu Nowojorskiego w 1967 roku stała się aktem uniwersalnym, pozbawionym ograniczeń czasowych i terytorialnych. Polska przystąpiła do Konwencji Genewskiej i Protokołu Nowojorskiego w 1991 roku[69]. Przytoczona definicja terminu „uchodźca" nie obejmuje w swym zakresie „migrantów ekonomicznych", którzy opuścili swój kraj z przyczyn skrajnej nędzy, a więc faktycznie nastąpił przymus ekonomiczny. Konwencja Genewska jako podstawowy akt prawa międzynarodowego regulujący zagadnienia ochrony uchodźców nie przewiduje udzielenia ochrony w sytuacjach, gdy okoliczności

[69] http://www.info-migrator.pl/informacje-prawne/opisy-ustaw/3428-konwencja-genewska-z-28-lipca-1951-r-dotyczaca-statusu-uchodzcow.

zmusiły jednostkę do opuszczenia kraju. Są to okoliczności spowodowane albo (1) przez siły przyrody (*natural disasters*), albo (2) przez bezpośrednie działanie człowieka (*man-made disasters*). Pierwsza kategoria przyczyn (susza, tsunami, powódź, trzęsienie ziemi itp.) nie jest przewidziana w Konwencji Genewskiej, przez co osoby, które opuściły swój kraj z tego powodu, nie podlegają zapisom Konwencji (Gracz, 2007, s. 33). Zasada „*nonrefoulement*" daje gwarancję uchodźcy, że nie zostanie on wydalony lub zawrócony z kraju (...) *do granicy terytoriów, gdzie jego życiu lub wolności zagrażałoby niebezpieczeństwo ze względu na jego rasę, religię, obywatelstwo, przynależność do określonej grupy społecznej lub przekonania polityczne* (...) (Konwencja Genewska, 1951, art. 33). Rozpatrując problematykę uchodźctwa należy wskazać istotne wydarzenia z kart historii, które to ukształtowały obraz migracji przymusowej. Wśród najpoważniejszych kryzysów uchodźczych ostatnich kilkudziesięciu lat wymienić można, np. powstanie węgierskie (1956 r., 200 tys. uchodźców), wojnę w Algierii (1956 r., 200 tys.), konflikt w Liberii (1989 r., 700 tys.), konflikt w Sierra Leone (1997 r., 400 tys.), konflikt w Pakistanie (1971 r., 10 mln.), konflikt w Afganistanie (od 1981 r., ponad 6 mln.), konflikt w Kolumbii (1997 r., 900 tys.), konflikt w byłej Jugosławii (1992 r., ponad 3,5 mln.), konflikt w Kosowie (1999 r., 1 mln. uchodźców albańskich), konflikty na Zakaukaziu (1990-2010 r., 2 mln. uchodźców), czystki etniczne w rejonie Wielkich Jezior Afrykańskich (1990-1993 r., 1,3 mln.), konflikt w Syrii (od 2011 r. do końca 2015 r., 4,9 mln. zostało uchodźcami, a 6,5 mln. - wewnętrznymi przesiedleńcami), wojna domowa w Jemenie (2015 r., 2,5 mln.), konflikt w Iraku (od 2003 r., 4,4 mln. ludzi zostało wewnętrznie przesiedlonych, a 250 tys. stało się uchodźcami). Pod koniec 2010 roku na świecie, zgodnie z danymi opublikowanymi przez UNHCR, było 43,7 mln. osób przymusowo przesiedlonych (w tym 15,4 mln. uchodźców przebywających poza granicami państwa lub zamieszkania; 27,5 mln. uchodźców wewnętrznych i ok. 850 tys. osób ubiegających się o status uchodźcy). Konflikty i prześladowania w 2015 roku spowodowały nagły wzrost liczby przymusowych przesiedleń, który osiągnął dotychczas nienotowany poziom 65,3 mln. osób. W porównaniu z 2014 rokiem liczba osób przymusowo przesiedlonych wzrosła o 5,8 mln. 65,3 mln. przesiedlonych to 3,2 mln. ludzi, którzy na koniec 2015 roku oczekiwali na decyzję o nadanie statusu uchodźcy (kolejny rekord w statystykach),

21,3 mln. uchodźców (1,8 mln. więcej niż rok wcześniej i jednocześnie najwięcej od wczesnych lat 90.) oraz 40,8 mln. osób, które musiały opuścić swoje domy w obawie przed wojną i prześladowaniem, ale nadal przebywały na obszarze swojego kraju (wzrost o 2,6 mln. w porównaniu z 2014 rokiem i kolejny rekord)[70]. Z raportu *Global Trends*, największej i najważniejszej publikacji na temat przesiedleń przygotowywanej przez UNHCR, wynika, że na koniec 2016 roku liczba osób przymusowo przesiedlonych na całym świecie wyniosła 65,6 mln. – była więc o 300 tys. wyższa niż rok wcześniej. Te statystyki pokazują, jak ogromne rzesze ludzi potrzebują wsparcia i ochrony. Liczba 65,6 mln. składa się z trzech ważnych elementów: (1) liczba uchodźców, która wyniosła rekordowe 22,5 mln., (2) liczba osób, które musiały opuścić swój dom, ale pozostają w swoich krajach, na koniec 2016 roku 40,3 mln. oraz (3) liczba osób ubiegających się o nadanie statusu uchodźcy, na koniec 2016 roku wyniosła ona 2,8 mln.[71].

Rysunek 21. Liczba uchodźców w latach 2005 - 2016



Źródło: opracowanie własne na podstawie *Raportu Global Trends 2016, http://www.unhcr.org/globaltrends2016/. (on-line: 2017.06.20).*

[70] http://www.unhcr.org/pl/363-plwiadomosci2016653-mln-osob-przymusowo-przesiedlonych-kolejny-rekord-w-statystykach-html.html
[71] http://www.unhcr.org/pl/2858-wojny-przemoc-i-przesladowania-przyczyna-rekordowej-liczby-przymusowych-przesiedlen.html.

Powyższe dane statystyczne odczytane z corocznych raportów[72] pozwoliły na sporządzenie rysunku 21, który przedstawia liczbę uchodźców od roku 2005 do roku 2016. Uchodźctwo jest problemem globalnym, a jego skutki są odczuwalne nie tylko w krajach, z których pochodzą uchodźcy, ale również w krajach, do których uchodźcy się udają. To nie są tylko statystki, które przedstawiają liczbę osób, które zostały zmuszone do opuszczenia swoich domów, ale to również zagrożenie, które jest bezpośrednio związane z przemieszczaniem się zbiorowości ludzkich. Wędrówki ludności przymusowo zmuszonej do migracji niejednokrotnie są „sterowane" przez zorganizowane grupy przestępcze, czerpiące korzyści materialne z ułatwienia, czy też zagwarantowania ucieczki. W strefach konfliktów zbrojnych, np. na terytorium Syrii i Iraku, informacje o „możliwych kierunkach" ucieczki są przekazywane przez służby tzw. Państwa Islamskiego. Wraz z „falą" migrantów do innych krajów mogą przemieszczać się również osoby zaangażowane w działania terrorystyczne o różnym podłożu.

Kontrola migracji

Ochrona UE przed przestępczością, nielegalną migracją oraz aktami terrorystycznymi stała się jedną z podstawowych zasad wprowadzenia tzw. strefy Schengen. Porozumienie stanowiące powstanie tej strefy zostało podpisane 14 czerwca 1985 roku w luksemburskim mieście Schengen - pomiędzy Francją, Niemcami i krajami Beneluksu. Do dorobku prawnego UE weszło na mocy specjalnego protokołu w Traktacie Amsterdamskim (Grzelak, 2008, s. 28). W 1995 roku, wraz z wprowadzeniem dorobku prawnego, został stworzony System Informatyczny Schengen (SIS). System ten umożliwiał przekazywanie pomiędzy państwami informacji w zakresie spraw wewnętrznych i wymiaru sprawiedliwości. Większość zarejestrowanych w systemie osób to osoby przebywające na terenie UE a pochodzące z innych krajów. System stał się instrumentem, który umożliwił kontrolę wewnątrz UE, przy zniesionych kontrolach na wewnętrznych granicach Państw Członkowskich Unii Europejskiej (PC UE). Wydarzenia z 9 września 2001 roku, związane z aktami terrorystycznymi, spowodowały nowe podejście do SIS i jego aktualizację

[72] http://www.unhcr.org/globaltrends2016/.

w celu zwiększenia przeciwdziałaniu terroryzmowi. Zainicjowano projekt SIS II (rozszerzony o dane biometryczne w stosunku do SIS) oraz VIS (*Visa Information System*), które skuteczniej mogą zabezpieczać państwa członkowskie UE przed przemieszczaniem czynnych terrorystów (Tomaszycki, Kuźniar, Łapińska, 2017, s. 158). Zapisy Konwencji Genewskiej oraz Protokołu Nowojorskiego dają podstawy prawne do tworzenia aktów prawa krajowego lub regionalnego, obejmujących unie państw, np.: Unia Europejska. Na poziomie Unii Europejskiej zasady ochrony prawnej oraz przemieszczania się uchodźców w jej obrębie są regulowane poprzez tzw. system dubliński (Konwencja Dublińska, 1990 roku). Zasady prawa obowiązujące na terenie Unii Europejskiej nie dają gwarancji wszechstronnego rozpatrzenia wniosków migrantów, czy też uchodźców, przez poszczególne PC UE. Wątpliwości pojawiają się również podczas ustalania, które państwo członkowskie odpowiada za rozpatrywanie poszczególnych wniosków o azyl, a zwłaszcza w czasie napierającej fali uchodźców. Obowiązujące przepisy (tzw. system dubliński) nie zostały zaprojektowane dla zapewnienia zrównoważonego podziału odpowiedzialności przez poszczególne PC UE oraz nie gwarantują terminowego rozpatrywania wniosków w czasie masowego napływu imigrantów. Kryzys migracyjny ostatnich lat w basenie Morza Śródziemnego wykazał, że dotychczasowe mechanizmy oraz polityka migracyjna UE nie sprawdzają się. Komisja Europejska dostrzegając wagę zaistniałej sytuacji, wydała 6 kwietnia 2016 roku komunikat, w którym przedstawiła propozycję reformy wspólnego europejskiego systemu azylowego, polegającej na utworzeniu bardziej sprawiedliwego, skuteczniejszego i bardziej zrównoważonego systemu rozdzielania wniosków o udzielenie azylu między poszczególne PC UE. W swych działaniach wystąpiła także z wnioskiem o przekształcenie European Asylum Support Office (EASO) w pełnoprawną Agencję Unii Europejskiej ds. Azylu (Krzemińska, Tomaszycki, 2017. s. 135-136). Chodzi tu również o wzmocnienie i rozszerzenie roli tej agencji oraz o zwiększenie możliwości zbierania informacji o uchodźcach. Jednym z elementów tej informacji jest unijna baza danych odcisków palców Eurodac[73] (*European Dactiloscopie*).

[73] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. *w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania* rozporządzenia (UE) nr 604/2013 *w sprawie ustanowienia kryteriów i mechanizmów*

System ten został utworzony w celu lepszego zarządzania systemem azylowym i przeciwdziałania nielegalnej migracji w oparciu o dane biometryczne. Składa się z: (1) skomputeryzowanej centralnej bazy danych daktyloskopijnych (tzw. System Centralny) i (2) infrastruktury łączności między systemem centralnym a państwami członkowskimi, zapewniającej szyfrowaną wirtualną sieć służącą do przekazywania danych Eurodac[74]. W Rozporządzeniu nr 603 określone zostały warunki występowania uprawnionych organów z wnioskami o porównanie danych daktyloskopijnych z danymi zgromadzonymi w systemie Eurodac na potrzeby zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub ścigania. W Polsce wyznaczonymi organami są jednostki operacyjne Policji, Straży Granicznej (SG), Agencji Bezpieczeństwa Wewnętrznego (ABW), Centralnego Biura Antykorupcyjnego (CBA). Każdy z powyższych organów, w ramach własnej organizacji, wyznaczył co najmniej jeden organ weryfikujący (Staż Graniczna wyznaczyła osiem organów weryfikujących, po jednym w każdym oddziale SG). Dla Policji funkcję organu weryfikującego pełni CLKP (Kot, Tomaszycki, 2017. s. 167-168). Wyznaczone organy (jednostki operacyjne) w uzasadnionych przypadkach, gdy jest to niezbędne do zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, dokonują sprawdzeń i weryfikacji danych identyfikacyjnych osoby podejrzanej. Podstawy prawne są realizowane poprzez działania organów państwowych (służby graniczne) i międzynarodowych (np. Frontex) na zewnętrznych granicach Unii Europejskiej. Wraz ze zgłoszeniem się uchodźcy do krajowych organów z wnioskiem o udzielenie ochrony na terenie danego PC UE, pobierane są dane biometryczne, które służą na terenie całej Unii Europejskiej do weryfikacji danych identyfikacyjnych każdego uchodźcy. Takie działania są standardowe

ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego oraz zmieniające rozporządzenie (UE) nr 1077/2011 *ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości* (DU UE L180 z 2013 r.).

[74] Art. 3 ust.1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 603/2013 z dnia 26.06.2013 r. *w sprawie (…).*

i wymagają od wszystkich PC UE jednolitego działania opartego o przepisy, tak unijne, jak i krajowe. Jednakże wśród uchodźców, tych którzy w sposób nielegalny docierają do UE, panuje przekonanie, że raz pobrane dane biometryczne „zamykają im drogę do lepszego świata". Informacja taka jest rozpowszechniana poprzez różne kanały komunikacji realnej i wirtualnej i stanowi narzędzie w rękach grup przestępczych zajmujących się przemytem ludzi. Przepisy UE wskazują, że uchodźca zweryfikowany w jakimkolwiek PC zostanie odesłany do państwa, na terytorium którego złożył swój „pierwszy" wniosek o ochronę w UE.

Zagrożenia wynikające z migracji

Tak jak proces migracji jest skomplikowany i wielopłaszczyznowy, tak zagrożenia z niego płynące są wielorakie i w niektórych przypadkach trudne do określenia. Jednakże podejmę próbę krótkiej syntezy tego zjawiska. Zagrożenia te mają charakter wieloaspektowy, tj. prawny, społeczny, ekonomiczny, czy też polityczny. Każde z zagrożeń może wystąpić jako samoistny byt lub też być kompilacją wielu okoliczności sprzyjających poczuciu braku bezpieczeństwa. Wśród zagrożeń towarzyszących migracji możemy miedzy innymi wyszczególnić: (1) tworzenie grup przestępczych, (2) wzrost przestępczości, (3) przemyt ludzi, narkotyków, broni oraz dóbr materialnych, (4) handel ludźmi i narządami ludzkimi, (5) ataki terrorystyczne, (6) szerzenie chorób zakaźnych, (7) radykalizacja życia społecznego, (8) fundamentalizm, (9) dżihad, (10) zachwianie rynku pracy, (11) tworzenie enklaw na terenie kraju docelowego.

Tworzenie grup przestępczych stanowi przyczółek w działalności indywidualnych przestępców, jak też działających pod „przykrywką" innych organizacji (np. tzw. Państwa Islamskiego) w skomplikowanej sytuacji uchodźców z Iraku, czy też pochodzących z Syrii. Wraz a falą uchodźców przemieszczają się w kierunku Unii Europejskiej ludzie wchodzący w skład zorganizowanych grup przestępczych, wykorzystując naiwność oraz emocje uchodźców. Chęć dotarcia do „Ziemi obiecanej" i iluzoryczne wsparcie, w celu osiągnięcia celu podróży, przysłania zdrowy rozsądek i rozpoznanie prawdziwych intencji członków takich grup. Działania grup przestępczych zajmujących się „wspieraniem" uchodźców cechują się: (1) zorganizowaniem

w działaniach, (2) współdziałaniem zawsze więcej niż jednej osoby, (3) hierarchiczną strukturą wewnętrzną, (4) planowością i podziałem zadań, (5) trwałością działania, (6) przemocą w działaniu, (7) nastawieniem na popełnianie przestępstw, (8) popełnianiem przestępstw, (9) celem zdobycia władzy nad ludźmi będącymi w trudnej sytuacji lub zysków, (10) licznymi strefami wpływów na terytoriach ich działalności, (11) wymiarem międzynarodowym, bo problematyka uchodźctwa taka jest, (12) hermetycznością zewnętrzną i wewnętrzną, (13) monopolizacją rynku oraz (14) legalizowaniem nielegalnych zysków (Miczkowska, 2009, s. 124).

Wraz z trwającym procesem migracyjnym, czy też uchodźczym, **wzrasta liczba popełnianych przestępstw** przez migrantów i w stosunku do tych osób. Powodami takich zachowań jest frustracja, złość i rozgoryczenie odmową uzyskania azylu, np. w Niemczech lub też skomplikowaną i długotrwała procedurą uzyskania azylu[75]. Liczba imigrantów podejrzanych o popełnienie przestępstw powiększyła się w roku 2016 o 52,7 % i wynosiła do 174 438. Nie jest to jednak wysoki wzrost w porównaniu z rokiem 2015, w którym, wg statystyk Federalnego Urzędu Kryminalnego, wzrost przestępczości wśród imigrantów wyniósł 91% w porównaniu z rokiem 2014. Nota bene: w roku 2015 przybyło do Niemiec 890 tys. imigrantów, w 2016 już tylko ponad 300 tys.[76]. Wraz z napływem migrantów wzrasta także liczba przestępstw, których ofiarami są azylanci. Liczba ataków na ośrodki dla uchodźców wzrosła w Niemczech 16krotnie od roku 2013, a liczba rasistowskich i ksenofobicznych przestępstw z nienawiści z użyciem przemocy o 87%. W roku 2013 zanotowano 693 takie przestępstwa, a w roku 2015 aż 1295[77]. Same liczby wskazują, że wzrost przestępczości wymyka się spod kontroli i władze nie tylko Niemiec, ale także innych PC UE, zmuszone są do podjęcia szeregu działań zaradczych.

Wraz ze wzrostem przestępczości związanej z migracją, niektóre jej kategorie uwidaczniają się bardziej. Są to przede wszystkim **przemyt ludzi, narkotyków, broni oraz dóbr materialnych**. I tu możemy po raz kolejny wskazać, że wraz z falą nielegalnej migracji, zorganizowane grupy przestępcze wykorzystują

[75] http://www.dw.com/pl/niemcy-migranci-i-przest%C4%99pczo%C5%9B%C4%87/a-38446517.
[76] http://www.rp.pl/Uchodzcy/304249891-Niemcy-Wzrost-przestepczosci-wsrod-mlodych-imigrantow.html.
[77] https://amnesty.org.pl/niemcy-wzrost-przestepstw-z-nienawisci/.

uchodźców w celu dokonywania przemytu. Bardzo zdecydowane słowa wygłosił Prezydent Grecji Prokopis Pawlopulos w stosunku do władz Tureckich, aczkolwiek nie miał na myśli Kierownictwa Państwa Tureckiego. (…) *dzięki naszym wysuniętym placówkom na wyspach zdobyliśmy dowody, że władze portowe współpracują z przemytnikami"* (…), wskazał, że (…) *ma na to dowody, znamy przypadki, gdy przemytnikom miała zostać udzielona pomoc. Przemyt ludzi określił mianem „niewolnictwa" (...)*[78].Działania przemytnicze do Unii Europejskiej stały się znaczącym źródłem dochodów grup przestępczych z Rosji, Ukrainy, Turcji, Syrii, Iraku i osób współpracujących z Państwem Islamskim. Proceder ten stał się bardziej dochodowym biznesem niż handel narkotykami czy bronią. Gangi przemytników ludzi zarobiły na nich w roku 2015 nawet 6 mld euro, jak wynika z raportu przygotowanego przez Europol[79]. Zdaniem Dyrektora Europolu (…) *z naszych danych wynika, że 90% imigrantów przybywających do Europy korzystało z usług organizacji przestępczych* (…)[80].Działania poszczególnych PC UE leżących w obrębie Morza Śródziemnego oraz organizacji międzynarodowych w opanowaniu oraz zablokowaniu przemytu ludzi do UE z jednej strony może się przyczynić do poprawy bezpieczeństwa, a z drugiej - do skuteczniejszych działań związanych z pokonaniem kryzysu migracyjnego. Warto w tym miejscu zaznaczyć, że obok przemytu ludzi istnieje inny równie groźny element przemytu. Jest nim przemyt i handel narkotykami. Czytając raport Europejskiego Centrum Monitorowania Narkotyków i Narkomanii (EMCDDA), możemy stwierdzić, że (…) *według ostrożnych szacunków rynek detalicznej sprzedaży nielegalnych substancji w Unii Europejskiej wart był w 2013 r. 24,3 miliarda euro (prawdopodobny przedział wartości to od 21 do 31 miliardów euro)* (…)[81].Grupy przestępcze przemycające wraz z falą uchodźców narkotyki do UE mają rozpoznanie „rynku" narkotykowego i dokładnie wiedzą, jak można dostarczyć „towar" do klienta i jaka będzie gratyfikacja ich działań. Jednakże służby odpowiedzialne za ograniczenie przemytu narkotyków odnoszą liczne sukcesy w zwalczaniu

[78] http://www.rp.pl/Uchodzcy/160119321-Grecja-oskarza-Turcje-o-przemyt-imigrantow.html.
[79] https://www.europol.europa.eu/publications-documents/migrant-smuggling-in-eu.
[80] http://www.polskatimes.pl/fakty/swiat/a/przemytnicy-pomagaja-uchodzcom-dostac-sie-do-europy-to-biznes-lepszy-niz-handel-bronia,9441109/.
[81] http://gis.gov.pl/images/%C5%9Brodki_zast%C4%99pcze/%C5%9Bz/raport_eur._nar_2016.pdf.

tego procederu. Dyrektor departamentu do zwalczania przestępczości zorganizowanej Europolu Michael Rauschenbach wskazuje, że (…) *dla handlarzy narkotykami, coraz atrakcyjniejszym interesem staje się nielegalna imigracja. Mamy konkretne informacje, że groźni przestępcy, czerpią coraz większe zyski z przemytu ludzi. Przemyt ludzi jest mniej ryzykowny dla przestępców niż przemyt narkotyków. Teraz swoje działania kierują na zorganizowanie sieci przemytu ludzi do Unii Europejskiej z Bliskiego Wschodu i Afryki* (…)[82].Obok przemytu ludzi i narkotyków duży udział grup przestępczych jest odnotowywany w zakresie przemytu broni i „cudzych" dzieci do krajów Europy Zachodniej. Niejednokrotnie w mediach zamieszczane są informacje o udaremnionych próbach przemytu broni do PC UE (…) *Włoska policja udaremniła gigantyczny przemyt broni. 800 sztuk karabinów transportowano przez półwysep Apeniński z Turcji w kierunku Niemiec, Belgii i Holandii w naczepie zarejestrowanej w Danii ciężarówki. Samochód z kontrabandą zatrzymano w Trieście, przy granicy ze Słowenią. Przechwycenie ładunku to zasługa - podkreślają włoskie media - uszczelnienia granic po zamachach w Paryżu, w których z rąk terrorystów powiązanych z tzw. Państwem Islamskim zginęło 130 osób* (…)[83].Omawiając zagadnienie przemytu należy zwrócić uwagę na jeszcze jeden aspekt tego procederu, a mianowicie na zmianę jakościową. Grupy przestępcze wykorzystując uchodźców „przekazują" im do przemycenia rzeczy o bardzo dużej wartości materialnej, m.in. kamienie szlachetne i półszlachetne, cenne kruszce oraz pieniądze.

Obok przemytu ludzi zjawiskiem, które wiąże się z migracją jest **handel ludźmi i ich narządami**. I po raz kolejny grupy przestępcze w celu osiągnięcia zysków nie liczą się z ludźmi i ich życiem. Człowiek staje się takim samy towarem jak jedzenie, ubranie, czy też artykuły niezbędne do życia. W Unii Europejskiej temat handlu ludźmi jest szczególnie akcentowany. Dotyczy to zarówno aktów prawnych, jak również działań służb odpowiedzianych za bezpieczeństwo. Głównym aktem prawnym jest Dyrektywa Parlamentu Europejskiego i Rady 2011/36/UE z dnia 5 kwietnia 2011 roku. w sprawie zapobiegania handlowi ludźmi i zwalczania tego procederu oraz ochrony ofiar, zastępująca decyzję

[82] http://www.dw.com/pl/europol-handlarze-narkotykami-aktywni-w-przemycie-ludzi/a-36999394.
[83] https://wp.tv/i,gigantyczny-przemyt-broni-do-ue-udaremniony,mid,1828277,cid,4051,klip.html?ticaid=619888.

ramową Rady 2002/629/WSiSW (Dz. UE L 101/1. z 15.4.2011). Kolejnym zagadnieniem, które jest związane z handlem „żywym towarem" jest handel narządami ludzkimi (tzw. *organ trafficking*). Uchodźcy, którzy wydali wszystkie oszczędności na podróż do „lepszego świata" płacą swoimi organami za taką podróż będąc dobrowolnymi dawcami. Sytuacja zmienia się, gdy narządy potrzebne do transplantacji są pobierane po śmierci człowieka w wyniku działania zbrodniczego.

Innym, ale jakże istotnym zagrożeniem, które może ze sobą nieść migracja są **ataki terrorystyczne**. W raporcie Europolu[84] sporządzonym w roku 2016 nie ma jednoznacznej odpowiedzi, czy terroryści w sposób systematyczny dostają się do Europy wraz z falą uchodźców. Jednakże wydarzenia roku 2016 (***22 marca*** *– dwa zamachy w Brukseli, lotnisku w Zaventem i przy stacji metra Maelbeek, w pobliżu siedzib instytucji unijnych. Zginęły 32 osoby i trzech zamachowców samobójców, a ponad 315 osób zostało rannych*. ***12 czerwca*** *– strzelanina w klubie nocnym Pulse w Orlando w amerykańskim stanie Floryda. Zginęło w niej ponad 50 osób, a 53 osoby zostały ranne,* ***14 lipca*** *– w święto narodowe Francji, zamachowiec wjechał ciężarówką w tłum spacerujący po Promenadzie Anglików w Nicei. Zginęły 84 osoby oraz zamachowiec, a ponad 200 zostało rannych*) oraz początku roku 2017 (***22 maja*** *- Manchester Arena w Manchesterze. Spowodował 23 ofiary śmiertelne (w tym sprawca), a rannych zostało ok. 119 osób*) wskazują, że inspiratorami lub wykonawcami byli ludzie związani z tzw. Państwem Islamskim. Przedstawione przykłady nie odzwierciedlają wszystkich zamachów, które były dziełem ludzi związanych z Państwem Islamskim. Jest ich znacznie więcej i jasno pokazują, że nie ma granic na tego typu działalność.

Czy migracja może być zagrożeniem związanym z **przenoszeniem chorób zakaźnych**? Przykłady mówią, że należy być w tej kwestii bardzo ostrożnym. Duński Państwowy Instytut ds. Szczepień poinformował o wykryciu dwóch przypadków błonicy wśród imigrantów, którzy w ubiegłym roku trafili do Danii. Obydwie zakażone osoby pochodziły z Libii. Władze w Kopenhadze zignorowały zalecenie Światowej Organizacji Zdrowia (WHO) i nie zaszczepiły

[84] https://www.europol.europa.eu/publications-documents/migrant-smuggling-in-eu.

nowo przybyłych[85]. Choroba ta w Dani nie występowała od 18 lat. Została „przywieziona" wraz z falą migrantów z Afryki. W Szwajcarii w 2016 roku odnotowano siedem przypadków gruźlicy, przy czym nosicielami choroby byli imigranci z państw Afryki (*Somalia, Etiopia oraz Erytrea*), przebywający w ośrodkach dla azylantów. Od tego czasu odnotowano kolejne przypadki zachorowań: sześć w Niemczech, dwa w Austrii oraz jeden w Szwecji[86]. Oczywiście możemy dyskutować, czy te dane są prawdziwe, czy też nie, ale jedno jest pewne: taka informacja znalazła się już w sieci internetowej – w cyberprzestrzeni.

Dwa kolejne zagadnienia związane z zagrożeniami dotyczą **radykalizacji życia społecznego** oraz **fundamentalizmowi**. Można powiedzieć, że oba ww. pojęcia są ze sobą powiązane i odnoszą się do zmiany sposobu myślenia i podejścia do religii oraz życia społecznego w kontekście masowej migracji. Fundamentalizm wiąże się z przeobrażeniem świata z wykorzystaniem przemocy, powrotem do „starych" zasad wiary, powrotem do korzeni. Jaskrawym przykładem jest fundamentalizm islamski na Bliskim Wschodzie, który w sposób szczególny określa powiązanie religii z kwestiami rozwoju gospodarczego, ekonomicznego, społecznego oraz władz geopolitycznych w ujęciu wspólnotowym (Bruce, 2006, s. 17-18). W islamie fundamentalizm określano jako powrót do korzeni wiary, do religii przodków, do stosowania w życiu codziennym zasad Koranu i tradycji proroka Mahometa. Jako przyczynę wskazywano oddzielenie sfery świeckiej od religijnej, co wiązało się z modelem europejskim funkcjonowania życia społecznego i politycznego. Fundamentalizm islamski wręcz wskazuje, że należy upolitycznić religię, a w konsekwencji odrzucić wszystko co europejskie i zachodnie (Tabi, 1995, s. 6-7). I tu możemy w korelacji z fundamentalizmem opisać radykalizm, który jest odpowiedzią na działania imigrantów z krajów islamskich. Radykalizacja związana jest z odpowiedzią środowisk prawicowych, i nie tylko, na zachowania społeczne migrantów. Odrzucenie „co nie nasze", stanowi motto działań licznych organizacji radykalnych. Wiąże się to z brakiem tolerancji dla „obcych" w życiu społecznym.

[85] https://www.wprost.pl/529961/Grozna-choroba-wykryta-w-Danii-Zakazeni-to-imigranci.
[86] http://pl.blastingnews.com/polityka/2017/01/imigranci-przywlekli-grozne-choroby-gdy-kaczynski-ostrzegal-mowiono-to-rasizm-001438649.html.

Dżihad można przetłumaczyć to z języka arabskiego jako „*zmaganie, walka*", nakłada on bowiem na wyznawcę islamu obowiązek szerzenia i obrony wiary muzułmańskiej. Może on być realizowany za pomocą metody pokojowej lub też brutalnej poprzez udział w tak zwanej „świętej wojnie". Śmierć w „świętej wojnie" daje wyznawcy islamu natychmiastowe zbawienie, otwartą drogę do raju. Prowadzi się go poprzez przezwyciężanie własnych słabości, jak też walcząc z niewiernymi. Niejednokrotnie Dżihad jest rozumiany jako każda wojna prowadzona w imię islamu, a obecnie jako walka z cywilizacją Zachodu.
Migracja jako zagrożenie związane z **zachwianiem rynku pracy** wiąże się z relacjami pracodawca-pracownik. Popyt na wysoko wykwalifikowanych pracowników stanowi siłę napędową każdej rozwijającej się gospodarki. Czy w wyniku ruchów migracyjnych rynek pracy jest stabilny, czy też następuje odpływ wykwalifikowanych pracowników z tego rynku i napływ pracowników bez kwalifikacji? Oczywiście patrząc na statystki bezrobocia w Polsce w latach 2016 – 2017 możemy powiedzieć, że przy spadku bezrobocia, nadal rynek pracy potrzebuje pracowników wysoko wykwalifikowanych. W ciągu ostatniego roku o 30% wzrosła w gospodarce liczba wakatów, pomimo napływu ponad 1 miliona dodatkowych pracowników z Ukrainy. Dziś wyraźnie widzimy, że brak dostępności rąk do pracy może w przyszłości negatywnie wpływać na rozwój gospodarczy naszego kraju[87]. Czynniki makroekonomiczne oraz polityczne decyzje UE mają duży wpływ na rynek pracy w Polsce. Wyrazem tego jest możliwość podróżowania po Europie przez mieszkańców Ukrainy bez wiz. Spowodowało to, że stawka minimalna za godzinę pracy obywatela Ukrainy zbliżyła się do stawki Polaka.
Ostatnim wymienionym przeze mnie zagrożeniem, ale jest jeszcze wiele innych, jest **tworzenie enklaw na terenie kraju docelowego** przez migrantów. Przybywający migranci mają tendencję do zamieszkiwania w osiedlach już zamieszkałych przez ich rodaków. Zamieszkiwanie w enklawach etnicznych może przekładać się na gorszą integrację społeczną, w następstwie niższą aktywność zawodową, wyższe bezrobocie i większe zależności od świadczeń społecznych. Tworzenie się takich enklaw nie jest tylko i wyłącznie zależne

[87] http://www.pulshr.pl/rekrutacja/bezrobocie-imigranci-emigracja-jak-wygladal-polski-rynek-pracy-w-2016-r,40236.html.

od przybywających migrantów (czynniki wewnętrze), lecz stanowi wymiar polityki społecznej i socjalnej danego państwa (czynniki zewnętrzne). Do czynników sprzyjających tworzeniu enklaw etnicznych należą przede wszystkim te, które wynikają z sytuacji migracyjnej i postaw osób zmieniających miejsce pobytu, a mianowicie (Suchocka, 2014, s. 241):

- zmiana wywołana nowymi warunkami i konieczność zaadaptowania się do nich, przystosowania się do życia w obcym kulturowo kraju, zwłaszcza w sytuacji braku znajomości języka, obowiązującego prawa, panujących obyczajów, poszukiwania pracy i mieszkania;
- występowanie kolejnych fal migracji, migracja grup, a nie pojedynczych jednostek;
- migracje łańcuchowe i występowanie sieci powiązań między osiadłymi a przybywającymi migrantami.

Tworzenie enklaw, i w konsekwencji - odizolowanych skupisk ludzkich - powoduje powstanie swoistych „państw-dzielnic" bez jakichkolwiek reguł funkcjonowania. Wytwarzają się lokalne zasady współżycia społecznego, pozbawione kontroli przez ogramy państwowe, rolę służb państwowych przejmują zorganizowane grupy, niejednokrotnie grupy przestępcze. Społeczności w takich enklawach poddawane są działaniom radykalizującym. Enklawy muzułmańskie w miastach Europy Zachodniej przyjmują wręcz fundamentalistyczny sposób funkcjonowania. Taki obraz tych społeczności nie jest akceptowany przez mieszkańców danego miasta i dochodzi do napięć etnicznych.

Przedstawiona krótka analiza niektórych zagrożeń, które niesie migracja wskazuje, że są to wielopłaszczyznowe aspekty bezpieczeństwa stanowiące przyczynek do innego spojrzenia na ten proces. Działania Unii Europejskiej zmierzające do ograniczenia migracji i lepszej ochrony jej zewnętrznych granic stają działaniami priorytetowymi.

Rzeczywistość – realna czy wirtualna?

Budowanie relacji społecznych w dużej mierze zależy od funkcjonowania poszczególnych grup, a zatem od procesu socjalizacji. My, tu i teraz, stanowi o sposobie patrzenia na otaczającą nas rzeczywistość. Postrzegając każdego z nas osobno lub też tworząc relacje mówimy o powstaniu pewnych zależności.

Jeśli odbywa się to w świecie realnym, to i relacje są realne. Nie wychodzimy poza krąg naszych spostrzeżeń, a nasze zmysły rejestrują następujące zmiany. Realność sytuacji pozwala na wnikliwą analizę stanu zachowań grupowych i interakcji. Odnotowujemy zaistniałe fakty i staramy się weryfikować źródła informacji. Chcemy, aby w naszym życiu te źródła były wiarygodne, a jeśli mamy wątpliwość, to dokonujemy ich weryfikacji. Oczywiście nasza rzeczywistość wiąże się z naszym przygotowaniem do jej postrzegania, to, co robimy, jest związane z naszymi intencjami, nadziejami i chęciami. Poprzez pryzmat swoich doświadczeń odbieramy to, co wokół nas się dzieje. To zmysły pozwalają nam na wszechstronne odbieranie bodźców zewnętrznych i wewnętrzne ich ocenianie. Jeżeli posiadamy odpowiednią wiedzę popartą doświadczeniem, to obserwowane zjawiska jesteśmy w stanie ocenić i zaakceptować lub odrzucić. Natomiast przy braku wiedzy na dany temat kierujemy się sądami innych osób, które to mogą być krytyczne, a wręcz nastawione na odrzucenie bez zagłębiania się w materię sprawy. Takie sytuacje stają się dla nas nieakceptowalne, a zdrowy rozsądek nie ma tu nic do powiedzenia. Świat, nasz świat, zaczynamy postrzegać oczami innych, a płynące z tego skutki obarczają nas, a nie innych, tych, którzy podsunęli nam rozwiązanie. W realnym świecie, tym za progiem naszych drzwi, za szybą okna, pewne zdarzenia jesteśmy w stanie zweryfikować i nadać wymierny efekt temu działaniu, np.: jeśli nie wiemy, jaka jest pogoda, to sprawdzamy ją patrząc przez okno lub wychodząc na zewnątrz pomieszczenia. Realność świata tak postrzeganego weryfikujemy codziennie poprzez nasze działania. Otaczamy się w swoim środowisku osobami, które znamy, a tych których nie znamy, nie zawsze darzymy niechęcią. „My" zawsze istnieje z „oni" i nabiera sensu tylko i wyłącznie razem, we wzajemnej korelacji. Ażeby moglibyśmy powiedzieć „my", potrzebni są też w naszym otoczeniu ludzie, którzy do „nas" nie należą - „oni". Z kolei „obcy" przeciwstawiają się przeciwstawieniu „my" – „oni". Aby kogoś uznać za „obcego", musimy o nim coś wiedzieć. Przede wszystkim, muszą się obcy pojawić kiedyś nie proszeni w polu naszego widzenia, co przejawia się ich obecnością w naszym otoczeniu. Obcy wkraczają w świat, w którym mieszkamy i żyjemy bez chęci wyniesienia się z niego. Gdyby nie to, byliby „nikim", nie zaś obcymi. Obcych natomiast dobrze widzimy i słyszymy, a ich działania niejednokrotnie nas drażni. Te określenia wprowadzają nas

w społeczny wymiar postrzegania świata. Oddzielają, wyróżniają i systematyzują „my", „oni" i „obcy".
Inny świat jest kreowany w cyberprzestrzeni, świat, do którego możemy wejść bez wychodzenia z domu. Nie potrzebujemy ani paszportu, ani wizy, a możemy być daleko od naszego miejsca zamieszkania, życia, pracy, daleko od naszej rzeczywistości. Media, przede wszystkim te elektroniczne z dostępem do internetu, dają nieograniczony dostęp do wielu informacji, do świata znajdującego w cyberprzestrzeni. Weryfikujemy go za pomocą naszych zmysłów, naszej wiedzy i doświadczenia. Informacje poparte obrazem wyróżniają się w naszym odbiorze. Wizualizujemy nasze pragnienia, „lepszy świat" i naszą w nim obecność. I tu rodzi się pytanie, jakie informacje my otrzymujemy za pomocą mediów? Czy telewizja, internet, gazety elektroniczne przedstawiają obiektywną rzeczywistość? Odbiorca niejednokrotnie otrzymuje informacje, które nie są zgodne ze stanem faktycznym. Otrzymany przekaz odbiega w swej treści od tego czego poszukiwaliśmy w cyberprzestrzeni. Rozbieżności te dotyczą nie tylko treści, ale również sposobu, w jaki ten przekaz został przygotowany i nam przedstawiony. W przypadku, kiedy jesteśmy nie usatysfakcjonowani, dokonujemy kolejnego wyszukania interesującej nas informacji. Proces ten może się powtarzać aż do chwili, gdy z mniejszą lub większą trafnością uzyskamy odpowiedź na nurtujący nas temat. I tu możemy wskazać na migrantów, którzy „wyruszając", poszukują swojej drogi do „lepszego świata". Korzystając z mediów elektronicznych otrzymują „sugerowaną" przez nie informację o dogodnych trasach podróży, warunkach i zasadach, które należy spełnić, aby przekroczyć poszczególne granice, itp. Takie postępowanie naraża tych ludzi na stawanie się „zakładnikami" wizji lepszego jutra lub też, co najgorsze, ofiarami w przypadku nielegalnej migracji. Stosowanie w mediach niepełnych informacji lub informacji wyselekcjonowanych, takich które są namiastką „lepszego jutra" prowadzi do tworzenia zniekształconego obrazu świata i rzeczywistości w głowach ludzi szukających swojego miejsca w rzeczywistym świecie. Jest to działanie wielowymiarowe. Obce kraje są spostrzegane jako miejsce oferujące dom, pracę, dogodne warunki socjalne, bezpieczeństwo ekonomiczne i społeczne. Odbiorca takich informacji korzystając z wizji kreślonej przez świat wirtualny, dowiaduje się o życiu, tak naprawdę elit danego kraju. Brak jest w tym

przekazie informacji o życiu codziennym mieszkańców i o ich problemach (Michalczyk, 2015, s. 61-62). Przekaz o życiu codziennym jest mało atrakcyjny dla nadawców i nie przynosi wymiernego efektu ekonomicznego. Media muszą z czegoś żyć, ten slogan powoduje, że w ramach szukania korzyści ekonomicznych zamieszczane są informacje, które zostały zlecone przez wpływowe kręgi. W przypadku obszarów objętych konfliktami, czy też krajów, gdzie panuje dyktatura, media przedstawiają tylko i wyłącznie informacje podporządkowujące społeczeństwo regułom ustanowionym przez władze. Każda informacja o możliwości wyrwania z takich warunków jest przyjmowana i niejednokrotnie w ogóle nie jest weryfikowana. Na terenach Iraku i Syrii, a kontrolowanych przez Państwo Islamskie, przekazywanie informacji oraz propagandy organizacji terrorystycznych nigdy wcześniej nie było tak łatwe i tak tanie. Obecnie organizacje terrorystyczne skupione wokół Państwa Islamskiego mają piony medialne odpowiedzialne za komunikację z otoczeniem zewnętrznym oraz serwisy propagandowe. W cyberprzestrzeni umieszcza się manifesty, informacje o sojuszach, pokazuje „bestialskie" egzekucje zakładników oraz wyroki wykonywane na zdrajcach. Osiągnięcia technologiczne dają łatwiejsze możliwości utrwalania takich informacji, internet daje nieograniczoną przestrzeń, a media komercyjne chętnie je cytują. Przekazy, a wśród nich filmy z pola walki i obozu szkoleniowego, wypowiedzi przywódców, zdjęcia bojowników, materiały światopoglądowe i instruktażowe stały się już elementem nie tylko walki terrorystycznej, ale częściej akcjami propagandowymi zamieszczanymi w cyberprzestrzeni (Wojtasik, 2016, s. 86-87). Takie informacje umieszczone w cyberprzestrzeni nigdy nie giną. Mogą być usunięte z jednego lub kilku portali internetowych, ale sieć ma to do siebie, że informacja pozostaje w innych miejscach. Dostęp do takich informacji oraz ich treść sprzyjają temu, że ludzie chcący zmiany swojego życia, decydują się na szukanie „lepszego" w cyberprzestrzeni. I oto w taki sposób rozpoczyna się proces migracji, od wirtualnej informacji, poprzez decyzję, kończąc na wędrówce poprzez świat rzeczywisty. Zagrożenia te, które niesie ze sobą migracja, a które zostały opisane powyżej, istniejące w świecie realnym, przenoszą się do świata wirtualnego i na odwrót. To szukanie lepszego świata, innego miejsca na ziemi, czy też schronienia przed konfliktami i prześladowaniami, ludzie opierają o uzyskane wirtualne informacje,

a weryfikowane są przez rzeczywistą „tułaczkę". Nie wszyscy, którzy podejmują się migracji, uczestniczą w kryminalnych procederach, ale wszyscy ci, którzy w migracji widzą możliwości na nielegalny biznes, uczestniczą w działalności przestępczej.

Podsumowanie

Tak jak sentencja Tytusa Liwiusza „*Hannibal ante portas*!" (łac. *Hannibal u bram*) odnosiła się w Starożytności do obawy Rzymian przed wojskami Kartaginy, że wkroczą do miasta, tak w dzisiejszych czasach możemy stwierdzić „*Aliena ante ianuam*" (łac. *Obcy u drzwi*). Migracja niezależnie od jej powodów powoduje przemieszczanie się nie setek, tysięcy ale milionów ludzi na całym świecie. To właśnie ci ludzie szukając „lepszego" życia niejednokrotnie stają u „naszych" drzwi i oczekują pomocy lub tylko zgody na pozostanie w „naszym" świecie. Dla tych ludzi, ten „nasz" świat, jest ich wymarzonym, lepszym światem, dającym szansę na inne, bezpieczniejsze w sensie i społecznym, i ekonomicznym życie. „Obcy", bo tak ich nazywamy, znaleźli się w „naszym" świecie, bo gdzieś w przekazie medialnym będącym w cyberprzestrzeni znaleźli drogę, którą do nas przybyli. W tym aspekcie „obcy" należę do świata *offline*, natomiast świat *online* należy do „mnie". Przewaga, jaką opcja *online* ma nad egzystencją *offline*, polega na tym, że obiecuje ona rychłe wyzwolenie od niewygód, trudności i niedoli, trapiących mieszkańca rzeczywistego świata. Tworzy wizję wolności od trosk, wynikającej nie tyle z rozwiania kłopotów i niepewności, które w świecie *offline* są męczące, ale niemożliwe do rozwiązania, ile z zawieszenia ich, zamiecenia pod dywan, ukrycia poza zasięgiem wzroku, a przede wszystkim z uczynienia ich nieistotnymi dla realizacji zadania, do którego zamierzamy dążyć. To właśnie iluzja niejednokrotnie przyprowadza do naszych drzwi „obcych", tych których nie znamy, ale mimo to możemy do nich mieć uprzedzenia.

Postawione w tytule opracowania pytanie „Proces migracji - realne czy wirtualne zagrożenie?" nie ma jednoznacznej odpowiedzi. Tak, jak jeszcze kilkanaście lat temu obawialiśmy się internetu, jego zaistnienia w „naszym" życiu, tak teraz obawiamy się migracji i zagrożeń z niej płynących. Obecnie internet, a można powiedzieć cyberprzestrzeń, stała się elementem naszego życia codziennego. Nie rozważamy, czy internet jest dobry, czy zły, czy jest zagrożeniem, czy też

szansą, ale możemy stwierdzić, że stał się on częścią naszego życia. Dziś tylko nieliczni mogą obejść się bez korzystania z internetu, a niewyobrażalnym stałby się zakaz jego użytkowania. Podobnie powinniśmy podejść do zagadnienia migracji. Migracja była, jest i będzie. Stała się ona rzeczywistością XXI wieku i jako fakt społeczny podkreśla nierówności i podziały w świecie. To my w „naszym" życiu musimy się nauczyć żyć obok „obcych". Obecne uwarunkowania polityczne i płynące z nich regulacje prawne wskazują na kontrolę i zarządzanie procesem migracyjnym, kontrolę i zamykanie granic oraz regulację napływu migrantów. Zanim zaakceptujemy proces migracji jako zjawisko naturalne, osadzone w rzeczywistości, musimy przeprowadzić analizę korzyści, ryzyka, możliwości zagrożeń oraz poczucia bezpieczeństwa obywateli. Akceptacja ta odnosi się do rzeczywistości i do cyberprzestrzeni. Jest to wielkie wyzwanie społeczne i wymaga znalezienia łącznika pomiędzy „my", „oni" i „obcy".

2.3. Szkolenie policjantów w aspekcie zastosowania kryminalistyki cyfrowej w dochodzeniu cyberprzestępstw

Wprowadzenie

Jednym z kierunków działalności Narodowej Policji Ukrainy (dalej - NPU) jest walka z cyberprzestępczością. W roku 2015 w strukturach NPU powstała nowa międzyregionalna formacja – Departament Cyberpolicji. Głównym jej zadaniem jest prowadzenie działań operacyjno-poszukiwawczych mających na celu zapewnienie realizacji polityki państwa w zakresie zwalczania cyberprzestępczości, wdrażania informacji oraz wsparcia analitycznego dla kierownictwa NPU i władz publicznych w sprawach należących do ich kompetencji [Rozporządzenie NPU 2015]. Jednostki Departamentu Cyberpolicji uczestniczą i wspierają inne jednostki policji w zakresie zapobiegania przestępstwom i ich zwalczania, wykrywania mechanizmów ich przygotowania, dokonywania lub ukrywania tychże przestępstw z wykorzystaniem komputerów, technologii zaawansowanych, systemów i sieci komputerowych oraz narzędzi telekomunikacyjnych.

Tak wiec, biorąc pod uwagę kierunki i zadania Cyberpolicji, pod pojęciem cyberprzestępstw rozumiemy działalność, w której komputery lub sieci komputerowe są sposobem, celem lub miejscem (środowiskiem) działań przestępczych.

Dochodzenie cyberprzestępstw nie jest możliwe bez użycia narzędzi kryminalistycznych, technik i metod pozyskiwania, oceny, badania oraz wykorzystania cyfrowych śladów i dowodów, źródłem których są urządzenia cyfrowe: komputery, urządzenia peryferyjne, sieci komputerowe, telefony komórkowe, kamery cyfrowe i inne urządzenia przenośne, w tym urządzenia dla magazynowania informacji oraz sieci internetowe. Informacja z tych źródeł nie posiada odrębnej swojej fizycznej formy.

Technologie informatyczne i urządzenia cyfrowe szybko się zmieniają i stają się bardziej zaawansowane, co właśnie wymaga ciągłego szkolenia ekspertów policji i rozwoju sposobów, technik i metod pozyskiwania, oceny, badania oraz wykorzystania cyfrowych dowodów w dochodzeniu cyberprzestępczości.

Zagadnienia kryminalistyki cyfrowej

Cyfrowe badania kryminalistyczne są szeroko stosowane w prowadzanych dochodzeniach i naukowo-praktycznych badaniach, które są wspierane działaniami różnych instytucji Unii Europejskiej i Stanów Zjednoczonych, takich jak:

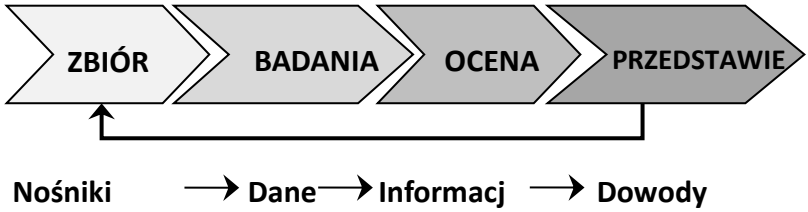
- Departament Sprawiedliwości Stanów Zjednoczonych (United States Department of Justice);
- Narodowy Instytut Standaryzacji i Technologii (The National Institute of Standards and Technology);
- SANS Instytut (Escal Institute of Advanced Technologies);
- Organizacja EC-Council (The International Council of Electronic Commerce Consultants, EC-Council);
- Stowarzyszenie do spraw audytu i kontroli systemów informatycznych (Information System Audit and Control Association, ISACA);
- Stowarzyszenie Szefów Policji (The Association of Chief Police Officers, ACPO) Wielka Brytania;
- Europol (European Cybercrime Centre, EC3);
- Stowarzyszenie Przeciwstawiania Cyberprzestępczości (Octopus Cybercrime Community).

Analiza dostępnych zaleceń i wytycznych odnośnie cyfrowych narzędzi na podstawie badań kryminalistycznych wykazały, że w tej dziedzinie istnieje obszerna baza wiedzy, która wymaga ciągłego przetwarzania, systematyzacji i wykorzystania praktycznego w celu zwalczania cyberprzestępczości.

Podstawowym zadaniem kryminalistyki cyfrowej podczas prowadzenia dochodzeń w zakresie przestępstw jest uzyskanie cyfrowych dowodów w postaci uogólnionego procesu sprzężenia zwrotnego. Proces wykorzystania cyfrowych dowodów przestępstw został przedstawiony na poniższym rysunku. Pod zbiorem dowodów cyfrowych na miejscu zdarzenia ujawniają nośniki cyfrowych danych, które ujawniają lub zabierają razem z nośnikiem zabezpieczając ich zachowania. Pod czas badania otrzymanej informacji sprawdza się otrzymana informacja, która jest treścią dowodów cyfrowych. Ocena informacji, która była uzyskana pod czas badania otrzymanej informacji, ustala się względność i dostępność dowodów, fakt istnienia i charakter więzi miedzy nimi, określają się sposoby wykorzystania dowodów cyfrowych w celu ustalenia prawdy. Następnie

ocenione dowody przedstawiają się w celu wykorzystania w postępowaniu dowodowym.

Rysunek 22. Proces wykorzystania cyfrowych dowodów przestępstw



Źródło: Opracowano na podstawie:*National Institute of Standards and Technology Special Publication 800-86. Guide to Integrating Forensic Techniques into Incident Response. August 2006. doi:10.6028/NIST.SP.800-86.*

Na każdym etapie uzyskiwania cyfrowych dowodów dla różnych okoliczności dochodzenia stosują się pełne narzędzia, techniki i metody. Kryminalistyka cyfrowa próbuje znaleźć odpowiedzi na te istotne pytania, które pomagają w zwalczaniu cyberprzestępczości:

- definicja i charakter cyfrowych dowodów;
- dopuszczalność i zasady pracy z cyfrowymi dowodami;
- źródła cyfrowych dowodów;
- odrębne cechy wyszukiwania i pozyskanie cyfrowych dowodów przy fizycznym i zdalnym ich dostępie;
- metody wyszukiwania cyfrowych śladów w sieci internet;
- metody badania i oceny cyfrowych dowodów;
- procedury przygotowania i nadania cyfrowych dowodów.

Szkolenie z zakresu kryminalistyki cyfrowej

Narodowy Uniwersytet Spraw Wewnętrznych w Charkowie – wyższa uczelnia w systemie Ministerstwa Spraw Wewnętrznych Ukrainy, szkoli fachowców ze specjalności „Cyberbezpieczeństwo" i „Prawo". Uniwersytet w ramach projektu „Cyberbezpieczeństwo i przeciwdziałanie cyberprzestępczości" (koordynator projektów OSCE na Ukrainie) był zaangażowany

do przeprowadzania dwutygodniowych oraz czteromiesięcznych szkoleń, których celem było podwyższenie kwalifikacji inspektorów i agentów specjalnych Departamentu Cyberpolicji.

Biorąc pod uwagę kierunki i zadania Cyberpolicji zostały opracowane plany szkoleń policjantów. Ustalając zakres szkoleń wzięto pod uwagę następujące podstawy:

- program szkoleniowy Centrum Dochodzenia Cyberbezpieczeństwa i Cyberprzestępczości Uniwersytetu w Dublinie (UCD (University College Dublin) Centre for Cybersecurity & Cybercrime Investigation)[88];
- program szkoleniowy Europejskiej Grupy Nauczania i Oświaty w Przestrzeni Cyberprzestępczości (European Cybercrime Training and Education Group, E.C.T.E.G)[89];
- Strategia Rady Europejskiej „Szkolenie Funkcjonariuszy Organów Ścigania" z roku 2014;
- wewnętrzne programy szkoleniowe.

W rezultacie podjętych działań powstały plany szkoleniowe: uniwersalny program szkoleniowy oraz program specjalistyczny dla funkcjonariuszy policji. Zapobieganie i przeciwdziałanie przestępczości jest związane ze zbieraniem, badaniem, oceną i wykorzystaniem dowodów przestępczej działalności, dlatego do programu specjalistycznego weszły zagadnienia z „Cyberbezpieczeństwa" oraz „Kryminalistyki cyfrowej".

Program szkoleniowy z „Cyberbezpieczeństwa" ukierunkowany jest na ujawnianie technologii popełnienia czynów przestępczych w cyberprzestrzeni, z kolei program szkoleniowy „Kryminalistyka cyfrowa" koncentruje się na technologii zbierania (ujawnienia) cyfrowych śladów przestępczego zachowania, które mogą stać się źródłem dowodów w sprawie, tj. dowodów cyfrowych. Tworząc program szkoleniowy „Kryminalistyka cyfrowa" wzięto pod uwagę, że zbiór dowodów (w tym cyfrowych) w ogólnym przypadku składa się z:

- ujawnienie śladów cyfrowych;
- zabezpieczenie śladów cyfrowych;

[88] http://www.ucd.ie/cci/education/prospective_students/fcci_programmes.html.
[89] http://www.ecteg.eu/courses.html.

- oceny śladów cyfrowych – działanie, które pozwala na ich wykorzystanie, dołączenia do akt i badania;
- utrwalania śladów cyfrowych.

Część teoretyczna programu szkoleniowego z „Cyberbezpieczeństwa" jest oparta na programie szkoleniowym Certified Ethical Hacker od EC-Council, a zadania praktyczne są realizowane w środowisku systemów operacyjnych: Kali Linux, Windows, CentOS. Celem programu szkoleniowego jest przekazanie wiedzy o różnych rodzajach atakach na systemy i sieci komputerowe, sposobach organizacji i ich ochrona. W trakcie szkolenia, m-kursanci nabywają wiedzy z następujących obszarów:

- podstawowa wiedza o cyberprzestrzeni;
- instalacja, konfiguracja i korzystanie z systemu operacyjnego Kali Linux;
- pasywny zbiór informacji z dostępnych serwisów internetowych, budowa i analiza relacji między częściami otrzymanej informacji. Znajomość narzędzi: HTTrack, Netcraft, Archive.org, google-dorks, theharvester, metagoofil, whois, host, dig, traceroute, Maltego, CUPP;
- aktywny zbiór informacji w sieci internet. Znajomość narzędzi: ping, arping, fping, hping3, p0f, nmap, telnet, amap, nbtscan, jxplorer, ldapse-arch, smtp-user-enum, dnsenum, dnsrecon, fierce, dig, openvas;
- wykorzystanie mechanizmów ochrony sieci od zbierania informacji, skanowania i penetracji. Znajomość narzędzi: snort, iptables, honeypot kippo;
- wykorzystanie serwisów kryptograficznych. Znajomość narzędzi: openssl, hashcat, oclHashcat;
- analiza ruchu w sieci komputerowej. Znajomość narzędzi: wireshark, tcpdump, macof, arpspoof, yersinia, msf auxiliary (dhcp);
- przechwyt sesji danych i przekazywanie informacji w sieciach komputerowych. Znajomość narzędzi: Ettercap, urlsnarf, mitmf, xplico, hamster, ferret;
- ocena bezpieczeństwa sieci bezprzewodowej. Znajomość narzędzi: kismet, Aircrack-ng Suite, Pyrit, hashcat;
- wrażliwość systemów operacyjnych. Znajomość narzędzi: metasploit framework, john the ripper, hashcat;

2.3. Szkolenie policjantów w aspekcie zastosowania kryminalistyki cyfrowej w dochodzeniu cyberprzestępstw

- technologia tworzenia złośliwego oprogramowania. Znajomość narzędzi: msfvenom, msfconsole, CodeBlocks, ProcessExplorer;
- analiza przepełnienia bufora. Korzystanie z narzędzi: CodeBlocks, ollydbg;
- ocena bezpieczeństwa serwerów www i aplikacji internetowych. Znajomość narzędzi: nikto, w3af, msfconsole;
- badania ataku „SQL injection". Znajomość narzędzi: dbeaver, sqlmap, DVWA;
- technologii inżynierii socjalnej. Znajomość narzędzia: setoolkit;
- kompleksowe badania na wrażliwość do ataków.

Część teoretyczna szkolenia „Kryminalistyka cyfrowa" została oparta na podstawie poszczególnych modułów szkolenia Computer Hacking Forensic Investigator od EC-Council, a część praktyczna korzysta z zadań i zbioru danych referencyjnych dla kryminalistyki cyfrowej (Computer Forensic Reference Data Sets, CFReDS) od National Institute of Standards and Technology U.S. Department of Commerce.

Szkolenie „Kryminalistyka cyfrowa" określa:

- definicję cyfrowych śladów;
- badania kryminalistyczne SO Windows;
- definicję zbioru informacji i tworzenie kopii nośników informacji;
- cechy techniczne oględzin narzędzi komputerowych ujawnionych na miejscu zdarzenia;
- odzyskiwanie skasowanych plików i logicznych podziałów nośników informacji;
- kryminalistyczne badania sieci komputerowych, czasopism audytu i ruchu sieciowego;
- kryminalistyczne badania atak bezprzewodowych;
- kryminalistyczne badania atak na serwery WWW.

Podczas szkolenia praktycznego kursanci starają się nabyć umiejętności:

- wykorzystania zasobów programowych badania kryminalistycznego SO Windows w celu sformułowania odpowiedzi na określone pytania w kontekście dochodzenia przestępstw, w których ślady cyfrowe pozostają w SO Windows:

2.3. Szkolenie policjantów w aspekcie zastosowania kryminalistyki cyfrowej w dochodzeniu cyberprzestępstw

- The Sleuth Kit&Autopsy, EnCase Forensic Imager, X-Ways Forensics, Web Historian, Skype Logview, USBDeview, USB Forensic Tracker;
- wykorzystania zasobów programowych zbioru informacji i stworzenia kopii nośników informacji:
- tworzenie obrazów RAM: RamCapture, DumpIt, MEMORYZE, AccessData FTK Imager;
- analizy obrazów RAM: Volatility, Bulk Extractor, Redline 1.14, MemGator - Memory Analysis Tool, Belkasoft Evidence Center (demo);
- zbierania wolitywnych (Volatility) danych (Live Acquisition) SO Windows: LiveGator, Redline, Win-UFO, DART, OSForensics;
- sterylizacja nośników danych przed kopiowaniem nośników cyfrowych śladów: WinHex;
- tworzenia obrazów nośników danych: z SO Windows dd, WinHex, AccessData FTK Imager, z SO Kali Linux dc3dd, Dcfldd, Guymager;
- wykorzystania kryminalistycznych systemów operacyjnych: BitCurator, SIFT, C.A.IN.E., DEFT, Kali Linux;
- wyłączenia i analizy danych z urządzeń komórkowych z wykorzystaniem oprogramowania: Oxygen Forensics, NowSecure Forensics;
- wykorzystania zasobów programowych z przywróconych skasowanych danych: Recuva, Puran File Recovery, Disk Drill, Glary Undelete, Pandora Recovery, FreeUndelete, PhotoRec, X-Ways Forensics;
- wykorzystania analizatorów protokołów sieci komputerowych i odzyskania śladów ataków: Wireshark, NetworkMiner, NetWitness Investigator;
- wykorzystania zasobów programowych badania sieci WiFi: Kismet, Vistumbler, inSSIDer, Wi-Fi Scanner, WiGLE, Aircrack-ng Suite;
- wykorzystania zasobów programowych badania czasopism audytu i ataków na serwery WWW: WebLog Expert Lite, Apache Logs Viewer, AWStats, Paros proxy.

Dodatkowo kursanci przechodzą testy on-line i off-line z rozwiązywania kryminalistycznych zadań z poszukiwania śladów cyfrowych różnych ataków:

- Logs analysis - web attack[90];

[90] https://www.rootme.org/en/Challenges/Forensic/Logs-analysis-web-attack.

- Find the cat (https://www.rootme.org/en/Challenges/Forensic/Find-the-cat);
- Forensic Challenge 2010 - pcap attack trace[91];
- Forensic Challenge 2011 - Forensic Analysis of a Compromised Server[92];
- Forensic Challenge 2010 - browsers under attack[93];
- Unicode String Searching Russian Text[94];
- Deleted File Recovery[95].

Współdziałanie z jednostkami policji

W ramach współpracy z jednostkami policji i praktycznych szkoleń na Uniwersytecie działa Centrum Szkoleniowo - Treningowe do Walki z Cyberprzestępczością i Monitoringu Cyberprzestrzeni[96].

Kursanci pod nadzorem wykładowców Uniwersytetu wykonują odrębne polecenia Departamentu Cyberpolicji w zakresie monitoringu cyberprzestrzeni w celu ustalenia miejsca przebywania zaginionych dzieci. Obecnie NPU koncentruje swoją działalność na poszukiwaniu zaginionych dzieci zgodnie z rozporządzeniem (Powiadomienie NPU 2017).

W wyniku realizacji rozporządzenia została opracowana metoda poszukiwania śladów cyfrowych, które pozostawiają zaginione dzieci w cyberprzestrzeni.

Jedną z okoliczności zbiegłych dzieci jest świadome opuszczanie miejsca zamieszkania bez zgody i powiadomienia rodziców, przy jednoczesnym korzystaniu przez te dzieci z telefonów komórkowych i sieci społecznych w internecie.

Zwykle podstawowymi danymi identyfikacyjnymi zaginionego dziecka są: imię, nazwisko, imię ojca; wiek; miejsce zamieszkania (zameldowania); nr telefonu komórkowego; dane kontaktowe opiekunów; czas i miejsce, gdzie dziecko ostatnio było widziane; opis wyglądu i ubrania dziecka.

Pierwszym krokiem podczas działań poszukiwawczych jest ustalenie w cyberprzestrzeni wszelkich możliwych śladów cyfrowych zaginionego

[91] https://www.honeynet.org/node/504.
[92] https://www.honeynet.org/challenges/2011_7_compromised_server.
[93] https://www.honeynet.org/challenges/2010_2_browsers_under_attack.
[94] https://www.cfreds.nist.gov/utf-16-russ.html.
[95] https://www.cfreds.nist.gov/dfr-test-images.html.
[96] https://www.facebook.com/cybercopua/.

dziecka, które często rejestruje się na wielu serwerach i ma kilka kont pod różnymi imionami. W tym celu przeprowadza się przesłuchanie rodziców, przyjaciół i znajomych dziecka, na podstawie którego ustala się:

- numery innych telefonów komórkowych z których korzysta dziecko lub mogło wykorzystać w celu rejestracji w serwisach sieciowych;
- dane identyfikacyjne stron w sieciach społecznych i serwisach komunikacyjnych;
- wszystkie dostępne zdjęcia dziecka;
- nazwiska i imiona wszystkich osób z rodziny dziecka, które dziecko mogło wykorzystać podczas rejestracji na stronie internetowej lub stworzenie tajnego pytanie aby odzyskania dostęp do serwisu w przypadku zgubienia hasła.

Na podstawie uzyskanych numerów komórkowych, imion (nazwisk) rodzeństwa, zdjęć, przez serwis odzyskanych haseł lub wyszukiwanie wizerunku, ustala się wszystkie możliwe strony portalów społecznych, które odwiedzało dziecko. W niektórych przypadkach w miejscu zamieszkania dziecka, rodziców lub przyjaciół pozostają narzędzia, z których dziecko korzystało wchodząc do sieci internetowej (nie zamknęło sesji, pozostawiło hasło dostępu do konta lub dostępna jest historia korzystania z sieci). Kryminalistyczne badania śladów cyfrowych daje dużo informacji, które umożliwiają kontynuowanie poszukiwań dziecka.

Drugim krokiem, analizując treść odzyskanych stron internetowych, jest weryfikacja tych stron należących do dziecka, gdzie zgromadzone są dodatkowe informacje o:

- innych dotąd nie znanych identyfikatorach dziecka;
- hobby i zainteresowaniach, członkostwie w grupach, tematach wpisanych przez dziecko wiadomości, grach sieciowych;
- kręgu komunikacji;
- czasie i typie (z terminalu komórkowego) ostatniego wejścia;
- danych statystycznych przebywania w sieciach społecznych;
- wystawianie ocen (*like, dislike*) w internecie.

Trzecim krokiem, jeżeli została ustalona aktywność dziecka w sieci, które

są związane z zaginionym dzieckiem, mogą być przeprowadzane następujące działania:

- jeżeli posiadamy hasło dostępu do konta dziecka, ustalamy czas i ostatni adres IP narzędzi, z których dziecko korzystało odwiedzając sieć internet;
- ustala się kontakt z osobami bliskimi dziecku, z portali społecznościowych i dokonuje się próby namówienia określonych osób do współpracy w celu otrzymania informacji o innych wiarygodnych kontaktach dziecka, wiarygodnym miejscem przebywania dziecka lub przeprowadzenie przez osoby bliskie próby nawiązania kontaktu z dzieckiem i omówienie się na spotkanie w kontrolowanym miejscu;
- wychodząc z ujawnionych zainteresowań oraz kręgu przyjaciół, dokonuje się próby przez osobę bliską dziecku ustalenia pośredniego lub bezpośredniego kontaktu z tym dzieckiem lub zainteresować dziecko przejściem na kontrolowaną stronę internetową, dzięki której można będzie ustalić adres IP urządzenia, typ i wersje aplikacji programowej, systemu operacyjnego, typ narzędzia za pomocą którego dziecko weszło do sieci internet;
- w przypadku publikacji zdjęć dziecka na podstawie geolokalizacji adresu IP możemy ustalić przybliżone miejsce lokalizacji dziecka.

Po otrzymaniu adresu IP i typu urządzenia z których dziecko korzystało w sieci internet, ustala się dostawcę usług internetowych (ISP), który prowadzi określone adresy i może nadać informację o lokalizacji określonych urządzeń internetowych. Wiedza o typie i wersji oprogramowania urządzeń komunikatywnych pozwala dokonać wstępnej lokalizacji poszukiwanego dziecka.

Podczas poszukiwań zaginionych dzieci są wykorzystywane następujące serwisy internetowe:

- wirtualizacja przyjaciół strony internetowej «VKontakte» (yasiv.com/vk);
- analiza strony internetowej «VKontakte» (vk.city4me.com);
- określenie preferencji sieci społecznej «VKontakte» aplikując «Komu stawia like mój przyjaciel? Odnajdziemy wszystkie like :)»;
- analiza strony internetowej «Facebook» (stalkscan.com);

2.3. Szkolenie policjantów w aspekcie zastosowania kryminalistyki cyfrowej w dochodzeniu cyberprzestępstw

- określenie adresu IP używając szablon (iplogger.org);
- wyszukiwanie za obrazem (images.google.com, images.yandex.ru, www.tineye.com, findface.ru);
- wyszukiwanie osób za nazwiskiem w sieciach społecznych (people.yandex.ru);
- analiza geolokalizacji zdjęć (exifdata.com);
- uporządkowany zbiór (*framework*) zasobów w celu otrzymania i analizy informacji (osintframework.com).

Całość opisanych działań ma na celu możliwość przeszkolenia policjantów w zakresie stosowania kryminalistyki w dochodzeniu cyberprzestępstw oraz uzyskania takich cyfrowych dowodów, które pozwolą na odnalezienie zaginionego dziecka.

Podsumowanie

Opracowane przez koordynatora projektów OSCE na Ukrainie szkolenia podwyższające kwalifikacje specjalistów jednostki Departamentu Cyberpolicji uzyskały aprobatę oraz pozytywne opinie funkcjonariuszy, którzy otrzymali niezbędną profesjonalną wiedzę pomagającą w ich działalności zawodowej w zwalczaniu cyberprzestępczości. Uzyskane efekty szkoleń pozwalają na wyjście z propozycją współpracy międzynarodowej w strefie walki z cyberprzestępczością. Posiadana wiedza, zgromadzone materiały naukowo-metodyczne i odpowiednie doświadczenie w prowadzeniu specjalistycznych szkoleń upoważniają do podjęcia działań w celu rozwoju, doskonalenia oraz wykorzystania we wspólnych inicjatywach szkoleniowych funkcjonariuszy policji różnych państw. Systematyzowanie narzędzi, metod i technik kryminalistyki cyfrowej oraz ich dalsze doskonalenie może jakościowo zmienić skuteczność prowadzonych dochodzeń w zakresie cyberprzestępczości lub ujawniania innych wykroczeń lub przestępstw.

2.4. Propaganda i świadomość w procesie radykalizacji - wzmacnianie i osłabianie czynników ryzyka w cyberprzestrzeni

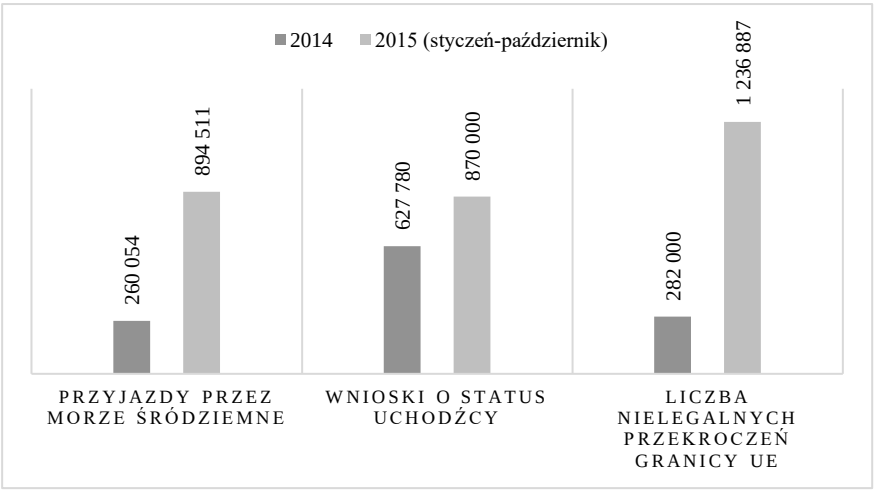
Wprowadzenie

Migracje w Europie nie należą do zjawisk nowych, a od wielu lat każdego roku na jej teren napływają imigranci z różnych kierunków świata. Wędrówki te uważa się nawet za najistotniejszy przejaw przestrzennej mobilności ludności, która wiąże się z trwałą zmianą miejsca zamieszkania lub też jedynie sezonowym lub czasowym przemieszczeniem polegającym na przekroczeniu granicy administracyjnej danej jednostki terytorialnej. W Europie, wciąż pozostającej otwartą na napływ cudzoziemców, już od 2012 roku obserwowane jest jednak nasilanie się ruchów migracyjnych zapoczątkowane pierwszymi zmianami układu z Schengen. Wzmocnione znacznie w ostatnim czasie między innymi przez bliskość geograficzną w stosunku do obszarów niestabilnych, a nawet zdezintegrowanych politycznie. Czynniki takie jak wysoki poziom dobrobytu, wysokie standardy zabezpieczenia społecznego, łatwość dotarcia do Europy, a zarazem trudność w kontrolowaniu europejskich granic powodują bowiem, że Europa staje się celem dla mieszkańców wspomnianych obszarów.

Na taką tendencję wskazują bowiem dane dotyczące liczby migrantów aktualnie przybywających do krajów europejskich gromadzone w kilku źródłach. Jedno z nich stanowi Europejski Urząd Statystyczny (Eurostat) gromadzący dane dotyczące wniosków o status uchodźcy złożonych w krajach członkowskich Unii Europejskiej, a kolejne – urząd Wysokiego Komisarza Narodów Zjednoczonych ds. Uchodźców (UNHCR) gromadzący dane na temat ogólnej liczby osób przedostających się do Europy oraz złożonych wniosków o ochronę międzynarodową. Inne źródło danych stanowi również Europejska Agencja Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej (Frontex) zbierająca dane na temat liczby nielegalnych przekroczeń granicy zewnętrznej Unii Europejskiej. Dane gromadzone przez wspomniane podmioty, a opublikowane przez Ośrodek Badań nad Migracjami wskazują, że tylko od stycznia do końca października 2015 roku

do Europy przedostało się przez Morze Śródziemne aż 894 511 osób, co oznacza ponad czterokrotny wzrost w stosunku do całego 2014 roku (216 054). Podobną tendencję można zaobserwować na podstawie danych dotyczących liczby nielegalnych przekroczeń granic Unii Europejskiej. Liczba ta wzrosła ponad czterokrotnie – z poziomu 282 000 w 2014 roku do blisko 1 miliona 300 tysięcy (1 236 887) przypadków we wspomnianym okresie roku 2015. Z kolei wzrost liczby odnotowanych wniosków o azyl w krajach Unii Europejskiej był mniejszy, gdyż od stycznia do końca października 2015 roku wyniósł 870 000, a w roku 2014 – 627 780 (Ośrodek Badań Nad Migracjami 2015, s. 3-4).

Rysunek 23. Liczba migrantów i uchodźców przybywających do Europy

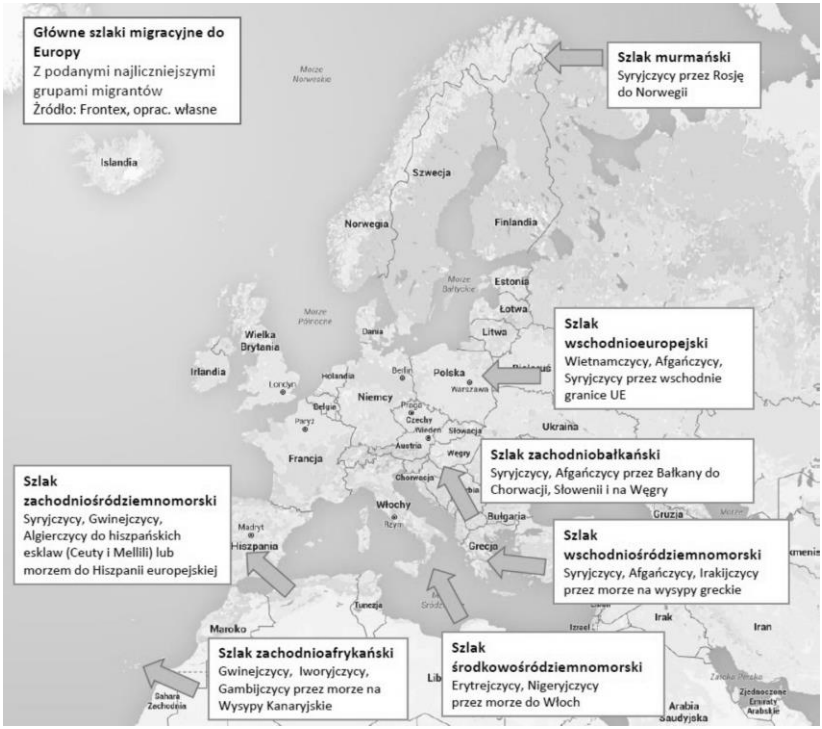


Źródło: Opracowanie własne na podstawie: Ośrodek Badań Nad Migracjami 2015. *Kryzys I co dalej?*, „Biuletyn Migracyjny", Nr 53/2015.

Aktualna sytuacja związana z migracjami, a szczególnie konieczność zapobiegania zagrożeniom bezpieczeństwa jakie z owymi ruchami mogą się wiązać, skłania również do przyjrzenia się kierunkom z jakich migranci najczęściej przybywają do Europy. Taka refleksja pozwala bowiem wnioskować o polityczno-społecznych przyczynach tych ruchów, o indywidulanych motywacjach skłaniających ludzi do migrowania, a zarazem przewidywać jakie

czynniki ryzyka mogą tym ruchom towarzyszyć. Opracowania udostępniane przez Ośrodek Badań Nad Migracjami wskazują zarówno na główne szlaki migracyjne do Europy, jak też na najliczniejsze grupy etniczne pośród migrantów (Ośrodek Badań Nad Migracjami 2015, s. 3).

Rysunek 24. Główne szlaki migracyjne do Europy



Źródło: Ośrodek Badań Nad Migracjami 2015. *Kryzys I co dalej?*, „Biuletyn Migracyjny", Nr 53/2015.

Zgodnie z nimi można zauważyć, że pośród najliczniejszych grup migracyjnych wyróżnia się Syryjczyków napływających do Europy szlakami wschodniośródziemnomorskim i zachodniośródziemnomorskim, zachodniobałkańskim, wschodnioeuropejskim oraz murmańskim oraz

Afgańczyków migrujący szlakami wschodniośródziemnomorskim, zachodniobałkańskim i wschodnioeuropejskim. Jednakże wśród osób napływających do krajów europejskich znajdują się także m.in. Erytrejczycy, Irakijczycy, Nigeryjczycy, Gwinejczycy, ale również Wietnamczycy. Co sprawia, że przemieszczenia ludności prowadzą do wzrostu różnorodności etnicznej i rasowej społeczeństw przyjmujących, a owa różnorodność kulturowa migrantów wpływa na kształtowanie się sytuacji społecznej w krajach imigracyjnych.

Migracje w świetle teorii zachowań zbiorowych

Literatura przedmiotu pozwala zaobserwować, że status kraju imigracyjnego ma swoje plusy i minusy. Dzięki migracjom zarobkowym państwa te mogą bowiem zyskiwać tzw. tanią siłę roboczą, a wskutek migracji religijnych czy turystycznych zyskiwać może ich branża turystyczna (Nowotnik, 2011, s. 61). Jednakże doświadczać mogą również konfliktów na tle religijnym i etnicznym czy też presji społecznej związanej z dostępnością do rynku pracy (Beets, Willenens, 2009, s. 19-37). Ponadto migracje międzynarodowe wpływać w tych krajach mogą na przyrost ludności, gdyż imigracja często powoduje obniżenie się wieku w społeczeństwie przyjmującym (Kałuża-Kopias, 2014, s. 37). Nie bez znaczenia dla sytuacji w krajach imigracyjnych jest jednak również wspomniana już różnorodność etniczna i rasowa, która nabiera szczególnego znaczenia w kontekście aktualnych zagrożeń bezpieczeństwa związanych z radykalizacją zachowań społecznych obserwowanych na gruncie europejskim. W miejscach tworzenia się dużych skupisk ludzkich towarzyszących masowym migracjom Europa doświadcza bowiem pewnych nowych, a co za tym idzie dotąd nie ustrukturyzowanych i nie zdefiniowanych sytuacji społecznych. Skupiska te wymagają z jednej strony zapewnienia właściwych warunków bytowych osobom migrujących, z drugiej natomiast – ze względu na zachodzące w nich procesy społeczne i psychologiczne towarzyszące zachowaniom zbiorowym – wymagają również zapewnienia szczególnych środków bezpieczeństwa. Miejsca te, dotąd nie zdefiniowane przez jednostki migrujące, mogą bowiem stwarzać pewne swoiste problemy związane z koniecznością funkcjonowania w zupełnie odmiennej rzeczywistości społecznej, a także sprzyjać radykalizacji.

2.4. Propaganda i świadomość w procesie radykalizacji - wzmacnianie i osłabianie czynników ryzyka w cyberprzestrzeni

Zgodnie bowiem z teorią zachowań zbiorowych w nowych, nieustrukturyzowanych i niezdefiniowanych sytuacjach społecznych, ludzie dążąc do rozwiązania napotkanych problemów uruchamiają swoistą komunikację „okrężną" służącą odpowiedzi na nieformalne sygnały i sugestie dotyczące natury ich aktualnej sytuacji. Przy czym o ile w małych grupach posługują się oni prostym i bezpośrednim mechanizmem, to w dużych grupach pierwszeństwo osiągają takie sposoby komunikowania się jak pozyskiwanie uwagi, manipulowanie niezadowoleniem, a nawet agitacja (Blumer, 1957, s. 89). Zachowania zbiorowe może również charakteryzować teoria zaraźliwości, zgodnie z którą w tłumie dochodzi do swoistego zanikania świadomości własnego „ja" i przekierowania własnych myśli, odczuć i działań w kierunku właściwym danej zbiorowości. Dusza zbiorowa, w której zacierają się indywidualności, różnorodność stapia się w jednorodność, a cechy nieświadome odgrywają decydującą rolę, każe bowiem jednostkom myśleć, czuć i działać inaczej niż każda z nich robiłaby to indywidualnie (Le Bon 1986, s. 51-53). Bo choć tłum charakteryzuje przestrzenne rozproszenie to jednocześnie towarzyszy mu swoista „bliskość duchowa" powstająca dzięki środkom wymiany opinii i informacji o aktualnej sytuacji poszczególnych jednostek (Szacki 2002, s. 328). Zgodnie bowiem z teorią wyłaniającej się normy sytuacja powstająca w niezwyczajnych okolicznościach może kierować zachowaniem jednostek poprzez dostarczanie znaczeń i interpretacji tej sytuacji (Turner, Killian, 1972, s. 67). W systemach zdestabilizowanych procesy wewnątrzsystemowe stają się w sposób szczególny podatne na wpływ subiektywizmu, jednostkowych decyzji i działań, ale również irracjonalności i kapryśności podmiotów działających czy też przypadkowych zdarzeń (Sztompka, 2011, s. 300-303). Dlatego w obliczu współczesnych masowych migracji nabierają znaczenia zarówno społeczne, jak i psychologiczne mechanizmy charakteryzujące zachowania zbiorowe mogące wywierać wpływ na jednostki migrujące, a zarazem narażać na oddziaływanie czynników ryzyka charakterystycznych dla procesu radykalizacji. Wspomniana destabilizacja, niezwyczajne okoliczności czy też nadawanie subiektywnych znaczeń nowej sytuacji przy jednoczesnym zanikaniu indywidualności, mogą być bowiem wykorzystywane we współczesnej Europie w celu wywierania wpływu

na te jednostki. Procesy charakterystyczne dla zachowań zbiorowych mogą bowiem wpływać na interalizowanie norm i wartości rozpowszechnianych przez jednostki agitujące, a w konsekwencji sprzyjać rekrutowaniu migrantów do grup radykalnych.

Ruchy migracyjne a radykalizacja

Choć „radykalizm" jako taki nie stanowi zagrożenia dla jednostek lub całych społeczeństw, to jego znaczenie zmieniło się dramatycznie w ciągu stulecia. Jeszcze w XIX wieku rozumiany był jako wierzenia czy też działania ludzi opowiadających za gruntowną reformę polityczną czy społeczną związaną z prodemokratycznymi i postępowymi stanowiskami politycznymi. Radykalizacja oznaczała zaś proces, w którym jednostki zyskują co prawda silne przekonania związane z przemianami politycznymi czy społecznymi, jednak wiele z nich nie odczuwa jednoczesnej potrzeby używania przemocy w celu ich manifestowania. Jednakże po atakach terrorystycznych następujących na całym świecie termin ten zaczął być interpretowany jako droga prowadząca do terroryzmu, do nielegalnej przemocy politycznej obejmującej antyliberalne, fundamentalistyczne, antydemokratyczne i agresywne postawy. Jeśli bowiem do osiągnięcia zmian w pewnych określonych systemach zaczyna być wykorzystywana przemoc to wówczas pojawia się pojęcie gwałtownego ekstremizmu (ang. *violent extemism*), do którego proces radykalizacji może prowadzić. I chociaż nie każdy radykalista jest terrorystą, a nie każdy terrorysta jest radykalistą to proces radykalizacji jest obecnie często postrzegany jako główna przyczyna aktów terrorystycznych (Sedgwick, 2010, s. 479-494). W oparciu o analizę aktualnej literatury przedmiotu można bowiem stwierdzić, że oznacza ona indywidualny lub kolektywny (grupowy) proces, w którym zazwyczaj dochodzi do polaryzacji politycznej, a tradycyjne praktyki dialogu, kompromisu i tolerancji między podmiotami a grupami o odmiennych poglądach i interesach są porzucane przez jedną lub obydwie strony konfliktu na rzecz zaostrzania konfrontacji. Konfrontacja ta może natomiast przyjmować postać niegwałtownego nacisku i przymusu czy różnych form przemocy politycznej innych niż terroryzm, jednakże może również przybrać postać aktów brutalnego ekstremizmu i terroryzmu (Schmid, 2013, s. 38-41).

2.4. Propaganda i świadomość w procesie radykalizacji - wzmacnianie i osłabianie czynników ryzyka w cyberprzestrzeni

Przy czym radykalizacja jest nielinearnym procesem, podczas którego jednostka może być poddawana wielu czynnikom mogącym zwiększać ryzyko wstąpienia na jej ścieżkę (Kordaczuk-Wąs, de Jongh, 2017, s. 10-25). Nie istnieje jeden wspólny powód dla którego ludzie ulegają radykalizacji, ani też jeden powód dla którego ów proces może pojawić się w danej społeczności (P. Neumann, 2015). Rezultaty badań wskazują na rozmaite przyczyny, dla których młodzi mieszkańcy współczesnej Europy manifestują radykalne zachowania. I tak dla przykładu Bakker i de Leede zdiagnozowali, że choć młodzi zradykalizowani Belgowie najczęściej pochodzą ze środowisk mocno zróżnicowanych pod względem warunków socjo-ekonomicznych, a także cechuje ich bardzo zróżnicowany poziom edukacji to łączy ich wszystkich poczucie niesprawiedliwości w społecznym traktowaniu ich samych lub też całych zbiorowości, do których należą (Bakker, de Leede, 2015, s. 45-47). Z kolei Bizina i Grey zauważyli, że młodzi ludzie o arabskich lub północnoafrykańskich muzułmańskich korzeniach żyjący w Europie Zachodniej bardzo często wskazują na otrzymywanie sygnałów o swej odmienności od społeczności lokalnych, w których zamieszkują, co sprawia, że występują u nich problemy z integrowaniem się z tymi społecznościami. Postrzegani są oni jako imigranci nawet wiele lat od momentu przybycia do kraju imigracji. W konsekwencji więc religijny ekstremizm, podobnie jak działalność przestępcza, jawi się tym młodym ludziom jako swoista możliwość manifestowania swej rzeczywistej odmienności (Bizina, Grey, 2014, s. 34). W literaturze przedmiotu wymienia się również wiele innych elementów (doświadczeń, sytuacji) najczęściej definiowanych jako czynniki ryzyka zagrożenia radykalizacją, które można pogrupować w pięć głównych kategorii (Treverton, 2011).

Wspomniana różnorodność przyczyn radykalizowania się jednostek społecznych pokazuje zatem, jak ważne – w kontekście zachowań zbiorowych towarzyszących ruchom migracyjnym – staje się zwrócenie uwagi na indywidualne społeczno-psychologiczne czynniki ryzyka. Szczególnie zaś te, które wiążą się z poczuciem wykluczenia, alienacji, dyskryminacji, frustracji, ograniczonej perspektywy przyszłości czy też z poczuciem beznadziejności, które w połączeniu z czynnikami związanymi z tożsamością kulturową mogą

powodować skłanianie się jednostek ku czynnikom związanym z ideologią wyznaniową.

Rysunek 25. Czynniki ryzyka zagrożenia radykalizacją

Źródło: Opracowanie własne na podstawie: Treverton G. F., 2011. *Comparing Early Warning Across Domains*, The Swedish National Defence College.

Głębokie poczucie niesprawiedliwości społecznej odgrywa bowiem często rolę mobilizującą ludzi znajdujących się w trudnej sytuacji do wkraczania w takie sieci czy otoczenia społeczne, które za sprawą ideologii mogą nakłaniać ich do podejmowania zachowań radykalnych wiodących do ekstremizmu czy nawet terroryzmu.

Propaganda islamistyczna w cyberprzestrzeni jako czynnik ryzyka

W kontekście rozważań zorientowanych na zapobieganie radykalizacji uwagi wymaga więc propaganda Państwa Islamskiego, a szczególnie ta, która

upowszechniana jest za pośrednictwem Internetu. Realizowana jest ona z ogromną precyzją, a zagrożenie ze strony używanych do tego celu mediów jest bezprecedensowe pod względem dostępności, skali i złożoności. Treści zamieszczane w zglobalizowanej Sieci zaspokajają bowiem i przyciągają ideologicznych zwolenników dżihadu na całym świecie (Winter 2015 (a), s. 29-30). Co sprawia, że mogą mieć one znaczenie również w procesie radykalizowania się jednostek migrujących po Europie. Powszechny dostęp do Internetu, w tym również młodych imigrantów, ułatwiać może bowiem proces internalizowania norm i wartości upowszechnianych przez ekstremistów, a w konsekwencji rekrutowania do różnych grup radykalnych.

Cyberprzestrzeń doświadczana jest bowiem każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach (Gibson, 2009, s. 43). Jej niewyobrażalna złożoność wynika z faktu, że jest to swoisty technosystem globalnej komunikacji społecznej odznaczający się interaktywnością i multimedialnością, który za sprawą integracji technosfery doprowadził do powstania globalnej zintegrowanej platformy teleinformatycznej (Sienkiewicz, 2009, s. 56). I choć cyberprzestrzeń stanowi obszar umożliwiający rozwój w różnych sferach życia społecznego to może być również wykorzystywana do upowszechniania ideologii wyznaniowej. Świat realny „przełożony" został bowiem na warunki sieci jaką jest Internet (Młyńska, 2004/2005, s. 53). Zaś przeniesienie rzeczywistości do cyberprzestrzeni dotyczy również Islamu. Od Malezji poprzez Arabię Saudyjską aż do Iranu, rządy państw muzułmańskich dążą bowiem do tego, aby ich państwowa religia była w cyberprzestrzeni dobrze reprezentowana (Lawrenc,e 2002, s. 244-246). Sieć stała się także niezwykle istotnym narzędziem rozpowszechniania oraz studiowania Koranu, a wiele sieciowych narzędzi używanych jest do cyfrowego poznawania świętej księgi (Bunt, 2004, s. 124-127). Jednocześnie Internet służy podkreślaniu różnic pomiędzy Islamem, a światem wobec niego zewnętrznym. Najjaskrawszy zaś przejaw owego „odróżniania się" stanowi obecność w Sieci islamskich fundamentalistów, których retoryka koncentruje się na wyrażaniu wrogich postaw i poglądów wobec odmiennych kultur i systemów społecznych (Weimann, 2006, s. 30-31). W konsekwencji Internet staje się również

doskonałym narzędziem szerzenia ideologii wyznaniowej, która ujmowana jest jako odrębna kategoria czynników ryzyka zagrożenia radykalizacją.
Za sprawą swej ponadnarodowości Sieć kieruje bowiem przesłanie do globalnej publiczności, a nie jedynie do populacji ściśle określonej przez terytorium czy narodowość. Jest zdecentralizowana, nie poddaje się cenzurze i kontroli, stąd jest doskonałym narzędziem gromadzenia informacji, a zarazem komunikowania się aktywistów i zwolenników grup ekstremistycznych. Pozwala ponadto rekrutować nowych członków i pozyskiwać fundusze na działalność terrorystyczną, ale przede wszystkim umożliwia szerzenie propagandy (Shavit, 2004, s.65-66). Wiele organizacji terrorystycznych stworzyło własne serwisy WWW zawierające informacje o historii, założycielach i liderach swych ugrupowań. Strony te zawierają zarówno informacje o politycznych, religijnych oraz ideologicznych celach organizacji, aktualne informacje o bieżących wydarzeniach, jak też swoiste sprawozdania z dotychczasowych działań i opisy planowanych akcji. Zawierają one również odezwy liderów adresowane do aktywistów i zwolenników, a także służą dystrybucji podręczników informujących o możliwościach wstąpienia w szeregi ugrupowań ekstremistycznych (Weimann, 2006, s. 30-31). Internet stał się bowiem narzędziem wojny propagandowej terrorystów islamskich nie tylko dostarczając informacji o przebiegu wojny i przeprowadzanych atakach terrorystycznych, ale przede wszystkim krzewiąc ideę „świętej wojny" (Szafrański, 2009, s. 78).
Odbiór propagandy Państwa Islamskiego spotyka się zaś ze znaczącym sukcesem za sprawą nieograniczania się propagandystów jedynie do wyrzucania treści do Internetu i biernego oczekiwania, że rezonują one we właściwych miejscach z odpowiednimi ludźmi. Opowiadają oni natomiast ściśle zdefiniowaną historię i budują konkretną markę. „Kalifat" – skupiając się na sześciu kluczowych narracjach, wśród których znajdują się: brutalność, miłosierdzie, przynależność, ofiarność, wojna oraz utopia – jawi się bowiem jako swoista alternatywa dla wszystkich sympatyków, niezależnie od ich politycznej, ekonomicznej czy ideologicznej motywacji (Winter, 2015 (b), s. 29-30). „Sprzedaje się" on jako wszechstronny ideał tysiąclecia, w którym projekt dżihadystyczny jest w pełni sprawny, w którym przestrzegane są islamskie wartości i obowiązuje sprawiedliwość społeczna (Ellul, 1973, s. 1-3). Mniej

wyraźne w propagandzie, choć nie mniej ważne, są również obietnice przynależności i miłosierdzia w obliczu skruchy. Zestawiane są one z obrazami brutalności, która używana będzie w odpowiedzi na zdradę lub szpiegostwo. Kluczową cechą propagandy Państwa Islamskiego jest więc manipulacja różnymi tematami zmieniającymi się zgodnie z jego aktualnymi priorytetami (Winter, 2015 (c), s. 67). Ponadto propagandyści kierują aktywność na zróżnicowane grupy odbiorców. Kieruje nimi bowiem zrozumienie, że różne argumenty odwołują się do różnych osób. Kładą w propagandzie silny nacisk zarówno na program „Kalifatu", jak też na świadczenie określonych usług i programy pomocy społecznej. Dzięki temu przyciągają zarówno fanatycznych dżihadystów, jak też jednostki niezadowolone czy zagubione w rzeczywistości społecznej (Winter, 2015 (d), s. 45). A globalna Sieć sprawia, że bez przeszkód mogą oni docierać również do uczestników współczesnych ruchów migracyjnych.

Kształtowanie świadomości społecznej w cyberprzestrzeni jako wzmacnianie czynników chroniących przed radykalizacją

Nieograniczoność Sieci oznacza jednak również ogromne możliwości dla skutecznego zapobiegania zagrożeniom bezpieczeństwa związanym z migracjami, w tym również zapobiegania radykalizacji migrujących jednostek. Kanał globalnej komunikacji jakim jest cyberprzestrzeń może być bowiem wykorzystywany w celu kształtowania świadomości uczestników zachowań zbiorowych towarzyszących migracjom. Obok szerzenia przez dżihadystów ideologii wyznaniowej, która może być znaczącym czynnikiem ryzyka wspierającym lub inicjującym proces radykalizacji, może on być bowiem doskonałym narzędziem zarówno w procesie zwalczania, jak też przekazu pożądanych treści i edukacji na rzecz zapobiegania temu zjawisku. Monitorowanie treści upowszechnianych w Sieci stanowi co prawda jedno z głównych działań podejmowanych przez podmioty odpowiedzialne za zapewnianie bezpieczeństwa na rzecz zwalczania aktywności grup ekstremistycznych, jednakże coraz częściej jej potencjał jest również wykorzystywany w upowszechnianiu treści profilaktycznych.

Przykład wykorzystania cyberprzestrzeni na rzecz upowszechniania anty-propagandowych treści stanowi między innymi kampania internetowa prowadzona przez rządowe północnoamerykańskie centrum zajmujące się przeciwdziałaniem terroryzmowi (ang. *Center of Strategic Counterterrorism Communication*). Przedsięwzięcie zainicjowane w 2015 roku w głównej mierze polegało na przekazywaniu swoim docelowym odbiorcom krótkich przekazów w języku arabskim zarejestrowanych podczas rozmów prowadzonych z uciekinierami z grup ekstremistycznych lub z uchodźcami (Winter, 2015 (b), s. 27-28). Podobne inicjatywy podejmowane są jednak również na gruncie europejskim. Na przykład działanie zainicjowane w Wielkiej Brytanii przez *Foreign and Commonwealth Office* w 2015 roku pozwoliło na utworzenie na Twitterze konta służącego informowaniu obywateli brytyjskich o działaniach brytyjskiego rządu podejmowanych wraz z partnerami Globalnej Koalicji na rzecz zwalczania brutalnych grup terrorystycznych (Perraudin, 2015, s. 12). Jednocześnie warto podkreślić, że o ile początkowo wspomniane przekazy skupiały się w głównej mierze na ukazywaniu ich odbiorcom brutalności zachowań podejmowanych przez ekstremistów i terrorystów, o tyle wraz z upływem czasu zaczęto skupiać się również na innych, bardziej skutecznych narracjach przekazów internetowych. Przykład stanowi amerykańska kampania informacyjna mającą na celu podniesienie świadomości społecznej w zakresie fałszowania przez członków grup ekstremistycznych założeń propagandowych tych ugrupowań. Ważny element przedsięwzięcia stanowiły krótkie filmy pt. „Dlaczego oni opuścili Daesh" będące relacją z wywiadów przeprowadzonych z byłymi członkami wspomnianych grup (Winter, 2015 (b), s. 28-29). Wśród działań podejmowanych na rzecz walki z propagandą poprzez wykorzystanie cyberprzestrzeni znajdują się również akcje korporacji zarządzających platformami internetowymi zorientowane na ograniczanie zasięgu przesłania dżihadystycznego upowszechnianego tymi kanałami. Zachęcają one społeczeństwo obywatelskie do działania, a także szkolą w zakresie sposobów zwiększania zasięgu kampanii anty-propagandowych. Na przykład platforma zatytułowana „Przeciw brutalnemu ekstremizmowi" (ang. *Against Violent Extremism*), która została uruchomiona przez Google Ideas w 2011 roku w celu „łączenia, wymiany, rozpowszechniania i wpływania

na wszystkie formy gwałtownego ekstremizmu". Jest to strona internetowa służąca wsparciem byłym ekstremistom, a także służąca radą wciąż aktywnym członkom grup ekstremistycznych w zakresie możliwości wycofywania się z przynależności do skrajnych ugrupowań. Poza tym także firmy działające w mediach społecznościowych angażują się w cenzurę treści o zabarwieniu radykalnym. Na przykład Facebook w ostatnich latach stał się stosunkowo nieprzyjaznym środowiskiem dla ekstremistów wypierając Państwo Islamskie z własnej platformy. Sympatycy ekstremizmu co prawda wciąż jej używają, lecz robią to w sposób znacznie ograniczony (Winter, 2015 (b), s. 30). Przyglądając się przytoczonym rozwiązaniom można jednak zauważyć, że opierają się one w głównej mierze na założeniach tzw. profilaktyki negatywnej. Poprzez ukazywanie negatywnych konsekwencji działania ugrupowań radykalnych koncentrują się bowiem głównie na eliminowaniu lub ograniczaniu czynników ryzyka związanych stricte z ideologią wyznaniową, muzułmańską polityką tożsamości, a także innymi czynnikami o zabarwieniu politycznym, które wiążą się stricte z działaniami grup ekstremistycznych.

Tymczasem skuteczne działania profilaktyczne muszą być zorientowane nie tylko na czynniki ryzyka, ale również – a może nawet przede wszystkim – na czynniki chroniące. Zgodnie bowiem z dwoma głównymi celami profilaktyki wymienia się dwa główne cele profilaktyczne polegające właśnie na: eliminacji lub redukcji czynników ryzyka i wzmacnianiu czynników chroniących (Modrzejewska, 2008, s. 214; Simm, Węgrzyn-Jonek, 2002, s. 24). Przy czym czynniki ryzyka to pewne – wspomniane już wcześniej w kontekście radykalizacji – cechy, sytuacje lub też warunki, które sprzyjają powstawaniu zachowań ryzykownych. Natomiast czynniki chroniące to te cechy, sytuacje lub warunki, które zmniejszają działanie (zwiększają odporność na) wymienionych czynników ryzyka (Szymańska, Zamecka, 2002, s. 19-33; Gaś, 1994). Współczesne skuteczne działania profilaktyczne mają bowiem wyposażać swych odbiorców nie tylko w rzetelną wiedzę, ale również w ważne umiejętności pozwalające na unikanie sytuacji ryzykownych.

Przykład takiej profilaktyki stanowi kampania zorganizowana przez Fundację Quilliam z Wielkiej Brytanii, która skupiła się na wspieraniu społeczeństwa w stawianiu czoła wyzwaniom związanym z zapobieganiem ekstremizmowi

i terroryzmowi. Jeden z istotnych elementów kampanii stanowiło bowiem wyprodukowanie i upowszechnienie w Internecie autorskiego filmu o narracji antyekstremistycznej pt. „#NotAnotherBrother". Natomiast drugi, istotniejszy element, stanowiły medialne warsztaty szkoleniowe dla młodzieży wyposażające w wiedzę i rozwijające umiejętności umożliwiające samodzielne przygotowanie przekazów medialnych związanych z zapobieganiem radykalizacji organizowane w szkołach i na uniwersytetach (Winter, 2015 (b), s. 30). Większe znaczenie drugiego z wymienionych elementów wynika z faktu, że skuteczne kampanie internetowe mające na celu zwiększanie świadomości społecznej w zakresie zapobiegania lub przynajmniej minimalizowania zakresu angażowania młodych ludzi w proces radykalizacji muszą służyć, oprócz informowania o negatywnych skutkach aktywności ekstremistycznej, również tzw. profilaktyce pozytywnej rozwijającej pewne określone umiejętności społeczne pozwalające na unikanie sytuacji ryzykowanych, a także wskazującej alternatywę dla tych zachowań. Co jest szczególnie istotne w warunkach będących wynikiem współczesnych ruchów migracyjnych. Wykorzystanie cyberprzestrzeni w celu wyposażania w taki rodzaj wiedzy i rozwijania takich umiejętności, które w nowych zdestabilizowanych warunkach pozwolą zagubionym jednostkom na właściwe funkcjonowanie pozwoli bowiem na właściwe definiowanie przez imigrantów nowej rzeczywistości społecznej oraz odzyskanie przez nich poczucia bezpieczeństwa. A dzięki upowszechnianiu rzetelnych treści związanych z różnicami etnicznymi i kulturowymi adresowanych do rdzennych mieszkańców krajów imigranckich mogą jednocześnie niwelować strach przed „przybyszami" i przygotowywać ich do bezpiecznej koegzystencji.

Podsumowanie

Wykorzystując zarówno potencjał towarzyszący nieograniczonej cyberprzestrzeni, jak też społeczne i psychologiczne mechanizmy charakterystyczne dla zachowań zbiorowych mogących towarzyszyć współczesnym migracjom, internetowe kampanie społeczne mogą zatem stanowić atrakcyjną, a zarazem skuteczną alternatywę dla ekstremistycznej propagandy. By osiągnąć poziom wysokiej skuteczności muszą jednakże skupiać

się zarówno na wspomnianych wcześniej realnych czynnikach ryzyka zagrożenia radykalizacją, jak również mocno akcentować czynniki wzmacniające, takie jak konkretne umiejętności społeczne ułatwiające funkcjonowanie jednostek w nowej zdestabilizowanej sytuacji społecznej. Treści tych oddziaływań muszą być zatem zależne od realnego problemu, jaki zostaje zdiagnozowany lub jakiemu chce się przeciwdziałać.

Masowe przemieszczenia ludności prowadzą bowiem do wzrostu różnorodności etnicznej i rasowej społeczeństw przyjmujących, a owa różnorodność powinna znajdować odzwierciedlenie zarówno w specyfice działań podejmowanych w celu adaptacji tych osób do nowej rzeczywistości społecznej, jak również w działaniach związanych z zapewnianiem szeroko rozumianego bezpieczeństwa. Rzeczywiste problemy wskazywać bowiem będą bezpośrednio na cele projektowanych oddziaływań profilaktycznych. Na przykład, jeśli w grupie imigrantów rozpoznaje się duże nasilenie czynników ryzyka w postaci wykluczenia, alienacji, frustracji czy poczucia beznadziejności, wówczas projektowane przekazy internetowe skupione muszą być właśnie na tych realnych problemach społeczno-psychologicznych, które mogą sprzyjać radykalizacji.

Konkretny, realnie zdefiniowany problem determinuje ponadto rodzaj przyjętej strategii profilaktycznej, którą można rozumieć jako sposób postępowania mający istotny wpływ na osiągnięcie założonych celów profilaktycznych (Kordaczuk-Wąs, 2017, s. 20-22). I tak w przypadku wykorzystania cyberprzestrzeni do działań adresowanych do środowisk imigranckich warto zwrócić uwagę na strategię edukacji normatywnej polegającej na wzmacnianiu i kształtowaniu określonych norm. W ramach tej strategii można bowiem zastępować niepożądane normy pożądanymi, a także korygować błędne lub stereotypowe wyobrażenia poprzez prezentowanie rzeczywistych warunków panujących w określonym otoczeniu (Krajowe Biuro Przeciwdziałania Narkomanii 2016). Dzięki temu w towarzyszących masowym migracjom dużych skupiskach ludzkich można w pewnym stopniu strukturalizować i definiować aktualne sytuacje, a w konsekwencji przeciwdziałać komunikowaniu się ich członków poprzez pozyskiwanie uwagi, manipulowanie niezadowoleniem, a nawet agitacją sprzyjającym kształtowaniu postaw i zachowań radykalnych.

2.4. Propaganda i świadomość w procesie radykalizacji - wzmacnianie i osłabianie czynników ryzyka w cyberprzestrzeni

W celu zapobiegania angażowaniu się jednostek w aktywność o zabarwieniu ekstremistycznym w medialnych przekazach profilaktycznych wykorzystywać należy również strategię informacyjną, której celem jest dostarczenie obiorcom informacji na temat skutków zachowań ryzykownych i umożliwianie dokonywania przez nich racjonalnego wyboru. Jednakże by możliwe było osiągnięcie takiego celu strategia informacyjna musi być uzupełniana przez strategię edukacyjną wspierającą rozwój istotnych umiejętności psychologicznych i społecznych, takich jak umiejętność nawiązywania kontaktów z innymi ludźmi, radzenia sobie ze stresem, rozwiązywania problemów, budowania pozytywnego wizerunku siebie czy też opierania się naciskom ze strony otoczenia (Szymańska, Zamecka, 2002, s. 19-33).

Dopiero bowiem skuteczne wykorzystanie cyberprzestrzeni do upowszechniania treści anty-propagandowych oraz edukowania zarówno jednostek migrujących, jak też rdzennych mieszkańców krajów imigranckich, będzie ogromną szansą dla podmiotów odpowiedzialnych we współczesnej Europie za zapewnianie bezpieczeństwa wewnętrznego. Poprzez osłabianie czynników ryzyka i wzmacnianie czynników chroniących pozwoli bowiem zarówno na normowanie relacji społecznych w systemach zdestabilizowanych, jak też na przeciwdziałanie mechanizmom mogącym w znaczący sposób wpływać na rozpoczęcie, a także na przebieg procesu radykalizowania się jednostek społecznych.

2.5. Patologia cyfrowego dzieciństwa

Perswazja w komunikacji społecznej

Perswazja i manipulacja jako sposoby nakłaniania i narzędzia wywierania wpływu stosowane są, odkąd istnieje gatunek ludzki i tworzy grupę. Komunikatywizm przez perswazję rozumie uświadomione przez obserwatora działanie werbalne nadawcy, dążące do zmiany postawy odbiorcy (Szymanek, 2005, s. 228-235). Za manipulację uznaje się natomiast ukryte działanie nadawcy na odbiorcę, w którym celem jest modyfikacja, utrwalenie lub osłabienie szczegółowej postawy odbiorcy w stosunku do obiektu konkretnego.

Perswazja i manipulacja są narzędziami wpływu w komunikacji społecznej, charakteryzującymi się mnogością pełnionych funkcji. Nie tylko bowiem odgrywają znaczącą rolę w interakcji oraz mogą stanowić istotny element rozwiązywania konfliktów poprzez negocjowanie wartości, ale także biorą udział w socjalizacji jednostek, uczestniczą w procesie kształtowania organizacji społeczeństwa, a nawet są związane z rozwojem ekonomicznym – poprzez aktywność w dyskursie politycznym czy reklamowym (Habrajska 2005, s. 19-20). Właściwości nakłaniające oraz mechanizmy perswazji i manipulacji wykorzystywane są zatem w komunikacji interpersonalnej, polityce, szkolnictwie, marketingu, reklamie, publicystyce i wszędzie tam, gdzie zachodzi potrzeba przekonywania. Jest to temat bardzo obszerny i głęboko penetrowany, a tutaj zostaną jedynie zasygnalizowane wybiórczo najważniejsze jego aspekty, które powinny być rozwinięte poprzez dalsze zgłębianie kolejnych źródeł wiedzy (Pleszkun-Olejniczak, Bachura, Worsowicz, 2010, s. 26).

Niewłaściwie użytkowany Internet może być doskonałym narzędziem manipulacyjnym. W obecnych czasach jest największym i najszybciej rozwijającym się medium na świecie. Wg danych Głównego Urzędu Statystycznego (GUS, 2016, s. 1), dostęp do internetu w 2016 r. posiadało 80,4% gospodarstw domowych oraz 93,7% przedsiębiorstw. Z usług e-administracji korzystało 30,2% osób w wieku 16-74 lat, a 67% przedsiębiorstw posiadało własne strony internetowe.

Z kolei o wyjątkowości internetu decyduje to, że cyberprzestrzeń daje możliwości, których nie oferuje żaden inny środek masowego przekazu: to ogromna encyklopedia zawierająca niemożliwe do całkowitego ogarnięcia pokłady informacji, które mogą zastąpić dziś radio, telewizję, telefon, prasę codzienną i książkę.

Cyberprzestrzeń jest także jedynym medium, dzięki któremu można w pełni śledzić zachowania internautów, poznawać ich zainteresowania, sposób odbioru rozmaitych form przekazu, taktykę oraz czas korzystania z sieci (Pleszkun-Olejniczak, Bachura, Worsowicz, 2010, s. 200).

Mówiąc o wpływie mediów, dotykamy nieuchronnie tego, co powszechnie rozumiemy pod pojęciem moralności. Kiedy mówimy na przykład o manipulacji, to pojmujemy ją jako próbę bądź efekt przełamywania barier stawianych przez kulturowe wzorce tego, co etyczne, tego, co nieuprawomocnione.

Pomijając czysto teoretyczne rozważania w odniesieniu do świata, który możemy postrzegać empirycznie, wpływ mediów zauważalny jest w interakcji między nadawcą i odbiorcą komunikatu. Nawet wtedy, gdy poruszalibyśmy zagadnienie automanipulacji, wcześniej czy później musimy spostrzec, iż podmiot uwikłany w tego rodzaju układ przyjmuje jednocześnie dwie zależne od siebie postawy. Niestety, podobnie jak w wielu innych obszarach życia społecznego, trudno byłoby oczekiwać wyraźnego rozdzielenia moralnego na to, co zgodne, a co sprzeczne z ogólnie przyjętą normą. W dobie szerokiej komunikacji międzykulturowej obszary prywatności, wolności obarczone są potrzebą identyfikacji przez kontekst unaocznień problemu. Nie ma bowiem w obrębie komunikacji czegoś takiego jak norma uniwersalna czy bezwzględne i jednolite w każdej kulturze rozumienie dobra jednostki. Możemy mówić o jakimś rodzaju negocjacji, dążeniu do utrzymania się w pewnej sferze norm lub o procesie wystawiania tych norm na próbę – przy jednoczesnym narażaniu się na ponoszenie konsekwencji ich naruszania (Dziadzia, 2007, s. 26-27).

Na wpływ mediów składają się środki językowe, dźwięk i obraz. Ponadto wyróżnić należy środki wpływu, a więc media posługujące się pełnym spektrum wymienionych środków komunikacji (jak telewizja czy internet), a także te, które wykorzystują tylko niektóre z nich (jak radio czy prasa). Zakres prób wpływu obejmuje wszelkie formy kształtowania postaw, unieważniających przy tym nadrzędność woli odbiorcy wobec interpretacji kierowanych do niego

komunikatów. Mówiąc o nadrzędności woli, odwołuję się do ogólnie przyjętego prawa człowieka do samostanowienia, czemu w ewidentny sposób mechanizmy wpływu, a szczególnie manipulacji, zdecydowanie przeczą, narzucając internalizację określonych norm i zachowań. Manipulacja w mediach przyjmuje niemal wyłącznie formę niejawną. Występuje pośród zwykłych, niebędących definiowanymi jako forma perswazyjna, komunikatów o charakterze rozrywkowym i informacyjnym. Tam, gdzie ów wpływ wynika z formuły komunikatu – mamy w istocie do czynienia z symulacją, sugestią informacyjnego i relaksującego produktu mediów, przez co ujawnienie perswazji wymaga wiedzy i kompetencji do jej unaocznienia (Dziadzia, 2007, s. 44).

Posługiwanie się kłamstwem i oszustwem, wykorzystywanie zaufania innych spotyka się z czasem z przyzwoleniem społecznym. W socjologii stan taki traktuje się często jako patologię więzi moralnej, zwaną „kulturą manipulacji". Rzecz w tym, iż bez posłużenia się sądami wartościującymi problemem manipulacji może być rozpatrywany jedynie w świetle teorii zależności i konfliktu. W niemal każdym innym przypadku będzie to przedstawienie modelu funkcjonowania określonej grupy społecznej (Dziadzia, 2007, s. 45).

Sprzeczność interesów, jaka dzieli nadawcę treści manipulujących i odbiorcę, wynika z tego, że pierwszy z nich chce mieć kontrolę nad drugim. Jeżeli nadawca występuje we własnym imieniu, wpływ staje się próbą sprawowania władzy. Zwierzchność ta jest wynikiem przyzwolenia bądź uzurpacji. Przez posługiwanie się dostępnymi technikami proces sprowadza się do mechanizmu sterowania postępowaniem ludzi. Ingeruje w przebieg i rodzaj emocji, wykorzystuje uprzedzenia i stereotypy, a także uwarunkowania fizjologiczne i psychiczne ludzi. Wpływ mediów to trzy odrębne i determinujące się zakresy problemy dotyczących nadawcy, przekazu i recepcji. Uwzględniając wielość intencji zawiązywania sytuacji komunikacyjnej, wpływ mediów należałoby rozumieć jako zawierające się w autonomicznych przekazach i zależne od kompetencji odbiorcy próby zmieniania postaw za sprawą form i treści masowych środków przekazu (Dziadzia, 2007, s. 45).

Czy media posiadają rodzaj uprawomocnienia pozwalającego stać ponad swoim odbiorcą? Mogło by się wydawać, że odpowiedź powinna być przecząca. I tak też jest, ale dopóki, dopóty woli publiczności nie przesłoni ignorancja. W tak przedstawionym kontekście otwarte i uzasadnione, ale też bez odpowiedzi

zostaje pytanie o uczciwość i odpowiedzialność jednostek dysponujących zdolnością wpływania, zarówno za stosowanie, jak i niestosowanie form perswazji (Berger, 1997, s. 70).

Edukacja cyfrowa w szkołach w zakresie cyberprzemocy w internecie i bezpieczeństwa psychologicznego oraz prawnego

Cyberprzemoc (inne pojęcia to cyberbullying lub agresja elektroniczna) to stosowanie przemocy poprzez prześladowanie, zastraszanie, nękanie, wyśmiewanie innych osób z wykorzystaniem internetu i narzędzi typu elektronicznego, takich jak: sms, e-mail, witryny internetowe, fora dyskusyjne i inne. Cyberprzemoc pojawiła się na przełomie XX i XXI wieku. Bardziej drastyczną formą ataku jest sporządzenie w tym celu witryn internetowych, wpisów na forach dyskusyjnych czy dręczenie przez komunikatory sieciowe takie jak: Gadu-Gadu, Tlen.pl (Kozak, 2014, s. 105).

Cyberprześladowanie jest szczególnie groźne dlatego, że kompromitujące czy poniżające materiały są dostępne w sieci krótkim czasie dla wielu osób i pozostają w sieci na zawsze, jako kopie na wielu komputerach, nawet po ustaleniu i ukaraniu sprawcy.

Pojęcie tożsamości oraz sposób, w jaki na nią oddziałują nowe technologie, są przedmiotem badań w takich dziedzinach jak psychologia i socjologia. Tworzenie się społeczności internetowej wynika z korzystania z sieci w celu wsparcia społecznego i stanowi przestrzeń, w której ludzie mają możliwość wyrażania i ujawnienia swojej tożsamości w kontekście społecznym. Na przykład określają wyraźnie swoją tożsamość, tworząc profile użytkowników czy serwisów społecznościowych. Prowadząc bloga i wyrażając własne opinie, ludzie określają swoje tożsamości w inny sposób. Tożsamości wyznaczone przez ludzi w społecznościach internetowych niekoniecznie są wiarygodne.

Dzieci zazwyczaj nie uświadamiają sobie, jak krzywdzące mogą być działania podejmowane online, a ofiary cyberprzemocy pozostawione sam na sam z problemem często nie potrafią sobie z nim poradzić. Dlatego bardzo ważną funkcję w przeciwdziałaniu w cyberprzemocy pełni najbliższe otoczenie dziecka. Rodzice i nauczyciele powinni podejmować działania profilaktyczne oraz szybko interweniować w sytuacji, gdy zachodzi podejrzenie, że dziecko jest ofiarą lub sprawcą przemocy w sieci. Problem cyberprzemocy coraz częściej jest

przedmiotem programów profilaktycznych i kampanii informacyjnych. W Polsce Fundacja Dzieci Niczyje realizuje od stycznia 2008 roku kompleksową akcję społeczną Stop Cyberprzemocy, w ramach której prezentowane są w mediach reklamy prasowe, telewizyjne i radiowe zwracające uwagę dorosłych na specyfikę i skalę problemu cyberprzemocy oraz rolę rodziców w zapewnieniu dziecku bezpieczeństwa w sieci (Kozak, 2014, s. 111).

Zapewnienie uczniom bezpieczeństwa w szkole jest ważnym elementem organizacji pracy każdej placówki oświatowej. Rolę szkoły, zadania dyrektora i nauczycieli w tym obszarze regulują przepisy prawa oświatowego, administracyjnego, cywilnego, karnego i pracy. Regulacje prawne w większości określają ogólne zasady zapewnienia bezpieczeństwa uczniów i odpowiedzialność prawną pracowników szkoły za ich przestrzeganie. Nie przedstawiają jednak systemu reagowania w konkretnych sytuacjach zagrożenia bezpieczeństwa uczniów czy szczegółowych procedur postępowania.

Zjawisko cyberprzemocy jest jednym z zagrożeń, o których warto pamiętać. Należy zdawać sobie sprawę z jego złożoności i możliwości wystąpienia. Pojawia się również potrzeba przygotowania i stosowania rozwiązań organizacyjnych w tym obszarze uwzględniających realia szkolne. Ujawnienie zjawiska cyberprzemocy wymaga podjęcia konkretnych działań interwencyjnych. Aby interwencja była skuteczna, warto zadbać o następujące sprawy:

- wprowadzić działania profilaktyczne w szkole, uświadamiające całej społeczności (uczniom, rodzicom, nauczycielom i innym pracownikom) zasady korzystania i zagrożenia płynące z użytkowania różnych technologii komunikacyjnych;
- opracować procedurę reagowania w szkole na zjawisko cyberprzemocy;
- podejmować interwencję w każdym przypadku ujawnienia lub podejrzenia cyberprzemocy (procedura nie będzie wówczas tylko martwym zapisem w dokumentach).

Rolą szkoły jest więc prowadzenie edukacji uczniów także w tym obszarze, co znajduje odzwierciedlenie w nowej podstawie programowej kształcenia ogólnego, która nakłada na szkoły obowiązek prowadzenia edukacji medialnej i profilaktyki zachowań ryzykownych w Internecie (Kozak, 2014, s. 112).

2.5. Patologia cyfrowego dzieciństwa

Jednym z ważnych zadań szkoły jest przygotowanie i stosowanie algorytmu interwencji w przypadku cyberprzemocy, uwzględniającego potrzeby i realia szkolne. Celem działań profilaktycznych szkoły jest ograniczenie lub wyeliminowanie zachowań agresywnych – przestępczych. „Niezależnie od tego, kto zgłasza przypadek cyberprzemocy, procedura interwencyjna powinna obejmować: udzielenie wsparcia ofierze przemocy; zabezpieczenie dowodów i ustalenie okoliczności zdarzenia; wyciągniecie konsekwencji wobec sprawcy przemocy oraz pracę nad zmianą postawy ucznia" (Wojtasik, 2013).

Dzieci korzystające z internetu narażone są na kontakt z materiałami, które mogą mieć szkodliwy wpływ na ich psychikę. Do niebezpiecznych treści zalicza się filmy, zdjęcia lub teksty o charakterze pornograficznym, prezentujące przemoc, promujące niezdrowe postawy i zachowania tj. hazard, używki, anoreksję, uczestnictwo w sektach itp. Część tych materiałów publikowana jest w sieci nielegalnie, inne – mimo wysokiej szkodliwości dla najmłodszych internautów – rozpowszechniane są zgodnie z prawem. Niebezpieczne treści występują w Internecie w ogromnej ilości. Materiały pornograficzne to najczęstsza kategoria treści publikowanych w tym medium, na które młodzi internauci trafiają coraz częściej, zazwyczaj przypadkowo!

Przyczyny stosowania cyberprzemocy są złożone. Ludzie w internecie mają skłonność do innych form zachowań niż w świecie realnym. Zjawisko „internetowego efektu odhamowania" opisuje zachowania części internautów, którzy przestają w sieci odczuwać zahamowania charakterystyczne dla kontaktów bezpośrednich. Odhamowanie może mieć wydźwięk pozytywny (gdy na przykład osoba nieśmiała dzięki możliwości wypowiedzenia się zyskuje pewność siebie) lub negatywny (gdy przejawia się ono w przemocy internetowej, większej łatwości obrażania innych ludzi i stosowania wobec nich różnych form agresji). Na to, czy dana osoba dopuści się agresji w Internecie, czy nie, w znacznym stopniu mają wpływ osobiste uwarunkowania i cechy, jednak sieć jest miejscem, w których stosunkowo łatwiej uaktywniają się ciemne strony osobowości. Czy młodzi sprawcy cyberprzemocy, zdają sobie sprawę z konsekwencji swoich czynów?

Sprawcy cyberprzemocy często nie zastanawiają się nad tym, co robią, nie potrafią lub nie chcą wyobrazić sobie, co czuje osoba prześladowana. Wiąże się to z niskim poczuciem empatii wśród współczesnej młodzieży. Jej relacje

są często bardzo skomplikowane – czasem nawet rówieśnicy promują zachowania antyspołeczne i agresywne, aby podkreślić swoją niezależność. Inne osoby biorą z nich przykład, mając na celu zaimponowanie i wyróżnienie się na tle grupy. Zdarza się też coraz częściej, że stosowanie cyberprzemocy staje się formą dobrej zabawy i spędzania wolnego czasu w grupie. Co za tym idzie, aby być tolerowanym, należy się podobnie zachowywać. Innym powodem stosowania tego typu agresji jest lęk przed staniem się ofiarą – przyjmuje się wtedy rolę sprawcy.

Młodzi ludzie często podejmują czynności określane mianem cyberprzemocy, nie mając świadomości konsekwencji swoich zachowań zarówno w wymiarze moralnym, jak i prawnym. Wpływa na to z jednej strony pozorna anonimowość internetu – łatwiej określonej anonimowo wyrazić kontrowersyjną opinię czy obrazić kogoś, niż narazić się na nieprzyjemności z tego wynikające w życiu realnym. Część internautów czuje się więc w sieci bezkarnie i uważa, że może wyrażać swoje opinie publicznie nawet wtedy, gdy ośmiesza i znieważa inne osoby (Kozak, 2014, s. 151-152).

Anonimowość nie jest jednak jedyną przyczyną agresji w cyberprzestrzeni. W internecie zazwyczaj nie widzimy postawy drugiej osoby, jej emocji – zdarza się, że odbieramy niewłaściwie zamiary i intencje innych ludzi, prowokując ostrą wymianę zdań lub kłótnie. Od tego krótka już droga do wzajemnych obelg. Ofiarą cyberprzemocy padają najczęściej osoby nieśmiałe, mające niską samoocenę lub wręcz przeciwnie – pewne siebie, wyróżniające się charakterem lub wyglądem. Często osoby te ukrywają ten fakt przed otoczeniem i próbują się od niego uwolnić samodzielnie, bez niczyjej pomocy. Cyberprzemoc wywołuje negatywne skutki w funkcjonowaniu każdego człowieka.

Przed cyberbullyingiem możemy się bronić jedynie, starając się maksymalnie chronić swoją prywatność poprzez nieujawnienie swoich danych osobowych w Internecie, stosowanie programów antywirusowych i zabezpieczeń.

Na agresję w sieci szczególnie narażone są dzieci, i to je należy szczególnie chronić. Podstawą w tym zakresie będzie bezpośrednia ciągła edukacja dotycząca istniejących w Internecie zagrożeń i uświadomienie konsekwencji stosowania przemocy w sieci. Trzeba interesować się tym, jakie strony dzieci przeglądają, uczulić je na ostrożność przy podawaniu informacji o sobie

i na zawieranie znajomości z osobami, które mogą próbować zrobić krzywdę, czasami również fizyczną.
Rolą rodziców i pedagogów, którzy mają większą świadomość narastającego problemu cyberprzemocy, jest także takie wychowanie i taka edukacja dzieci, aby te nie brały udziału w wirtualnym prześladowaniu innych. Trzeba uświadomić dzieciom, że takie działanie nie jest zabawą czy żartem i może prowadzić do bardzo nieprzyjemnych konsekwencji. Poza tym małoletni powinni wiedzieć, jakie są ich prawa i za co są odpowiedzialni. Powinni również szanować prawa innych osób.
Najmłodsi coraz częściej padają ofiarą cyberprzemocy, a ich rówieśnicy bywają bezwzględni w dręczeniu i wyśmiewaniu się za pomocą internetu. W każdym przypadku należy jednak reagować i przeciwstawiać się agresji (Pyżalski, 2009).

Patologiczne formy komunikowania się dzieci i młodzieży w cyberprzestrzeni

Powszechnie wiadomo, że internetoholizm to uzależnienie przejawiające się w silnej potrzebie, wręcz przymusie, spędzania czasu w Internecie, dążeniu do jak najczęstszego używania internetu i odczuwania dyskomfortu, nawet złości, kiedy nie można tego robić, a w wyniku czasu spędzonego w Internecie zostaje zaniedbywana nauka, praca, rodzina czy kontakty społeczne. Dopóki internet nie przeszkadza w codziennym życiu, nie ma powodów do mówienia o uzależnieniu. W dzisiejszych czasach z internetu korzysta prawie każdy. Wraz z postępem technicznym coraz łatwiej jest się z nim połączyć. Życie bez internetu jest bardzo utrudnione. Każdy z nas korzysta z niego w inny sposób. Jedni używają go do komunikacji interpersonalnej, inni do wyszukiwania informacji czy nauki. Jednak najważniejszą zaletą sieci, ale też wadą, jest to, że zrzesza ludzi poprzez fora czy czaty tematyczne. Osoby o podobnych zainteresowaniach mogą prowadzić rozmowy na interesujące tematy. Mogą się oni wzajemnie wymieniać informacjami, tworzyć od podstaw ekonomie „świata", a czasem nawet prawo. Dla wielu jest to odskocznia od rzeczywistości zwanej przez użytkowników realem.
Każdej osobie internet służy do czegoś innego, jednak dla wszystkich ma taką samą wartość – zaspokaja potrzeby. Trzeba przyznać, że sieć ma naprawdę wiele zalet, ale nie możemy też zapominać o jej wadach. Jako że sieć stała się

powszechnym narzędziem, rozwinęła się wraz z nią przestępczość internetowa (Kozak, 2014, s. 125).

Internetoholizm jest to patologiczne zachowanie osoby polegające na uzależnieniu od internetu. Samo uzależnienie to „nabyta silna potrzeba wykonywania jakiejś czynności lub zażywania jakiejś substancji. W praktyce określenie to ma kilka znaczeń. W języku potocznym „uzależnienie" jest stosowany głównie do osób, które nadużywają narkotyków, leków, alkoholu czy papierosów (Kozak, 2011, s. 102).

Internetoholizm jest to zaburzenie nawyków i popędów w zachowaniu. Obecnie na świecie istnieją dwie najczęściej przyjmowane definicje i klasyfikacje związanych z uzależnieniami. Internetoholizm jest uzależnieniem od czynności, podobnie jak hazard czy zakupoholizm. Nie należy jednak zaliczać tego uzależnienia do schorzeń z grupy zaburzeń psychicznych i zachowań spowodowanych używaniem substancji psychoaktywnych, gdyż nie ma w tym przypadku czynnika fizycznego wywołującego objaw, a także większość stanów związanych z nadużywaniem substancji psychoaktywnych (Bednarek, 2005).

Uzależnienie internetowe, jest to nowy rodzaj nałogu polegający na ustawicznym spędzaniu czasu na kontaktach z komputerem, a zwłaszcza z siecią internet, charakteryzujący się wewnętrznym przymusem bycia w sieci.

Długotrwałe spędzanie czasu przed komputerem zaburza układy rodzinne, pracę i naukę. Osoba uzależniona spędza więcej czasu przed komputerem niż z własna rodziną. Nie wykonuje codziennych obowiązków. Wszyscy powinniśmy przyjrzeć się krytycznym okiem temu, jak korzystamy z internetu i jak ważny jest on w naszym życiu.

Każdy z nas może paść ofiarą jednej z pułapek internetu, jego ciemnych stron. Nie należy jednak rezygnować z niego. Komputer stwarza możliwości rozwoju zarówno w dobrą, cenną stronę, jak i te mniej pozytywną. Musimy pamiętać jednak o tym, że nie wszystko co znajdziemy w sieci, jest prawdziwe, musimy nauczyć się odróżniać rzeczy złe od dobrych, segregować informacje, porównywać je i oceniać. Nie możemy bezkrytycznie dać się podporządkować sieci.

Racjonalne korzystanie z tego, co zostało wynalezione, jest podstawą prawidłowego rozwoju każdego człowieka. Każdy z nas powinien pamiętać o rodzinie, która jest podstawą naszego bytowania. Dane są jednak niepokojące,

dlatego internet śmiało można nazwać nałogiem XXI wieku, któremu niestety, jak również innym nałogom, dajemy się podporządkować i zabrać nasz „cenny życia czas" (Kozak, 2014, s. 131).

Internetoholicy bardzo często dokonują hierarchii potrzeb, stawiając internet na pierwszym miejscu. Jest to nowa choroba cywilizacyjna. Pojawiła się i ukształtowała wraz ze skokiem cywilizacyjnym. Ludzie szukają w Internecie nowego życia, gdyż ich normalne, nie jest takie, jakie sobie wyobrazili. Z powodu zalet i praktycznie nieograniczonych możliwości internet stał się czymś potrzebnym, niezastąpionym, więc ludzie, choć wiedzą, jak bardzo pochłania użytkownika, dalej z niego korzystają (Kozak, 2014, s. 133).

Wielkim problemem w świecie internetu jest względna anonimowość. Niestety ludzie nie zdają sobie sprawy z faktu, że to, że ktoś jest anonimowy, nie znaczy wcale, że jest nie do wyśledzenia. Cyberprzemoc jest to stosowanie przemocy poprzez: prześladowanie, zastraszanie, nękanie. Osobę dopuszczającą się takich czynów określa się mianem stalkera (Kozak, 2013, s. 16-32).

Podsumowując rozważania, internet, który jest dobrodziejstwem naszych czasów, może stać się dla nas, współczesnych ludzi, dużym zagrożeniem. Korzystanie z internetu jest ciekawą alternatywą spędzania czasu, ale nie może stać się jedynym sposobem na spędzanie wolnego czasu. Otaczający nas świat jest często trudny do zrozumienia, a młodzi uciekają w miejsca atrakcyjne i pozornie bezpieczne. Złe i nierozsądne korzystanie z internetu może powodować uzależnienie. Dlatego też obowiązkiem dorosłych jest dbanie o to, by dzieci były bezpieczne w Internecie i by korzystały z niego świadomie. Internetoholizm oraz uzależnienie od gier komputerowych to tylko jedne z nielicznych zagrożeń występujących w sieci (Guerreschi, 2010, s. 95).

Tożsamość w Internecie – Ja realne – Ja wirtualne

Żyjemy w czasach, które ściśle wiążą się z pogonią za dobrami materialnymi i najwyższą pozycją społeczną bez względu na to, w jaki sposób się do niej dochodzi. Młoda osoba, która znajduje się w świecie pełnym sprzeczności, z bagażem silnych przemian wewnętrznych, ma stać się w pełni ukształtowaną i podmiotową jednostką o dojrzałej i spójnej tożsamości. Określenie swojej tożsamości, określenie tego, kim się jest w świecie, jest procesem, na który wpływ ma wszystko to, z czym człowiek się styka, czemu ufa, do czego

ma prawo, co może, i to, co chce robić. Należy jednak pamiętać, że pojęcie tożsamości nie jest proste do zdefiniowania.

Tożsamość jest całością konstrukcji podmiotu, która odnosi się do siebie, do podstawowej potrzeby przynależności, identyfikacji z dziedzictwem, dorobkiem przodków. Pojęcie tożsamości wskazuje przede wszystkim na kontynuację w czasie pewnych cech osobowości. Wskazuje na fakt bycia tym samym, bycia kimś, kto jest tożsamy z sobą, z przeszłością, a więc tożsamy ze swoimi przekonaniami, wartościami, myśleniami, działaniami. Podstawowym zadaniem jednostki w czasie poszukiwania odpowiedzi dotyczącej własnej tożsamości jest określenie swojego Ja.

Poszukiwania własnej tożsamości są różne, począwszy od poszukiwania jej ciągłości istnienia, przez próby zmieniania własnej osobowości, eksperymentowania z samym sobą, po poznawanie samego siebie, które jest związane ze smakowaniem doznań, pogrążaniem się w nich. J. Czachorowska wyróżniła trzy sposoby poznawania siebie:

- poznawanie siebie realizowane samodzielnie poprzez refleksję, zastanawianie się nad sobą,
- poznawanie siebie realizowane samodzielnie za pomocą rzeczowych źródeł informacji,
- poznawanie siebie przy pomocy innych osób (Bednarek, Omelaniuk, Tyszka, Zieliński, 2002).

Kształtujące się w tym okresie poczucie siebie, rozumiane jako jednostkowe poczucie osobowej tożsamości, rozwija się jednocześnie w dwóch kierunkach: indywidualnym (osobistym), w którym poczucie siebie jako osoby ma pewne możliwe do rozpoznania fizyczne, społeczne, emocjonalne i intelektualne właściwości. Kształtuje się w ten sposób obraz własnej osoby, który dotyczy poznawczej świadomości tego, jaką osobą się jest.

Tożsamość osobista wiąże się z uformowaniem Ja, co wyraża się postrzeganiem siebie jako niepowtarzalnej jednostki oraz identyfikowaniem się z celami i standardami osobistymi. Tożsamość osobista stanowi zbiór cech przypisanych tym aspektom Ja, które wywodzą się z jednostkowych cech człowieka. Jest to świadomość własnej spójności w czasie i przestrzeni – w różnych okresach życia, sytuacjach społecznych i pełnionych rolach, a także świadomość własnej odrębności, indywidualności, niepowtarzalności (Kozak, 2014, s. 196).

2.5. Patologia cyfrowego dzieciństwa

Drugi kierunek, to kierunek społeczny. Poznawcze powiązania własnej osoby z innymi ludźmi oraz identyfikowanie się z ich celami i wartościami są wyrażeniem uformowania My. Procesy te również pełnią funkcję obrony obrazu własnej osoby i osiągania własnych celów. Zatem obie te ścieżki – indywidualna i społeczna – są powiązane.

Niekiedy młodzi, dojrzewający ludzie unikają przechodzenia przez trudny proces poszukiwań w zakresie własnej tożsamości. Młodzież włącza się wtedy w grupę społeczną i z niej przyjmuje gotowe wzory ukształtowane przez daną zbiorowość. Wynika z tego, że identyfikacja jest progiem do wejścia na drogę ku dojrzałości, koniecznym etapem w rozwoju tożsamości. Tak kształtuje się Ja realne każdego człowieka (Kozak ,2014, s. 197).

Dzięki internetowi możemy zmienić te elementy naszego życia, z których jesteśmy niezadowoleni, marząc o tym, że aktywnie zrekonstruujemy aspekty własnej tożsamości, często licząc na to, że nasze Ja, stanie się dzięki temu lepsze, bardziej lubiane lub bardziej atrakcyjne. Często nieświadomie przyjmujemy nową osobowość, mającą zupełnie inną postać, niż ta, która jest nam znana. Wydaje się nam, że e-osobowość daje nam odskocznię od napięć i stresów prawdziwego życia.

W realnym życiu bardzo trudno wycofać się z odgrywanej roli, dlatego internet jest tak atrakcyjny dla młodego człowieka, gdyż daje możliwość wylogowania się w każdej chwili, niemal bez żadnych konsekwencji. Lęk przed konsekwencjami ogranicza nasze eksperymenty z tożsamością w Realu, a internet daje możliwość zakazania zakosztowanego owocu. Doskonale ową podatność na zmianę tożsamości ujął Z. Bauman (Jawłowska 2001) określając osoby często zmieniające tożsamość jako gatunki „wszystkoistyczne", czyli osoby nie doskonale wyspecjalizowane, ale te, które jak kameleon dopasowują się do określonego środowiska.

Dzisiejszy nastolatek bardzo często to, co wie o sobie i życiu, czerpie z mediów. Doświadczenie zdobyte przez kontakt z mediami w coraz większym stopniu zastępuje doświadczenie rzeczywiste.

Cyberprzestrzeń kusi brakiem ograniczenia, anonimowością i możliwością restartu, rozpoczęcia w każdej chwili wszystkiego od nowa. Niezależnie od tego, czy używamy internetu często, czy sporadycznie, czy zanurzamy się bez reszty w przestrzeni wirtualnej, nie możemy pozwolić sobie na lekceważenie

psychologicznego wymiaru kreowania drugiego Ja w przestrzeni wirtualnej. Należy mieć świadomość, że to nowe, wirtualne Ja, choć często tak odmienne od realnego, jest to ciągle nasze Ja i zawsze musimy być za nie odpowiedzialni oraz mieć świadomość konsekwencji jego istnienia i wpływu na nasze życie. Jak konstatuje E. Aboujaoude (Aboujaoude, 2012), są ludzie, którzy bywają niezwykle sprawni w rozdzielaniu różnych sposobów funkcjonowania. Ich życie w sieci może być bardzo odmienne od tego poza siecią, ale mimo to udaje im się zachować dość wyraźną granicę między nimi.

Każdy człowiek musi stanąć przed odpowiedzią: kim jestem? – poprzez codzienne decyzje i wybory stylów życia. W czasach społeczeństwa nazwanego informacyjnym tożsamość jest płynna, tymczasowa, powstająca jako rezultat walki różnych wersji i w zależności od sytuacji i światów, w których obecnie się znajdujemy, zmienia się. Kreowanie nowego Ja w cyberprzestrzeni prowadzi do wielu pozytywnych, ale także szkodliwych następstw. Z jednej strony jednostka ma możliwość sprawdzenia się w rolach, w których nie miałaby okazji nigdy się sprawdzić lub posiadałaby wewnętrzne opory w świecie rzeczywistym, do takich zachowań jest przełamywanie różnych barier, jak budowanie większej pewności siebie, odważniejsze podejmowanie życiowych decyzji i wiele innych. Z drugiej jednak strony, kreowanie się w wirtualnej rzeczywistości, tak dalece odległe od realnego wzorca, może prowadzić do sytuacji, w której otrzymujemy ludzi doskonale poruszających się w świecie nowych technologii, lecz nieprzystosowanych do życia w społeczeństwie, radzących sobie lepiej w wirtualnym świecie, ale nie potrafiących radzić sobie ze swoją psychiką i problemami życia codziennego (Kozak, 2014, s. 198).

Poszukiwanie tożsamości, zarówno zbiorowej, jak i indywidualnej, przypisanej i konstruktywnej, staje się fundamentalnym źródłem sensu. Ludzie budują swoje sensy nie wokół tego, co robią, ale wokół tego, kim są lub wierzą, że są. Tożsamość zostaje tu scharakteryzowana jako energiczna siła, która opiera się na niepewnej dynamice społeczeństwa w sieci.

Coraz częściej podkreśla się konsekwencje kształtowania się tożsamości, w której doświadczenie istnienia jest w znacznym stopniu kreowane w przestrzeni medialnej. Technologie informacyjne zdobywają nad ludźmi władzę. Można pokusić się także o stwierdzenie, że obecnie dotarliśmy do miejsca, w którym możemy mniej lub bardziej świadomie zmienić swój świat

zarówno realny, jak i wirtualny, możemy wpływać na zmianę, wartości, przekonań, priorytetów, preferencji, wybranych, bądź wszystkich cech osobowości – zmienić to, kim jesteśmy, na to kim chcielibyśmy być. Coraz szybsze i sfragmentyzowane życie, pozbawione głębszego sensu i punktów odniesienia, sprawia, że internet staje się coraz bardziej popularną formą kreacji siebie samych, a co za tym idzie – sprzyja dramatycznym zmianom w zakresie tożsamości i zachowania (Kozak, 2014, s. 198).

Czy osobowość użytkownika po wkroczeniu do wirtualnego świata uległa zmianie i jak to rzutuje na jego realne Ja? E. Aboujaoude (Aboujaoude, 2012) w swojej książce wymienia następujące cechy całkiem nowej e-osoby: wyolbrzymione poczucie naszych możliwości, wyniosła postawa wobec innych, nowy zbiór fasad moralnych, które przyjmujemy w sieci, skłonność do impulsywnego zachowania oraz tendencja do regresji stanów dziecięcych. Rzeczywiście, wszystko to, co robimy w sieci, to kim próbujemy się stać, co mówimy, jakie mamy cele, zasadniczo różni się od tego, jacy jesteśmy w świecie realnym. Miejsce, czas, forma w cyberprzestrzeni właściwie nie istnieją, gdyż mogą przybierać różne postaci nieskończenie wiele razy.

W rzeczywistym świecie jesteśmy ostrożniejsi i ważymy swoje słowa, ponieważ jesteśmy obserwowani i rozpoznawani; gdy tylko przekroczymy granicę świata wirtualnego, nasze zachowania często ulegają zmianie. Wówczas już tylko krok do zagubienia kontaktu z rzeczywistością i wpadnięcia w wir cyberprzestrzeni.

Podsumowując, nie warto tworzyć na siłę swojej wirtualnej rzeczywistości, bo można na tym wiele stracić. Życie realne jest o wiele bardziej ciekawe od wirtualnego, a żyjąc w nim, mamy pewność, że osoby, z którymi rozmawiamy i spędzamy czas, są wobec nas szczere, a przede wszystkim wiemy, jak wyglądają. Każdy z nas przez chwilę pragnie być innym, ale należy pamiętać o tym, aby się w tej inności internetowej nie zatracić.

Zapobieganie patologii cyfrowej uzależnionych

Od najdawniejszych czasów aż do początków XX wieku naszej ery kobieta uważana była w wielu społeczeństwach za istotę „niższą", gorszą od mężczyzn. Płeć jako pojęcie sprowadza się do zróżnicowania organizmów na męskie i żeńskie. Płeć to zespół właściwości charakteryzujących organizmy osobników

żeńskich i męskich i przeciwstawiających je sobie wzajemnie; też zbiorowo: osobnicy o tych samych właściwościach (Strzałko, 2006, s. 18).

Płeć biologiczną determinuje zespół cech wrodzonych kobiet i mężczyzn wynikających z materiału genetycznego, chromosomów i gospodarki hormonalnej. Cechy te są naturalne, a także niezmienne oraz niezależne od czasu i miejsca urodzenia człowieka (Moir, Jessel, 2010, s. 32).

Dziecko przychodzi na świat z wykształconymi cechami genetycznymi definiującymi jego płeć biologiczną. Na tym etapie wykształca się tożsamość płciowa. Zaczyna się kształtowanie płci psychicznej. Najważniejszy wpływ na rozwój tej tożsamości mają czynniki zewnętrzne, społeczne. Na to stadium ogromny wpływ mają tożsamość kulturowa i społeczeństwo. Zasadniczo przyjmuje się, że około 5 roku życia podstawowa tożsamość płciowa jest już ukształtowana.

Pod wpływem technologii komunikowania się w cyberprzestrzeni, tabletów i smartfonów dochodzi do cyfrowej demencji w mózgu dzieci i młodzieży. Jak pisze dr M. Żylińska w lekturze „Cyfrowej demencji", czytelnik musi zmusić się do myślenia i zweryfikowania pozornie oczywistych tez. Dlatego jest to książka konieczna, bo przecież kto zajmuje się ich wychowaniem lub kształceniem dzieci, powinien odpowiedzieć sobie na pytanie, w jakim wieku i w jaki sposób mają one zacząć nieuniknioną przygodę z nowoczesnymi technologiami. Lekarz Spitzer uświadamia, jak wielka odpowiedzialność spoczywa na nas, dorosłych. Na dzieciach nie wolno eksperymentować. Zanim więc kupimy maluchom laptopy, najpierw zapoznajmy się z wynikami badań w tej tematyce (Spitzer, 2013, s. 45).

Jak pisze M. Brzezińska w „Charakterach": *Liczba bodźców w każdej sekundzie atakujących człowieka zawsze przekraczała możliwości jego percepcji. I zawsze ewolucyjny wyścig wygrywali ci, którzy z kakofonii informacji potrafili wyłonić i przetworzyć najwięcej i najszybciej. Dziś źródła bodźców są potężniejsze niż kiedykolwiek, bardziej inwazyjne, wszechobecne. Człowiek próbuje się do tego dostosować, usiłuje nadążyć. Zmieniają się jego zmysły, sposób przetwarzania informacji. Powstaje nowy homo sapiens (*Charaktery, 2013, s. 29). Można z ostrożnością stwierdzić, że w internecie są prawie wszystkie pytania i odpowiedzi przydatne dzieciom w życiu szkolnym i nie tylko.

2.5. Patologia cyfrowego dzieciństwa

Jak zapobiegać bądź jak leczyć uzależnienia od cyberprzestrzeni? Jest wiele metod zapobiegania tudzież leczenia od uzależnień technologii cyfrowych.
Pierwszą z nich będzie biblioterapia, *biblion* – książka oraz *therapeo* – leczę. Najprościej ujmując, jest to leczenie książką. Najpowszechniejsza w Polsce definicja biblioterapii została zaproponowana przez E. Tomasik, według niej jest to zamierzone działanie przy wykorzystaniu książki lub materiałów niedrukowanych, które prowadzi do realizacji celów rewalidacyjnych, resocjalizacyjnych, profilaktycznych oraz ogólnorozwojowych. Koniecznym elementem biblioterapii jest międzyosobowy kontakt indywidualny lub też grupowy z biblioterapeutą (Konieczna, 2005, s. 16).
Kolejnym sposobem zapobiegania od uzależnienia jest geletologia – metoda relaksacji w życiu realnym i wirtualnym (śmiechoterpia). Jest to termin pochodzący od greckiego słowa gelos – śmiech. Nauka ta zajmuje się badaniem wpływu śmiechu na zdrowie oraz terapia śmiechem.
Formą terapii, szczególnie popularną wśród dzieci są łaskotki. Do glotologii można zaliczyć również kursy rozwijające poczucie humoru. Grupowa terapia śmiechem staje się sposobem na zajęcia integracyjne i relaksacyjne także dla pracowników dużych firm. Praca w ciągłym stresie ma negatywne skutki dla zdrowia człowieka, także źle wpływa na efektywność i wydajność w pracy. Warsztaty „śmiechowe" odstresowują i uczą spontanicznego śmiechu.
Podsumowując, terapią śmiechem jest wszystko to, co nas pobudza do śmiechu. Wielką zaletą leczenia śmiechem jest, że wpływa ona zarówno na ciało, jak i umysł człowieka. Śmiech uczy patrzeć z nadzieją w przyszłość, czerpać radość z poznawanego świata i ludzi, wykorzystując siłę pozytywnego myślenia, pomaga w walce z chorobą (Kozak, 2014, s. 278).
Elektroniczny uśmiech, to ciąg znaków – emotikony. Jak pisze w swoim artykule J. Krywko, pierwszego emotikonu użył prof. Scott E. Fahlman i zapoczątkował modę, która rozpełzła po świecie i… lekko zmieniła działanie naszych mózgów. Doprowadzono do eksperymentu, który miał sprawdzić, jak nasz mózg rozpoznaje emotikony. Pokazywano im prawdziwe uśmiechnięte twarze ☺, a także szereg znaków tworzące popularne emotikony, m.in. emotikon z uśmiechem, czyli „:)". Okazało się, że emotikon uaktywniał u badanych te same części mózgu, co wizerunek prawdziwej uśmiechniętej twarzy (Krywko, 2014, s. 15).

2.5. Patologia cyfrowego dzieciństwa

Podsumowanie

Czas adolescencji powoduje zmiany fizyczne w człowieku, pociągając za sobą konieczność psychicznego, emocjonalnego i społecznego odniesienia się do nich, akceptacji swojego nowego wizerunku i roli społecznej.

Ucieczka w nałóg może być związana z problemami emocjonalnymi czy też słabym poczuciem własnej wartości (Woronowicz, 2012, s. 14). Leczenie uzależnionych jest sprawą niezwykle trudną. Osoby uzależnione w zasadzie muszą samodzielnie poradzić sobie z fizycznymi i psychicznymi dolegliwościami. Najlepszym i skutecznym sposobem na wyzwolenie jest fachowa terapia.

Celem tej publikacji jest zaprezentowanie funkcjonowania współczesnych dzieci pod wpływem oddziaływania nowoczesnych technologii cyfrowych. Myślą przewodnią było wskazanie patologicznych zagrożeń cyfrowego życia..

Gwarantowana wolność prasy i innych środków społecznego przekazu jest ogromnym dobrem, ale tylko wówczas, gdy jest właściwie wykorzystywana. Negatywny wpływ mediów może być zneutralizowany zaangażowaniem w promowanie wartości ogólnoludzkich tą samą drogą, a przy tym w sposób atrakcyjny i rzetelny. Droga przekazu wiedzy i myśli powinna być drogą dialogu i dyskusji, tak, by odbiorca miał wybór, a tym samym możliwość aktywnego uczestniczenia w procesie medialnego przekazu.

Niniejsza tematyka pozwala odpowiedzieć na pytanie: czy media są pomocne w utrwalaniu i ochronie tych wartości, czy też stanowią dla nich zagrożenie? Wydaje się, że i jedno, i drugie. A efekt w konkretnej sytuacji zależy zarówno od nadawców, jak i odbiorców.

2.6. Cyberprzestrzeń – miejsce spotkań migrantów i rodzin globalnych

Wprowadzenie w wybrane procesy społeczeństwa globalnego – relacje rodziny na odległość osadzone w cyberprzestrzeni.

Społeczeństwo XXI wieku przybrało znamiona społeczeństwa globalnego – bez granic, barier technologicznych, ograniczeń kulturowych oraz naznaczonych wieloma nowymi procesami (Beck, 2002, s.40). Jest nazywane również społeczeństwem sieciowym, w którym cyberprzestrzeń stała się nowym miejscem życia wielu ludzi (Baran, Misiewicz, 2014, s.7). W dobie powszechnej nowoczesności warto zwrócić uwagę na pewne procesy wpływające na podstawową komórkę budującą społeczeństwo, jaką jest rodzina. Dzięki otwartym granicom i ułatwionym dostępem do wyboru nowego miejsca pracy i życia, migracja stała się powszechnie znanym zjawiskiem. Oznacza wędrówkę ludności, której konsekwencją jest zmiana miejsca zamieszkania (Kubitsky, 2012, s. 8). W ostatnich latach emigracja, imigracja i sama migracja nabrały szczególnego znaczenia oraz zainteresowania ze względu na swój zasięg i następstwa. Jednym z następstw, o których będzie mowa w dalszej części, to powstanie – jak to określa Ulrich Beck – rodzinnych relacji na odległość (Beck, 2013, s. 5), osadzonych w cyberprzestrzeni.

Migracja jako początek rodzin globalnych.

Zaczynając do pojęcia migracji, należy zauważyć, że jest to zjawisko o szczególnym przedsięwzięciu, które nosi znamiona nadziei - na lepsze jutro, a zarazem ryzyka - utraty czegoś ważnego. Zmieniając miejsce pobytu, człowiek może być kimś innym, robić coś całkiem innego, nadać nowy kształt swojemu życiu. Jednakże, każda migracja odciska swego rodzaju piętno na psychice ludzkiej - dobre i złe. Z jednej strony, życie poza granicami własnego państwa jest swego rodzaju rozbudowanym kapitałem społecznym dla danej jednostki – przynosi jej wiele nowej wiedzy na temat życia innych ludzi, ich warunkach gospodarczych, walorach kulturowych oraz wiedzy na temat samego siebie. Z drugiej strony, często zdarza się, że migrant traci kontakt z rodziną,

z najbliższymi osobami, łatwo jest także zgubić własną tożsamość w obcym i dalekim miejscu, co więcej, w obecnym świecie pojawiają się coraz to nowsze zagrożenia sfery publicznej związanej z organizacją i funkcjonowaniem ludzkiej przestrzeni (Bonisławska, 2012, s. 114), rzeczywistej i wirtualnej.

Migrację można podzielić na wiele podtypów (np. migrację zewnętrzną i wewnętrzną, trwałą i okresową, zarobkową i polityczną, czy stosunkowo nowe typy jakimi są migracje z miłości, itp.), jednak to właśnie migracja zarobkowa jest jednym z najpopularniejszych tematów – wciąż aktualnych - rozmów i wszelakich publikacji.

Największą chęcią wyjazdu w celach zarobkowych interesują się przede wszystkim ludzie młodzi - do 24 roku życia. W badaniu przeprowadzonego dla CBOS w 2008 roku, niemal 19% respondentów odpowiedziało, że zamierza w przyszłości pracować poza Polską lub już posiada propozycję pracy za granicą, natomiast 11% respondentów zastanawia się nad wyborem miejsca pracy w kraju lub poza nim. Wyjazdem najbardziej są zainteresowani studenci i uczniowie. Wśród starszych badanych - w wieku od 25 do 34 lat, 14% respondentów twierdzi, że zamierzają ubiegać się o pracę lub już podjęli kroki w sprawie pracy za granicą. Kolejną kategorią ludzi najbardziej zainteresowanych migracją zarobkową są bezrobotni, 18% badanych przyznało, że starają się o zatrudnienie poza granicami państwa (CBOS, 2008, s. 2). Decyzja o emigracji jest nie zawsze łatwa, lecz czasem świadomość tego, że ktoś z członków rodziny lub znajomych jest już zatrudniony w innym państwie ułatwia podjęcie decyzji o swoim własnym wyjeździe.

Niezależnie od czasu przygotowania i wewnętrznych przemyśleń, moment wyjazdu jest zawsze bardzo trudny. W rozmowach przed wyjazdem, przyszli emigranci ukrywają swoje obawy - jak tam będzie?, czy sobie poradzę?, a co jeśli mi nie wyjdzie?. Rozmowy kierują wtedy na tematy neutralne - stan pogody, plan podróży, przygotowanie dokumentów i najpotrzebniejszych rzeczy do wyjazdu (Kubitsky 2012, s. 10). Migracja odciska pewien rodzaj piętna na człowieku, choć ślad po nim bywa różny. Istotną rolę w doznaniach migranta odgrywa wiek. Inaczej wyjazd przeżywa nastolatek, który żyje w świecie marzeń i pragnień oraz ma całe życie przed sobą, inaczej na tę kwestię będzie patrzyła osoba starsza, która więcej żyje przeszłością niż przyszłością, a zupełnie inaczej

jest w przypadku dziecka, dla którego wyjazd do innego kraju będzie oznaczał nowy dom, a socjalizacja nie odbyła się jeszcze w pełni.
„Ten kto mówi o rodzinie, musi także mówić o pracy i pieniądzach, kto mówi o małżeństwie, musi mówić o wykształceniu, zawodzie, mobilności, a ponadto o utrzymujących się nierównościach, przy (dalece) wyrównanych w międzyczasie warunkach zdobywania wykształcenia" - Ulrich Beck mówi otwarcie i wprost, że rodzina musi pamiętać i myśleć o pieniądzach, które są niezbędne do utrzymania domu, o pieniądzach które zapewniają spokój oraz dają szansę na lepsze jutro. Mając w świadomości wagę pieniędzy, rodzice, którzy zamierzają wyjechać, są zwykle tak zajęci praktyczną stroną migracji, że często zapominają (albo ukrywają w podświadomości) o psychologicznych następstwach u dzieci. Dzieci nie mają wyboru, najczęściej rodzic jest już zdecydowany na wyjazd, jego zadaniem wtedy jest wytłumaczenie dziecku, że "tak będzie lepiej". Przez wiele lat utrzymywało się przekonanie, że migracja w przypadku najmłodszych członków rodziny jest przeżyciem pozbawionym ryzyka - całkowicie. Natomiast samo życie mówi już całkiem co innego. Mnóstwo dzieci migrantów, pomimo upływu lat nosi w sercu ogromny żal do rodziców, dla których stały się one *bagażem podręcznym* (Beck, 2013, s. 22). W przypadku takich miejsc migracji jak Hiszpania, Grecja, Portugalia czy Finlandia zdążyło wyrosnąć już kilka pokoleń dzieci, które musiały dorastać bez jednego z rodziców - najczęściej ojca. Badacze psychologii dziecięcej zauważali u większości z nich syndrom nieobecnego rodzica, co skutkowało nie raz uczuciem zagubienia w życiu oraz niepewności. W przypadku kobiet - matek, najczęściej migrują one na Zachód, stają się „matkami na odległość" dla własnego potomstwa. Jest to swoistego rodzaju dylemat kobiety - matki, która zostawia swoje ukochane dziecko w kraju z miłości do niego, aby za granicą zarobić pieniądze na sfinansowanie nauki, leczenia czy godnego życia. Tutaj skutkiem psychologicznym odbijającym się na dziecku może być tzw. choroba sieroca. Skutki tego rodzaju odległości rodziców od dzieci czasem ukazują się już wtedy, kiedy (nieraz) wieloletnie rozstanie dobiegnie końca, kiedy rodzice wracają i mogą mieć znów swoje dzieci u boku. Często bywa wtedy tak, że między ludźmi, którzy stali się sobie w pewnej mierze obcy, nierzadko rozwijają się konflikty i nieporozumienia.

2.6. Cyberprzestrzeń – miejsce spotkań migrantów i rodzin globalnych

Podjęcie decyzji o wyjeździe cały czas oparte jest na kalkulacji - rozrachunku zysków i strat. Bezsprzecznym wnioskiem jest to, że w określeniu *migracja zarobkowa,* jest zawarte, iż głównym celem wyjazdu jest, dzięki pracy za granicą, zdobycie środków pieniężnych. Jednocześnie należy zauważyć, że w migracji zarobkowej, nie tylko same pieniądze odgrywają pierwszorzędną rolę. Migrant jest świadom tego, że istnieją również inne korzyści, jak na przykład zwiększenie własnego kapitału społecznego - poznanie innej kultury, nabranie nowych doświadczeń oraz wzrost szans naukowych dla swoich dzieci (Kawczyńska – Butrym, 2008, s. 110-111). Jest to świat kuszących obietnic związanych z przyszłością nie tylko swoją, ale także swoich dzieci.
Z socjologicznego punktu widzenia, migrację ludności można obserwować pod dwoma kątami - zysków i strat. Po stronie zysków można przypisać efekty finansowe, wzrost kwalifikacji zawodowych, co jest bardzo cenioną wartością w środowisku pracowniczym, opanowanie języka oraz kontakt z inną kulturą, uzyskanie znacznie wyższych finansów na kształcenie dzieci, sama w sobie poprawa jakości życia (życie na godnym poziomie, uzyskanie bezpieczeństwa socjalnego poprzez np. spłatę kredytów, opłacenie długów czy opłacenia środków medycznych) oraz poczucie spełnienia i sukcesu, wzrost wiary we własne możliwości. Natomiast po drugiej stronie kryje się ryzyko dnia codziennego: rodzina pozostała w kraju pozostaje formalnie pełną, lecz funkcjonuje jako niepełna, co stwarza ryzyko rozpadu rodziny, codzienny ból rozłąki - tych, którzy zostali i tych, którzy wyjechali, trudności w socjalizacji dzieci, zmiany w systemach wartości migrantów, brak udziału w podstawowych jednostkach życia społecznego, wycofanie się z pełnienia niektórych ról społecznych oraz częste zjawiska wykluczenia i marginalizacji. Łatwo zauważyć, że po stronie plusów stoją wartości materialno- finansowe, po stronie minusów stoją już wartości rodzinno – emocjonalne (Kawczyńska – Butrym, 2008, s. 114). Czy można twierdzić, że jedne wartości są ważniejsze od drugich? Jest to kwestia bardzo indywidualna, nie jest łatwa do jednogłośnego werdyktu.
Kolejny problem jaki pojawia się w migracji jest moment powrotu. Można się zastanawiać, dlaczego? Osoby wyjeżdżające za granicę tak samo długo przygotowują się do wyjazdu z kraju, jak i do powrotu do niego. Przyzwyczajenie do miejsca oraz do nowego stylu życia powoduje pewien dyskomfort dla jednostki, której życie toczy się dwutorowo. Po pierwsze,

migrant musi zmierzyć się z myślą o tym, do czego i do kogo wraca. Czas nieobecności w kraju odgrywa ważną rolę. Wystarczy kilka miesięcy, aby taka osoba zauważyła różnicę pomiędzy dwoma światami. Lecz nie tylko otoczenie się zmienia, ludzie również. Rodzina zauważa pewne zmiany u osoby wyjeżdżającej za granicę do pracy, ta natomiast dostrzega różnice w zachowaniu rodziny, dzieci czy znajomych. Każda ze stron zdobyła pewne, nowe doświadczenia oraz przeżycia, wszystkim przybyło lat. Nie zawsze, ale często jest trudno zaczynać od początku poznawanie świata życia codziennego. Tylko nielicznym udaje się dbać o bliskie związki na odległość. Współczesna technologia ułatwia kontaktowanie się pomimo wielotysięcznej odległości dzięki takim wirtualnym narzędziom jak SMSy, portale społecznościowe, Skype. I w tym momencie pojawia się pytanie, o społeczne wartości cyberprzestrzeni.

Cyberprzestrzeń jako nowe miejsce spotkań rodzin na odległość

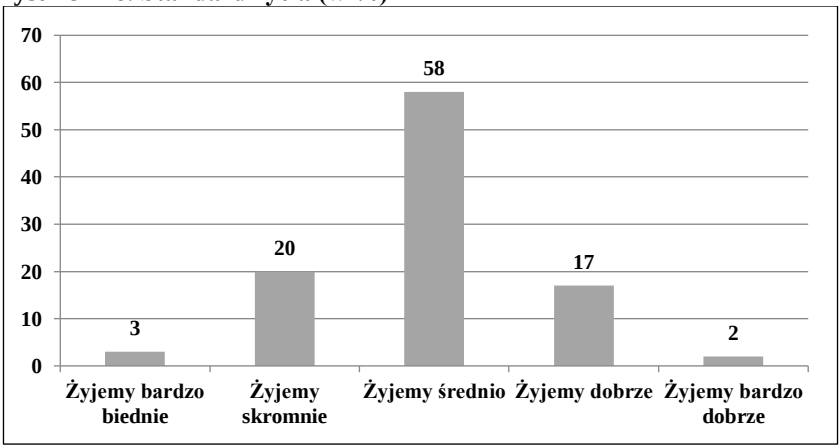
W teoriach socjologicznych można zauważyć powstanie teorii społeczności *bezlokalnych*. W tej teorii uznaje się, że lokalne społeczności ulegają pewnej specjalizacji, gdzie w ich obrębach tworzą się społeczności o bardzo wąskich cechach. Nazwanie ich społecznościami *bezlokalnymi* wzięło się stąd, że nie ograniczają się tylko do jednego, konkretnego i wyznaczonego obszaru, kontakty międzyludzkie są oderwane od danego terytorium, mają przeróżne zasięgi przestrzenne, a ich składy wzajemnie się nie pokrywają (Baran, Misiewicz, 2014, s. 8). Rodziny na odległość zaczynają wpadać w grupy zaliczające się w społeczność bezlokalową ze względu na brak określonego miejsca w przestrzeni realnej. Cyberprzestrzeń jest określana jako *konsensualna halucynacja*, w której bardzo trudno jest odróżnić realny świat, miejsce życia jednostek i rodzin od istniejących tylko i wyłącznie w pamięci komputerów świata wirtualnego (Limanówka, 2007, s. 229-230). Dlatego w pewnym momencie, w życiu rodzin, gdzie jeden z ich członów jest daleko, zaczynają pojawiać się problemy. Wirtualna przestrzeń i nowinki technologiczne pozwalają na kontakt z przeróżnych miejsc na całej ziemi. Nie jest problemem, żeby ojciec lub matka zadzwoniła przez Whats App do dziecka, lub żeby babcia zobaczyła się z wnukiem na Skype. Ale nigdy nie będzie to prawdziwy, realny kontakt. W każdym momencie, kiedy rozmowa z rodziną zaczyna być niewygodna można się rozłączyć i nie wracać do tematu. W realnym świecie,

w codziennym życiu rodzinnym nie można się tak nagle rozłączyć. Kolejną sprawą są światy, w których rodziny przebywają. Po zgaszeniu ekranu komputera, każda z osób wraca do swojego, czasem nowego świata. Jedna zostaje w domu, druga wpada w wir nowych doświadczeń na nowym miejscu. Czas spotkań w cyberprzestrzeni jest również dobierany dla wygody – kiedy ma się czas lub ochotę. Czy w realnym życiu, również można dogodnie wybierać momenty i nabierać ochoty na spotkania z rodziną?

Przyszłość migracji

Kolejnym pytaniem, które można zadać i które można analizować, w kwestii migracji ludności, jest: czy pomimo wszelakich konsekwencji (pozytywnych i negatywnych) ludzie nadal będą wyjeżdżać w poszukiwaniu lepszej przyszłości? Uważam, że tak. Ludzie zawsze migrowali, migrują i będą migrować - nawet nieświadomie.

Rysunek 26. Standard życia (w %)



Źródło: Komunikat z badań CBOS, http://www.cbos.pl/SPISKOM.POL/2014/K_044_14.PDF

Migracje towarzyszą ludziom od samego narodzenia, zmiana szkoły, miejsca pracy czy zamieszkania, a nawet wyjazd na wakacje – wszystkie te przykłady wiążą się ze zmianą miejsca przebywania, czyi innymi słowy – z migracją. Jednakże często ludzie nie zwracają albo nie przywiązują uwagi na to. Jest to normalna kolej rzeczy, stojąc w jednym miejscu bez żadnych zmian, jednostka

nie rozwija się i nie poszerza swojego kapitału społecznego. Jednakże, najczęstszym wyborem dla osób decydujących się opuścić swój dom, jest migracja zarobkowa. I jeśli już kierować przemyślenia konkretnie w stronę migracji zarobkowej, można wyprowadzić tezę, że Polacy nadal będą wyjeżdżać w poszukiwaniu lepszych rozwiązań finansowych.
Na podstawie badań CBOS z 2014 roku, tylko 19% badanych odpowiedziało, że żyją bardzo dobrze przez co mogą sobie pozwolić na pewne luksusy - powyższy rysunek. Natomiast 81% respondentów twierdzi, że ich życie materialne jest średnie bądź skromne (CBOS, 2014, s. 1). Nikt nie chce żyć biednie, czy liczyć pieniądze, aby wystarczyły do przysłowiowego *pierwszego*. Dlatego czasem praca poza granicami własnego państwa jest jedynym możliwym rozwiązaniem.

Podsumowanie

W XXI wieku pojęcie migracji nabrało szczególnego znaczenia oraz cieszy się wielkim zainteresowaniem wśród badaczy. Szeroki wachlarz typologii migracji daje ogromne możliwości szczegółowych analiz migrantów, ich rodzin oraz samego środowiska wyjazdowego. Szczególną uwagę zwraca na siebie migracja zarobkowa, na którą zdecydowało się do tej pory już około dwóch milionów Polaków. Czy ludzie nadal będą wyjeżdżać? Z pewnością tak, lecz nie zawsze będzie to wyjazd typowo do pracy za granicą, są podróże, wymiany studenckie czy delegacje, które rozbudowują kapitał społeczny danej osoby.
Z przedstawionych rozważań wynika, że pomimo przedstawionych wad i zalet migracji (o których prawdopodobnie migranci wiedzą), ludzie i tak będą podejmowali decyzję o wyjeździe. W obecnym świecie pojawiające się nowinki technologiczne i wszechobecna cyberprzestrzeń pozwalają na pewną imitację spotkań rodzin globalnych. Dzięki wielu dostępnym w cyberprzestrzeni aplikacjom on-line, ból spowodowany rozłąką staja się mniejszy, ale czy nie staje się pewną imitacją prawdziwych emocji i uczuć? Łatwo jest się *wyłączyć* z życia rodzinnego będąc tysiące kilometrów od domu. W dobie zagrożeń spowodowanych terroryzmem, kataklizmami, klęskami żywiołowymi, cyberprzestrzeń i brak poczucia osobistej odpowiedzialności za jej nadmierne wykorzystywanie, staje się kolejnym społecznym problemem. W dobie postępującej informatyzacji i mediów społecznościowych, cyberprzestrzeń stała

się „miejscem spotkań" dla wielu osób, zwłaszcza tych, które opuszczają swoją ojczyznę w poszukiwaniu lepszego życia. Dzięki temu moment wyjazdu i uczucie bólu związany z rozłąką z bliskimi staje się jakby mniejszy. Człowiek żyje w przeświadczeniu, że nie opuścił swojego poprzedniego życia tak do końca – wirtualnie przecież zawsze może wrócić w miejsca, gdzie są jego bliscy. Tylko czy takie relacje mogą przetrwać i zastąpić życie „w realu"? Z pewnością nie, ale taka alternatywa staje się narzędziem podtrzymującym więzi rodzinne i społeczne.

2.7. „Papierowe małżeństwo" jako efekt kontaktów w cyberprzestrzeni

Wprowadzenie

Celem niniejszego opracowania jest zdefiniowanie i opisanie zjawiska tzw. „papierowych małżeństw" zawieranych przez osoby pochodzące z różnych państw, kultur i religii. „Papierowe małżeństwo" to potoczne określenie oszustwa matrymonialnego, w wyniku którego związek zawierany jest po to, aby zyskać dostęp do korzyści ekonomicznych oraz społecznych lub też, co interesuje migranta, otrzymać wizę lub zezwolenie na pobyt. W wyniku „zawartego związku" następuje „łączenie rodzin", a migracja wtedy staje się legalna. Podkreślić należy, jak kontakty w cyberprzestrzeni w celach zawarcia „papierowego" - fałszywego małżeństwa oraz zalegalizowania pobytu w kraju docelowym mogą mieć daleko idące konsekwencje społeczne i kulturowe, a nawet polityczne. Opracowanie jest próbą syntezy zjawiska pod względem teoretycznym, jak również jego empirycznego oparcia na przeprowadzonych badaniach. Zastosowanie obserwacji oraz przeprowadzone dla Urzędów Wojewódzkich wywiady środowiskowe, w ramach prowadzonych postępowań administracyjnych, w sprawach dotyczących zezwolenia na pobyt na terenie Polski, pozwoliło na zebranie materiału, który odzwierciedla fragment tego ciekawego, ale jakże skomplikowanego zagadnienia badawczego. Małżeństwa międzynarodowe ze swej natury są zderzeniem cywilizacji w podstawowej komórce społecznej - rodzinie. W związku z tym brak porozumienia na poziomie kulturowym jest a priori wpisane w ich charakter. Barbara Szacka wskazuje, iż w polskiej rodzinie konflikty pojawiają się najczęściej z przyczyn (1) finansowych, zaraz potem głównymi powodami są: (2) podział obowiązków domowych oraz (3) problemy związane z wychowaniem dzieci (Szacka, 2003, s. 392). Owe przyczyny będą się bardziej intensyfikować w małżeństwach międzynarodowych, gdzie stykają się różne wzorce kulturowe, decydujące często o podziale obowiązków i sposobie wychowywania dzieci.

„Papierowe małżeństwa"

Każde państwo w swoich dokumentach ustrojowych przedkłada między innymi suwerenność jego obywateli, poczucie bezpieczeństwa, równości wobec prawa oraz prawo do zawarcia małżeństwa i założenia rodziny, i w następstwie - prawo do poszanowania życia rodzinnego. Wśród najważniejszych przepisów wzmacniających ochronę prawa do poszanowania życia rodzinnego oraz zawarcia małżeństwa są: (1) Powszechna Deklaracja Praw Człowieka z 1948 r., (2) Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności z 1950 r., (3) Międzynarodowy Pakt Praw Obywatelskich i Politycznych z 1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167), (4) Karta Praw Podstawowych Unii Europejskiej (Dz. Urz. UE 2012 Nr C326/391) oraz (5) Kodeks rodzinny i opiekuńczy (Dz. U. z 2017 r. poz. 682). Terminy „papierowe małżeństwo", „małżeństwo dla pozoru", „fałszywe małżeństwo", czy „fikcyjne małżeństwo", nie posiadają definicji stanowiącej legalne osadzenie zjawiska w prawie. Istnieje rozbudowana linia orzecznicza, jak również opracowania prawnicze pozwalające ustalić, iż przez „papierowe małżeństwo" możemy rozumieć małżeństwo zawarte między obywatelem państwa o zaostrzonym systemie wizowym (docelowego) a obywatelem państwa trzeciego (lub obywatelem państwa trzeciego posiadającym prawo do zgodnego z prawem pobytu na terytorium państwa docelowego a obywatelem państwa trzeciego), którego wyłącznym celem jest nadużycie procedur wizowych (określone w prawie warunki wjazdu i pobytu obywateli państw trzecich na terytorium państwa docelowego). Obywatele państw trzecich chcący zawrzeć „papierowe małżeństwo" wśród czynników, które wpłynęły na podjęcie ich decyzji wymieniają: (1) czynniki ekonomiczne (poprawa sytuacji materialnej), (2) czynniki związane z bezpieczeństwem (uniknięcie prześladowań, dyskryminacja, konflikty wojenne i etniczne) oraz (3) czynniki kulturowe (perspektywy rozwoju osobistego i zawodowego). Zawarcie i pozostawanie w związku małżeńskim osoby z państwa trzeciego pozwala na uregulowanie statusu pobytowego cudzoziemca na uproszczonych zasadach, co w konsekwencji stanowi utrudnienia w wydalaniu takich osób z terytorium danego kraju. Zjawisko to nie dotyczy tylko uwarunkowań Unii Europejskiej, ale również innych rozwiniętych gospodarczo i społecznie krajów świata. „Papierowe małżeństwa" funkcjonują w krajach rozwiniętych od lat i mają

wypracowane swoje schematy. Ludzie zawierają związki małżeńskie z różnych powodów. Jedni z miłości, inni dla pieniędzy, jeszcze inni dla zapewnienia sobie poczucia bezpieczeństwa. Niektórzy imigranci natomiast chcą w ten sposób otrzymać „zieloną kartę" umożliwiającą im legalny pobyt w Stanach Zjednoczonych Ameryki (USA). Małżeństwo z obywatelem amerykańskim jest jednym z najpopularniejszych sposobów zdobywania zielonych kart przez imigrantów. Tylko w latach 1998-2007 tą drogą status rezydenta USA (*Lawful Permanent Resident – LPR*) otrzymało przeszło 2,3 miliona osób. W 2007 roku 274 358 zielonych kart (ponad 1/4 wszystkich wydanych w tym roku) należała do małżonków obywateli amerykańskich. Od 1985 roku liczba osób, które zalegalizowały w ten sposób swój status, wzrosła dwukrotnie; od 1970 - czterokrotnie. Popularność legalizacji statusu przez „papierowe małżeństwo" jest nieprzypadkowa. Liczba związków wzrasta wraz ze wzrostem restrykcji przepisów imigracyjnych. (Kern-Jędrychowska, 2009). Przed przystąpieniem Polski do Unii Europejskiej obywatele naszego kraju korzystali z takich możliwości w celu zalegalizowania swojego pobytu w krajach Europy Zachodniej. Sytuacja zmieniła się radykalnie z chwilą przystąpienia Polski do Unii Europejskiej. Nasze granice stały się otwarte poprzez rozszerzenie Strefy Schengen, przez co łatwe do przemieszczania się osób, a polskie dokumenty podróży - przepustką do większości krajów Europy. Bez wiz obywatel Polski może poruszać się po całej Unii Europejskiej. Uzyskanie polskiego obywatelstwa przez cudzoziemca następuje między innymi (…) *przez cudzoziemca przebywającego nieprzerwanie w Polsce co najmniej od 2 lat na podstawie zezwolenia na pobyt stały lub zezwolenia na pobyt rezydenta długoterminowego UE, który pozostaje co najmniej od 3 lat w związku małżeńskim zawartym z obywatelem polskim lub nie posiada żadnego obywatelstwa* (…), (Ustawa z dnia 2 kwietnia 2009 r. o obywatelstwie polskim Dz. U. z 2012 r. poz. 161 z późn. zm.). W wyniku działań prawnych cudzoziemiec może uzyskać obywatelstwo Polskie w wyniku zawarcia związku małżeńskiego i łączenia rodzin. Formalnie rzecz biorąc związek małżeński uznawany przez prawo Rzeczpospolitej Polskiej jest z definicji związkiem zawartym przez kobietę i mężczyznę przed urzędnikiem Urzędu Stanu Cywilnego w obecności świadków, którzy własnymi podpisami zaświadczyli o zaistnieniu tego faktu. Jednakże może on być tylko i wyłącznie „papierowym

małżeństwem", dlatego też jest wielce prawdopodobne, że nastąpi w takim przypadku odmowa udzielenia obywatelstwa. Ustawa z dnia 12 grudnia 2013 roku (Dz.U. z 2016, poz.1990 z późn. zm.) wskazuje w art. 165, że (…) *cudzoziemcowi odmawia się udzielenia zezwolenia na pobyt czasowy w celu połączenia się z rodziną – w przypadku cudzoziemca pozostającego – w związku małżeńskim z cudzoziemcem, o którym mowa w art. 159 ust. 1 pkt 1 – gdy związek małżeński został zawarty w celu obejścia niniejszej ustawy* (…). Zawarcie małżeństwa z cudzoziemcem w celu ułatwienia mu legalizacji pobytu („papierowe małżeństwo") na terytorium Polski podlega sankcjom karnym zgodnie z treścią art. 264 i 264a ustawy z dnia 6 czerwca 1997 r. – Kodeks karny , które stanowią, iż: (…) *Art. 264: § 2. Kto wbrew przepisom przekracza granicę Rzeczypospolitej Polskiej, używając przemocy, groźby, podstępu lub we współdziałaniu z innymi osobami, podlega karze pozbawienia wolności do lat 3. § 3. Kto organizuje innym osobom przekraczanie wbrew przepisom granicy Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8. Art. 264a: § 1. Kto, w celu osiągnięcia korzyści majątkowej lub osobistej, umożliwia lub ułatwia innej osobie pobyt na terytorium Rzeczypospolitej Polskiej wbrew przepisom, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. W wyjątkowych wypadkach, gdy sprawca nie osiągnął korzyści majątkowej, sąd może zastosować nadzwyczajne złagodzenie kary, a nawet odstąpić od jej wymierzenia* (…). Tak właśnie przepisy prawa polskiego określają zasady zawierania związku małżeńskiego, łączenia rodzin, udzielania obywatelstwa i sankcji karnych za czyny wykraczające poza prawo w tym zakresie.

Kontakty w cyberprzestrzeni początkiem znajomości i drogą do „papierowego małżeństwa"

Jaki jest cel zawierania małżeństw „tylko na papierze" i nie realizowania zawartych w prawie, zarówno formalnym, jak i zwyczajowym, określonych obowiązków? Odpowiedź na to pytanie jest prosta, uzyskanie obywatelstwa jednego z Państw Członkowskich Unii Europejskiej (PC UE) daje nieograniczone możliwości w całej Unii. Wprowadzenie Strefy Schengen pozwoliło na swobodny przepływ ludzi, wartości ekonomicznych, kultury i wielu jeszcze innych dóbr i zjawisk współczesnego świata. Otworzyło to drogę

do zalegalizowania migracji w UE oraz dało możliwość obywatelom „państw trzecim" na swobodne podróżowanie i szukanie „swojego" miejsca w życiu. Przede wszystkim pobyt na terenie strefy Schengen i, co z tym się wiąże, prawo swobodnego przemieszczania się po terenie Unii Europejskiej, ułatwiły cudzoziemcom dostęp do świadczeń socjalnych, dały sposobność umorzenia ewentualnych procedur wydaleniowych, a w dalszej perspektywie nawet uzyskanie obywatelstwa kraju Unii Europejskiej i tzw. „łatwe, lepsze życie" bez konieczności podjęcia pracy zarobkowej, z licznymi profitami oferowanymi przez kraj docelowy.

Małżeństwo, do którego zawarcia dążą obcokrajowcy, staje się faktem w świetle prawa, ale nie zawsze jest faktem w aspekcie społecznym i kulturowym. Do chwili zawarcia takiego związku wszystko wydaje się, że jest normalne, a dalsze „szczęśliwe" życie jest tylko kwestią czasu. Pierwszym etapem zaistnienia małżeństwa jest zawarcie znajomości zainteresowanych osób. W normalnych okolicznościach ludzie poznają się, spędzają ze sobą czas i w wyniku wspólnej decyzji zawierają związek małżeński. Tak idealizując to zagadnienie nie widzimy innych, odbiegających od „normalności", sytuacji. Małżeństwa są zawierane przez osoby z różnych kręgów kulturowych, różnych religii, różnych narodowości i z różnych pobudek. Małżeństwo stało się dziś instytucją o zasięgu międzynarodowym, globalnym. Ulrich Beck tak ujął to zjawisko: (…) *Wielu spośród tych, którzy należą do rodzin światowych nie jest ani zwróconych do świata, ani otwartych na niego, ani doświadczonych na międzynarodowym parkiecie, ani mówiących płynnie wieloma językami, z pewnością zaś nie otacza ich aura dalekiego, wielkiego świata (...) i niepokoi ich wszelka obcość. Niektórzy stali się częścią rodziny światowej w efekcie przemocy, wojny domowej albo wypędzenia; inni w wyniku nadziei uniknięcia biedy i bezrobocia w ojczyźnie; jeszcze inni przez ogłoszenia w internecie bądź przypadek miłości. Mówiąc krótko wielu z nich tworzy rodziny światowe w mniejszym lub większym stopniu ze względu na okoliczności i konieczności zewnętrzne, a nie na zamiłowania czy w wyniku swobodnej decyzji* (…), (Beck, Beck-Gernsheim 2013, s. 21-22).

We współczesnej Europie, według Barbary Szackiej, małżeństwo coraz częściej traktowane jest jako związek dwojga ludzi, którego głównym celem jest zaspokojenie potrzeb emocjonalnych i seksualnych, nie zaś potrzeb

ekonomicznych ani nawet reprodukcyjnych. Związek oparty wyłącznie na wzajemnych uczuciach staje się bardziej kruchy i częściej ulega rozpadowi niż związek, którego podstawą była współzależność ekonomiczna, (Szacka 2003, s. 384). Inne natomiast jest podejście obywateli krajów islamskich, gdzie małżeństwo nie jest sakramentem, a jedynie umową cywilno – prawną, dlatego też ewentualny rozwód dla mężczyzny nie pociąga za sobą żadnych konsekwencji i nie jest związany z żadnymi formalnościami, a zawarcie małżeństwa z osobą odległą emocjonalnie nie jest problemem, (Nydell 2001, s. 92). Kiedy natomiast ewentualne korzyści znacznie przewyższają straty, mamy do czynienie ze swego rodzaju „interesem", czy „współzależnością ekonomiczną", które łączą obie strony. Czy jednak powoduje to większą trwałość związku małżeńskiego? Sakrament małżeństwa jest pewnego rodzaju wyzwaniem i to nie tylko w sferze uczuć. Jeżeli celem związku małżeńskiego jest migracja ekonomiczna lub ucieczka z obszaru objętego konfliktem zbrojnym (uchodźctwo), to osoby zainteresowane związkiem będą same szukały w cyberprzestrzeni odpowiedniego kandydata na współmałżonka. Media społecznościowe, portale internetowe, czy też strony z usługami „randkowymi", stają się miejscem odwiedzin osób zainteresowanych „papierowym małżeństwem". Dawniej, w dobie braku dostępu do internetu, poznanie osoby z obcej kultury było niemalże nieosiągalne i na pewno wiązało się to z wyjazdem w odległe krańce świata. Dziś, wraz z rozwojem mediów społecznościowych w cyberprzestrzeni nawiązywanie kontaktów, również międzynarodowych, jest znacznie ułatwione. Portale społecznościowe przepełnione są potencjalnymi kandydatami czy kandydatkami na współmałżonków. O ile Europejczycy (zarówno kobiety, jak i mężczyźni, być może częściej szukają przygód niż trwałych związków), o tyle obywatele tzw. „krajów trzecich" poszukują raczej trwałych związków, a wraz z nimi - kart pobytu. Mężczyźni z reguły poszukują Europejek. Sytuacja, kiedy kobieta posiada wśród znajomych na portalu społecznościowym jednego mężczyznę pochodzenia arabskiego, prowadzi do znaczącego zainteresowania profilem tej kobiety innych mężczyzn pochodzenia arabskiego wraz z prośbami o dodanie do kontaktów. Najczęściej to są mężczyźni z krajów Afryki Północnej, Bliskiego Wschodu. Scenariusz ich działania jest bardzo prosty: nawiązać kontakt, poznać, zainteresować sobą oraz skłonić do zawarcia związku. Oczywiście jest to jeden ze scenariuszy działania.

Bardzo ważnym aspektem w działaniu zmierzającym do zawarcia „papierowego małżeństwa" jest chęć osiągnięcia korzyści majątkowej. Kobiety otrzymują zwykle, w wyniku zawarcia takiego związku, ustaloną z góry kwotę pieniędzy. Mieszane kulturowo małżeństwa zawierają często kobiety z wykształceniem podstawowym lub zawodowym, pozbawione perspektyw życiowych, żyjące z dnia na dzień, często pochodzące z rodzin patologicznych, charakteryzujące się prymitywizmem w hierarchii swoich wartości życiowych. Takie małżeństwo jest dla nich specyficzną nobilitacją, swego rodzaju awansem społecznym. Inną kategorią są kobiety wykształcone (lub nie), ustabilizowane finansowo, często z bagażem doświadczeń, w średnim wieku, posiadające dorosłe i samodzielne dzieci. Pobudkami, które nimi kierują są potrzeba zabicia samotności, dowartościowania się, a także podniesienia swojej atrakcyjności poprzez wejście w związek z obcokrajowcem, najlepiej młodszym i pochodzącym z Bliskiego Wschodu. Zdarzają się nieliczne wyjątki, kiedy w tego typu związkach mężczyzna bywa starszy. (…) *Polki przeważnie są postrzegane jako bardzo dobre żony: Poza tym, że są urodziwe, są jeszcze pracowite, opiekuńcze, dbają o dom i męża. Są też uważane za bardziej pruderyjne od Niemek czy Francuzek. Ta ostatnia opinia może u niektórych cudzoziemców, zwłaszcza pochodzących z krajów islamskich, powodować skojarzenia z ich rodzimymi skromnymi, spolegliwymi kobietami, które można zamknąć w domu i mieć tylko dla siebie* (…), (Nydell 2001, s. 65-70). Polki zatem wydają się partnerkami bardziej atrakcyjnymi, ponieważ związek z nimi jest szansą na uzyskanie „karty pobytu w lepszym świecie". Kandydaci na mężów nie zdają sobie jednak sprawy z faktu, że są one, wbrew ich wyobrażeniom, bardziej wyemancypowane i niezależne. Istotną rolę w ułatwianiu nawiązywania bliskich znajomości odgrywają również tzw. „swaci" - grupy przestępcze, których działalność polega na „kojarzeniu par" za stosowną opłatą Legalizują oni pobyt cudzoziemcom, których tytuły pobytowe już się skończyły lub okres ich ważności zbliża się ku końcowi. Jako kandydatki na żony „rekrutowane są" mało atrakcyjne kobiety o niskiej samoocenie, z rodzin ubogich lub patologicznych, które chcą się wyrwać z „błędnego koła ubóstwa i marazmu". Często za obecność na ślubnym kobiercu otrzymują ustaloną kwotę pieniędzy. Obiecuje się im dostatnie życie, dlatego też bez wahania podejmują decyzję o wejściu w taki związek małżeński. Kiedy jednak dochodzi do sfinalizowania tzw. „papierowego małżeństwa, wszystko

zmienia się diametralnie, życie takiej kobiety przeradza się w koszmar. Jest to proces stopniowy i przebiega z różną intensywnością. Małżeństwo międzynarodowe, w którym pojawiło się dziecko, nie jest wolne od podejrzenia, iż zostało zawarte w celu obejścia przepisów pobytowych i zalegalizowania pobytu ojca dziecka. Nierzadko zdarzają się przypadki porzucania żony z dzieckiem, znęcania się nad rodziną, porywania dzieci, czy też szantażu emocjonalnego dziećmi. Wreszcie jako przykład można podać starania cudzoziemca o zalegalizowanie pobytu w Polsce w celu sprawowania opieki nad małoletnim dzieckiem widywanym raz na pół roku, lub rzadziej, albo które z matką wyjechało z Polski jakiś czas temu.

Trudności związane z badaniem zjawiska „papierowych małżeństw"

Zjawisko to jest trudne do zbadania w sposób metodologiczny. O ile możliwym do sprawdzenia jest wykonywanie przez małżonków tzw. obowiązków małżeńskich, o tyle sfera emocjonalna związku jest nieweryfikowalna, a stanowi bardzo istotny element badania całego zjawiska. W badaniach ankietowych potrzebna jest obiektywna ocena danych faktów społecznych. I tu rodzi się wątpliwość o obiektywne udzielenie odpowiedzi przez badanych. Zawieranie małżeństw w celu obejścia przepisów zgodnie z art. 264a kodeksu karnego jest kwalifikowane jako umożliwianie lub ułatwianie innej osobie pobytu na terytorium Rzeczypospolitej Polskiej wbrew przepisom i jest karalne (Kodeks karny, Dz.U. 1997 Nr 88 poz. 553 z późn zm.). Rodzi to wątpliwość, dlaczego ktoś, kto zawarł „papierowe małżeństwo" w celu uzyskania tytułu pobytowego, a także w celu stworzenia przed organami państwa polskiego iluzji praworządności, miałby bez powodu demaskować się? Możliwe jest podanie ilości ujawnionych małżeństw zawartych w celu obejścia przepisów, ale jaka jest ilość tych nieujawnionych? Ilościowe trudności badawcze nie negują jednak istnienia zjawiska. Dlatego w opracowaniu posłużono się studium przypadku, w celu zobrazowania tego zjawiska bez podawania jego skali.

Pożycie „papierowych małżeństw" – studia przypadków

Jak trudne to jest życie „papierowych małżeństw", możemy się dowiedzieć z przykładów, które są w zakresie badanego zjawiska społecznego, a które w sposób wyraźny odzwierciedlają jego skomplikowaną naturę. Jeśli

cudzoziemiec tuż po ślubie oddali się od żony, nie będzie utrzymywał z nią kontaktów chyba, że jedynie w chwilach, kiedy ważność czasowa tytułu pobytowego się kończy, a ponadto będzie wspierał ją ekonomicznie od czasu do czasu, to kobieta ta nie będzie chciała rozwodu. Będzie ona pozostawać wprawdzie w fikcyjnym związku małżeńskim, ale nie będzie to stanowiło dla niej problemu. Co jakiś czas odegrają zgodną parę przed organami administracji państwowej. Po uzyskaniu stałego pobytu mężczyzna jednak może oddalić się od żony na zawsze. Pominąć tu można kwestię, że taki cudzoziemiec może mieć problemy z uzyskaniem legalizacji pobytu, ponieważ okoliczności prowadzenia wspólnego gospodarstwa domowego są sprawdzalne. Wielu mężów cudzoziemców unika podjęcia pracy – najczęściej pod pretekstem nieznajomości języka, nic jednak nie robią w kierunku nauczenia się go. W przypadku, kiedy związek małżeński został – przynajmniej z jednej strony – zawarty tylko w celu zalegalizowania pobytu, najczęściej ta strona stwarza jeszcze pozory zgodnego życia małżeńskiego , aby jak najdłużej utrzymać tytuł pobytowy. Natomiast w sytuacji, kiedy mąż – cudzoziemiec mimo, że z jego strony zostało zawarte „papierowe małżeństwo", nie wytrzyma gry pozorów, to pojawiają się konflikty. Może to zdarzyć się tuż po ślubie lub w dłuższej perspektywie czasowej. Zdejmie „maskę" wchodząc w rolę „pana i władcy" i usiłując wprowadzać swoje, w jego mniemaniu, jedynie słuszne zasady wspólnego życia. Wtedy zwykle pojawia się przemoc w rodzinie, szantaż, ma miejsce porywanie dzieci, wzajemne upokarzanie się, (Nydell, 2001, s. 90).

Przypadek pierwszy:

(…) *Możemy tu przedstawić dialog pomiędzy funkcjonariuszem Straży Granicznej, a mieszkanką jednego z Polskich miast dotyczący jej męża pochodzącego z Egiptu i dzieci:*

- funkcjonariusz Straży Granicznej (fSG): „Gdzie jest pani mąż i dzieci?"

- Kobieta (K): „Jak to gdzie?!" Są na placu zabaw. Mąż zabrał je do piaskownicy!"

- (fSG) „Nie, pani mąż i pani dzieci są w drodze do Egiptu."

- (K) „niemożliwe, przecież przed chwilą jeszcze tu byli".

Można sobie wyobrazić zaskoczenie tej kobiety. Niezwłocznie odebrała swoje dzieci z lotniska, a jej maż sam poleciał do Egiptu (…).

Jest to przykład jak dalece zakorzenione w psychice mężczyzn krajów islamskich jest poczucie przynależności dzieci do rodziny ojca. Można przypuszczać, że miał on plan wywiezienia z Polski i oddania ich pod opiekę własnej matce lub siostrze, aby wyrośli na przykładnych muzułmanów. Jest to również przykład, jak bardzo ci mężczyźni ukrywają własne poglądy i w jakim stopniu potrafią stwarzać pozory. Przywołanemu zdarzeniu osobliwości dodaje fakt, że rodzina ta nie przejawiała żadnych cech patologii czy anomalii. Było to małżeństwo międzynarodowe wspólnie wychowujące dzieci, żyjące bezkonfliktowo. Nic nie wskazywało na to, że mąż – ojciec będzie chciał wywieźć dzieci z Polski – nota bene polskich obywateli.

Przypadek drugi

(...)*Po ślubie mąż bardzo się zmienił. Stał się chorobliwie zazdrosny. Zabrania mi spotykać się z moimi znajomymi. Zabrania mi wychodzić z domu. Toleruje tylko moje wyjścia do pracy, bo jestem jedynym żywicielem rodziny. Mąż nie podjął żadnej pracy i nie czynił żadnych starań w tym kierunku. Zmusza mnie żebym przeszła na islam i żyła według jego zasad. Często mnie bije i stosuje terror psychiczny. W trakcie wyrabiania przez niego kart pobytu zastraszał mnie, żebym nie wspominała o jego postępowaniu. Namawiał mnie do porzucenia pracy i wyjechania z nim do Niemiec lub Szwecji żeby żyć z tamtejszego „socjalu". Tam mieszka jego rodzina. Mówił, że nie będziemy musieli nic robić. Odkąd dostał kartę stałego pobytu jest jeszcze bardziej nieznośny.. Nie mogę już wytrzymać. Pomóżcie*.(...).

Przypadek trzeci

(…) *Poznałam męża przez internet. To on mnie znalazł i pierwszy napisał. Szybko nawiązaliśmy kontakt, wymieniliśmy się numerami telefonów. Pierwsze spotkanie było na neutralnym gruncie w restauracji (pada nazwa miasta na południu Polski). Następnie spotykaliśmy się u niego w mieszkaniu. Ja do niego jeździłam, bo twierdził, że nie ma samochodu. Zaprosiłam go do domu na Święta Wielkanocne. Mohamed postarał się aby wszyscy go polubili. „Owinął sobie wokół palca" moich rodziców i moje córki. Nadskakiwał nam na każdym kroku. Mieliśmy wspólne plany. Zaplanowaliśmy ślub na wrzesień, ale Mohamed nalegał na przyśpieszenie terminu, bo nie miał*

żadnego tytułu pobytowego na terenie Polski. Wcześniej miał już żonę Polkę. Powiedział, że musiał się rozwieźć, bo żona go nie chciała i wyrzuciła go z domu. Jego była żona odnalazła mnie i jeszcze przed naszym ślubem ostrzegała mnie przed nim. Mówiła, że ożenił się z nią po to, aby szybko zrobić dziecko i dostać dokumenty. Teraz jego syn ma sześć lat, a on nigdy nie interesował się nim i nie łożył na jego utrzymanie. Bywał w domu tylko wtedy, gdy kończyła się jego karta pobytu. Wtedy był bardzo miły i troskliwy. Uważałam, że ta kobieta jest zazdrosna. Nie brałam pod uwagę tego co mówiła, bo go kochałam. Wzięliśmy ślub z Mahomedem. Zamieszkaliśmy w domu u moich rodziców. Oddali nam do dyspozycji całe piętro. Mąż po ślubie zmienił się o 180 stopni. Był niemiły, wręcz wulgarny. Nie cieszyłam się nim długo bo wyjechał nad morze do pracy. Prosił żebym go nie odwiedzała. Latem poinformowałam go telefonicznie, że jestem w ciąży. Nie ucieszył się, że będzie tatą. Nie interesował się moim samopoczuciem i rozwojem dziecka. Tematem naszych rozmów były głównie jego dokumenty pobytowe i czy wszystko załatwiłam jak należy. W ciągu pół roku odkąd wyjechał do pracy odwiedził mnie tylko trzy razy i to tylko dlatego, że musiał przywieźć dokumenty potrzebne do karty pobytu. Podczas tych odwiedzin był bardzo niemiły i dręczył mnie psychicznie. Straszył mnie, że jak zasnę to podczas snu udusi mnie poduszką (…).

Powyższe przypadki obrazują konflikty powstałe w „papierowych małżeństwach" na bazie różnic kulturowych pomiędzy wyemancypowanymi, niezależnymi Polkami, przyzwyczajonymi do równego i godnego traktowania ludzi, niezależnie od ich płci, a mężczyznami drażliwymi na punkcie swojego honoru, pochodzącymi z kultury, gdzie honor mężczyzny zależy od uległości, bezwzględnego posłuszeństwa i wstrzemięźliwości jego żony. Z przyczyn czysto ekonomicznych pozwalają lub wręcz zmuszają oni swoje żony do pracy zawodowej, ale po pracy odcinają je od dotychczasowego trybu życia. Wszelkie kontakty, a zwłaszcza z innymi mężczyznami, są im surowo zabraniane. Opisani cudzoziemcy przyzwyczajeni są do tego, że mężczyźni mają diametralnie inne prawa i obowiązki niż kobiety, o czym szerzej pisze Margaret Nydell, (Nydell, 2001, s. 65-70). Od Europejczyków wymaga się tolerancji na odmienność kulturową. Pojęcie to jest jednak obce cudzoziemcom pochodzącym spoza Europy. Bardzo często objawia się u nich rasizm, który w kulturach ich

pochodzenia jest traktowany jako coś naturalnego służącego dowartościowaniu i ochronie własnej grupy etnicznej. O tym zderzeniu kultur również należy pamiętać mówiąc o konfliktach etnicznych wewnątrz podstawowej komórki społecznej.

Dla równowagi należy wspomnieć o przypadkach – chociaż nielicznych – kiedy to kobiety wykazują agresywne zachowania.

Przypadek czwarty
(…) *Pewna, pochodząca z Górnego Śląska, żona obywatela Algierii, wymierzyła swojemu mężowi potężny cios, kiedy ten usiłował wprowadzać w ich związek „swoje zasady". Mężczyzna przeżył tak silny szok i to nie tylko fizyczny ale też i kulturowy, że nawet jej nie oddał. Od czasu tego krótkiego nieporozumienia żyją zgodnie. Cudzoziemiec dostosował się do nowych reguł prawnych i kulturowych, a ich związek przestał być tylko i wyłącznie „papierowym małżeństwem"* (…).

Działania władz w celu ukrócenia „papierowych małżeństw"
Biorąc pod uwagę, że większość „papierowych małżeństw" kojarzonych jest poprzez pośredników, płyną z tego tytułu korzyści materialne. Ów pośrednik, niezależnie od pobudek, którymi się kieruje , swoim działaniem wyczerpuje znamiona przywoływanego wyżej artykułu 264a kodeksu karnego:
(…) *§ 1. Kto, w celu osiągnięcia korzyści majątkowej lub osobistej, umożliwia lub ułatwia innej osobie pobyt na terytorium Rzeczypospolitej Polskiej wbrew przepisom, podlega karze pozbawienia wolności od 3 miesięcy do lat 5. § 2. W wyjątkowych wypadkach, gdy sprawca nie osiągnął korzyści majątkowej, sąd może zastosować nadzwyczajne złagodzenie kary, a nawet odstąpić od jej wymierzenia* (…).
Obok przepisów prawa istotna jest w tym zakresie szersza współpraca różnych organów państwa w celu ujawnienia tego typu przestępstwa. Jesteśmy informowani okresowo o takich działania organów państwa, Policji, Straży Granicznej, prokuratury oraz o wyrokach, które zapadły w sądach różnych instancji. Są to działania nie tylko ostatnich lat, ale działania te trwają sukcesywnie od dłuższego czasu. (…) *Czy Polacy i Wietnamczycy pobierali się z miłości czy też był to zwykły biznes i papierowe małżeństwa? Prokuratura bada*

polsko-wietnamskie śluby zawierane w gminie Mirzec (...) Kilka miesięcy temu Straż Graniczna przeprowadziła kontrolę w Urzędzie Stanu Cywilnego w Kunowie. Okazało się, że dwa zawarte tam w 2002 r. śluby między Polakami a Wietnamczykami były fikcyjne. Cudzoziemcy potrzebowali ich tylko po to, aby łatwiej uzyskać kartę stałego pobytu (…), (Słowo Kieleckie, 2006).

Podsumowanie

Z podanych wyżej przykładów mogłoby wynikać, że jedynie Polki zawierają „papierowe małżeństwa" z cudzoziemcami z Bliskiego Wschodu. Oczywiście nie jest to prawdą. Są to przykłady najbardziej jaskrawe, ale nie jedyne. Polscy mężczyźni również zawierają związki małżeńskie z cudzoziemkami. Sposoby są jednak odmienne od opisanych powyżej. Zwykle poznają swoją wybrankę podczas podróży służbowej w mniej lub bardziej egzotycznym kraju, lub też w czasie urlopu. Miejscem nawiązania znajomości jest często terytorium Polski. Polacy żenią się zwykle z cudzoziemkami pochodzącymi z krajów byłego Związku Radzieckiego lub dalekich egzotycznych, afrykańskich, południowoamerykańskich, czy dalekiego wschodu (Wietnam, Korea, Tajlandia). W pożyciu małżeńskim bywają również niesympatyczni i agresywni. Wtedy żona cudzoziemka jest w bardzo niekomfortowej sytuacji. W obcym kraju, zastraszona, bez elementarnej wiedzy odnośnie miejsca, w którym może uzyskać pomoc, osamotniona w swoim cierpieniu i bojąca się „deportacji".

Głównym celem wielu cudzoziemek wychodzących za Polaków bywa podwyższenie standardu życia dla siebie i swojej rodziny. Małżeństwo traktują bardzo instrumentalnie. Zdarzają się przypadki kobiet uprawiających nierząd na terenie Unii Europejskiej, wyłudzających kredyty, wykorzystujących swojego męża jako sponsora dla swoich interesów, których on jest często nieświadomy. Wyżej wymienione przykłady obrazują wykorzystywanie Polek i Polaków jako współmałżonków w „papierowym małżeństwie", w celu zalegalizowania pobytu cudzoziemca w Polsce, a jednocześnie w całej Unii Europejskiej.

Polacy zawierają różne znajomości na portalach społecznościowych, ale nie dotyczą one kobiet z Bliskiego Wschodu. Te bowiem mają kulturowy zakaz wiązania się z mężczyznami pochodzącymi z innych kultur z uwagi na panującą tam zasadę, że dzieci należą do rodziny ojca. Powodowałoby to akulturację. Muzułmański mężczyzna wchodzący w kontakt seksualny z kobietą nie

muzułmanką płodzi dzieci muzułmańskie będące obywatelami krajów członkowskich Unii Europejskiej. Należą one do rodziny ojca i, według jego tradycji, powinny być wychowywane przez kobiety z nim spokrewnione, np. matkę, siostry, ponieważ wychowanie dzieci nie należy w krajach arabskich do obowiązków mężczyzny.

W tym miejscu należy również wspomnieć o małżeństwach nazywanych przez ogół społeczeństwa polskiego „normalnymi", małżeństwach heteroseksualnych, które wychowują dzieci, dzielą się na co dzień obowiązkami. Cudzoziemcy, w zdecydowanej większości, niezależnie od płci, przyjeżdżają i przestrzegają obowiązującego w Polsce prawa. Zachowują swoje obyczaje, przekonania religijne i nawyki żywieniowe, jednak bez narzucania się rdzennej ludności. Z drugiej strony jednak można obawiać się, że taki zasymilowany imigrant może być członkiem grupy terrorystycznej, który czeka na odpowiedni moment do podjęcia działań przestępczych, a póki co odgrywa rolę przykładnego męża i ojca. Taki idealny kamuflaż jest nie do zdemaskowania w działalności terrorystycznej.

Należy w tym miejscu jednak zaznaczyć, że wśród małżeństw międzynarodowych bywają małżeństwa, oparte na „czystej relacji". Wymagają one jednak od obydwu małżonków głębokiego zrozumienia drugiej strony i wzajemnego szacunku. Tworzą je osoby o dość wysokim poziomie intelektualnym i kulturowym, (Giddens, 2010, s. 124-137).

Nie mniej jednak regułą opisywanego zjawiska jest to, że „papierowe małżeństwa" zawierane są zwykle, gdy istnieje zagrożenie dla legalności pobytu. Fakt ten oddziaływuje na pozorny przypływ uczuć ze strony osoby zagrożonej deportacją. Można byłoby więc wysnuć pochopny wniosek, że nie ma lepszego afrodyzjaku, jak kończąca się wiza.

Urzędy Stanu Cywilnego w Polsce nie traktują „papierowych małżeństw" jako sposobu na zalegalizowanie pobytu cudzoziemca na terenie Polski. W związku z tym proceder legalizacji pobytu poprzez zawieranie małżeństw w celu ominięcia przepisów migracyjnych jest procesem ciągłym. Mamy tu do czynienia z sytuacją opisaną przez Robina Williamsa, (…) *kiedy publicznie uznawana norma jest potajemnie gwałcona na skalę masową przy milczącej zgodzie lub nawet aprobacie samego społeczeństwa lub grupy, przynajmniej tak długo jak to pogwałcenie pozostaje w ukryciu* (…), (Sztompka 2005, s. 236).

2.7. „Papierowe małżeństwo" jako efekt kontaktów w cyberprzestrzeni

W ten sposób cudzoziemiec jeśli nawet nie otrzyma od polskiego organu administracji państwowej karty pobytu na terenie Polski, a co za tym idzie na terenie Unii Europejskiej na podstawie aktu ślubu, może ją otrzymać od innego państwa członkowskiego jako członek jego rodziny. W ten sposób imigrant ma szerokie uprawnienia do pełnego wykorzystania wolności przysługujących mu w Strefie Schengen.

2.8. Topical issues on investigation of crimes connected with cybercrime in Ukraine

Today the development pace of the Ukrainian component „world wide web" can compete as with European components as with global ones. At the same time, along with the spread of information technology the vulnerability of electronic computers (PCs), automated systems, computer and telecommunication networks to commit crimes with the use of computer technology is increasing drastically. Thus, energy supply facilities, transportation systems, financial and banking industry, military and law enforcement agencies, commercial, medical and scientific institutions - all of them who use the World Wide Web are potential victims of criminal attacks.

Criminal offenses in this sphere are stipulated by Chapter XVI of the Criminal Code of Ukraine (further – CC of Ukraine), namely: Article 361 „Unauthorized interference in the work of electronic computers (PCs), automated systems, computer or telecommunication networks", Article 361-1 „Creation with the purpose of stealing, distribution or sale of harmful software or technical means, as well as their distribution or sale", Article 361-2 „Unauthorized sale or distribution of classified information stored on electronic computers (PCs), automated systems, computer networks or data carriers with such information", Article 362 „Unauthorized actions with information that is being processed in the electronic computers (PCs), automated systems, computer networks or stored on data carriers, committed by a person who is entitled to access it", Article 363 „Inappropriate use of electronic computers (PCs), automated systems, computer

or telecommunication networks or data protection rules, which is being processed in them", Article 363-1 „Obstruction to work of electronic computers (PCs), automated systems, computer or telecommunication networks by means of mass distribution of telecommunication messages".

The object of these crimes is a part of information relationships that are provided by electronic computers (PCs) (further – PCs), automated systems, computer or telecommunication networks.

Analysis of the statistics indicates that in our country the dynamics of crime in the use of electronic computers (PCs), automated systems, computer or telecommunication networks is unstable. Thus, since 2010 a trend of their decline (by 12,4% in comparison with 2009) has started. This trend accelerated in 2011, when it was registered 131 crimes as opposed to 190 crimes, that were published in 2010. In 2012, 138 crimes were registered, indicating a small increase (7%). In 2013, the number of registered crimes of the mentioned category has reached the number 595, but in 2014 their number decreased to 443. In 2015 the number of reported crimes increased again to 598. In 2016 the number of accounted crimes was 818.

In 2010, according to official court statistics data for crimes specified in Chapter XVI of the Criminal Code of Ukraine (further – CC of Ukraine) 69 people were convicted. In 2011, the number of prisoners has slightly decreased to 56. At the same time, in 2012, guilty verdicts entered into force for up to 80 persons. Starting from 2013 there was a reduce of the number of convicted persons to 49. The above pattern lasted for over the next three years: in 2014 – 37 persons, in 2015 – 31 persons, in 2016 – 24 persons.

2.8. Topical issues on investigation of crimes connected with cybercrime in Ukraine

Thus, for the past six years law enforcement bodies carried out the investigation of 2913 crimes of the mentioned category, according to the results of trial, 346 persons received guilty verdicts, one person was acquitted.

It should be noted that the above mentioned chapter of the Criminal Code of Ukraine does not include all of the criminal offenses in this area. At present these crimes cannot be classified on the legislative level due to the absence in the current legislation of the basic concept „cybercrime". These criminal offenses may be committed in various ways (steal of computer information, DoS-attacks, website defacement, distribute malware (viruses), carding, phishing, erasing programs or data distribution messages (spam), creating false online auctions, etc.) and are often qualified as ordinary crimes.

In particular, Article 190, part 3 of the CC of Ukraine (fraud committed by illegal transactions using computer technology), Article 200 of the CC of Ukraine (use of counterfeit electronic access to banking accounts), Article 301, part 4 of the CC of Ukraine (sale and distribution of pornographic materials using computer technology), Article 191, part 2 of the CC of Ukraine (withdrawal by financial institution official of electronic funds from bank accounts of clients that were in possession of that person on a legal basis) and others. In this regard, the recommendation also refers to other criminal offense in this area, for which we use the terminology „cybercrime"; „computer crimes"; „crimes in the sphere of information relations" and so on.

Experience shows that one of the biggest problems is the collection and study of electronic evidence during the investigation of criminal offenses of this category and their court proceedings. This problem applies not only to crimes related to computer data (provided by Articles 361 - 363-1 of the CC of Ukraine),

but also to many „traditional" socially dangerous acts that leave electronic traces in computer networks, magnetic and optical media or screens.

In our opinion key sources of the emergence of this problem lie in two reasons. First, lack of adequate initial training for officers of law enforcement and judicial bodies of the state. In particular, without basic knowledge in the field of IT technologies and fully formed techniques of collection and use of such evidence it is necessary to attract professionals to remove large amounts of equipment or spend a lot of time on their disclosure and fixation. In addition, lack of means which can be used by investigators for this purpose by themselves (without specialists), is another obstacle to effective work with electronic evidence [3, p. 314].

Even more problems cause so-called electronic evidence, which act as the means of committing criminal offenses in the field of computer technology. Usually, it's „malware"that are used in the form of computer viruses; programs designed to neutralize passwords or other means of information protection from unauthorized access; spyware etc [4, p. 946]. To investigate such evidence it is necessary to use a special kind of methods and tools that will not only demonstrate the essence of such evidence, its internal structure, structural elements and their relationships, means of existence and distribution, but also the level of danger of the program, actual effects of its use and the level of damage.

In most cases, research of such information actually comes in the form of expertise without the participation of investigators. Moreover, initiators of this research cannot formulate the right questions in legal documents to experts without the help of specialists, because they have no idea what evidence may be available on expropriated objects. The indicated usually leads to the need

to study a large number of electronic carriers for the purpose to detect the presence or absence of electronic traces of the criminal offense.

However, during court proceedings while carrying out criminal proceedings and while interrogating the experts who carried out the study of electronic evidence the conclusions are only announced. Demonstration of their features would increase the efficiency of evidence investigation, but there is a question of whether the level of knowledge of court, parties and other participants of criminal procedure duly accept such demonstration.

The second reason for the study of the problem is „poverty" of national legislation in this area. Despite the presence of a number of existing regulations on cyberspace security problems of the state, they do not cover the entire spectrum of necessary social relations.

Terminological field in this area remains fragmented, which prevents the formation of effective legal documents on combating cyberthreads. It should be noted that not only established definition of key terms („cyberspace"; „cyber security"; „cyber defense";„cyberattack";„cyberterrorism") are absent, but also those ones that can be effectively used in the practice of law enforcement bodies. The absence of a specific legal definition „electronic evidence" leads to some problems while collecting and evaluating the evidence in order to establish the circumstances that are relevant to the criminal proceedings.

Thus, in accordance with Article 84, part 2 of the CPC of Ukraine procedural sources of evidence can be found among other documents. Paragraph 1, part 2, Article 99 of the mentioned Code stipulates the fact that documents may include drives and carriers, including electronic ones. So, we have provided the

definition of „electronic evidence", which is inextricably linked with the notion „document".

However, such understanding of electronic evidence is not optimal, because it brings into question the legality of use while proving other effective electronic sources.

As an example, in order to establish the possible traces of the crime there should be conducted an examination on the program's damage installed on the main server of accounting department of the central governmental authority. Withdrawal of material carrier (base unit), taking into account the duration of the examination, will save the opportunity to give salary to civil servants.

Using the appropriate forensic tools - namely, software tools for forensic investigation of disk content, the required examination was conducted.

The question remains of whether we can consider a disk image as a proof in the sense defined in the Criminal Procedure Code of Ukraine? Definite answer at this time is not possible, because Ukrainian courts have different attitude to it.

Summary

All of the above indicates that the solution to these problems requires, first of all, professional development of officials level of various departments working in law enforcement bodies and judges by introducing mandatory trainings in the universities.

Also, there is a need to develop common methods of collecting electronic evidence during the preliminary investigation and present them in court.

3. Streszczenia i słowa kluczowe:

Garwol Katarzyna

1.1. Prywatność w sieci w ujęciu przepisów prawa i analiz badawczych

Streszczenie:
Prywatność jest wartością, która wydaje się być istotna dla każdego człowieka. We współczesnym świecie, gdzie media cyfrowe, a zwłaszcza internet, zajmują poczytne miejsce, prywatność zmienia swoje znaczenie. Z jednej strony technologia sprawia, że ludzie są nieustannie obserwowani i lokalizowani, z drugiej strony często sami dzielą się w internecie swoim życiem, przekraczając nie tylko granice prywatności, ale też i intymności. Niniejszy artykuł opisuje jak prywatność jest definiowana przez badaczy zjawiska, jakie są normy prawne odnoszące się do ochrony prywatności oraz przedstawia badania na temat prywatności użytkowników w sieci.

Słowa kluczowe:
prywatność, internet, bezpieczeństwo, media społecznościowe.

Prokopowicz Dariusz

1.2. Rozwój złośliwego oprogramowania ransomware jako nowy wymiar cyberprzestępczości przejmowania kontroli nad systemami informatycznymi firm i banków

Streszczenie:
W artykule opisano problematykę odnotowanego w 2016 roku silnego wzrostu aktywności w internecie złośliwego oprogramowania typu ransomware, za pomocą którego cyberprzestępcy blokują działanie komputera, smartfona lub innego urządzenia podłączonego do globalnej sieci. W zainfekowanym w ten sposób komputerze lub innym urządzeniu ofiary cyberataku wyposażonym w mikroprocesor i internet wyświetlany jest komunikat z żądaniem zapłacenia okupu za przywrócenie prawidłowego działania zainfekowanego urządzenia. W obliczu narastających zagrożeń ataków hakerskich, w tym rozsyłania spamu zawierającego złośliwe oprogramowanie typu ransomware coraz więcej firm i banków tworzy dodatkowe zabezpieczenia systemów informatycznych i stale udoskonala pod tym względem wykorzystywane w prowadzonej działalności oprogramowanie i infrastrukturę informatyczną. Obecnie dominuje opinia, że proces ten nigdy się nie zakończy, przynajmniej dopóki realizuje się postęp technologiczny, ponieważ powstają nowe aplikacje i platformy internetowe, nowe wersje systemów operacyjnych oraz urządzenia infrastruktury informatycznej powszechnie wykorzystywane przez użytkowników. Każda niedoskonałość systemów informatycznych, teleinformatycznych sieci internetowych, wewnętrznych procedur bezpieczeństwa zostaje szybko wykryta i wykorzystana przez cyberprzestępców. Dotychczas dominował model łatania luk w zabezpieczeniach wcześniej wykrytych przez hakerów. Biorąc pod uwagę silny wzrost aktywności niebezpiecznych programów ransomware model ten powinien ulec zmianie polegającej na odwróceniu kolejności działań. To zatrudnieni w firmach, bankach i instytucjach publicznych informatycy powinni wyprzedzając cyberprzestępców możliwie najwcześniej wykrywać luki w zabezpieczeniach. W związku z tym obecnie wzrasta potrzeba prewencyjnego,

profilaktycznego w swej istocie procesu doskonalenia procesów zarządzania ryzykiem systemów informatycznych funkcjonujących w instytucjach finansowych, przedsiębiorstwach oraz podmiotach sektora publicznego.

Słowa kluczowe:
bezpieczeństwo systemów informatycznych, złośliwe oprogramowanie, ransomware, Business Email Compromise, cyberprzestępczość, cyberatak, internet, raporty dotyczące zagrożeń, luki w zabezpieczeniach, bezpieczeństwo usług bankowych, bezpieczeństwo informacji, systemy bezpieczeństwa, bankowość internetowa

Orzechowska Anna
Gugulski Marcin

1.3. Rozwój cyberprzestrzeni zagrożeniem dla bezpieczeństwa baz danych.

Streszczenie:
Postępujący rozwój społeczeństwa informacyjnego połączony z doskonaleniem i upowszechnianiem rozwiązań informatycznych i telekomunikacyjnych powoduje przenoszenie kolejnych aspektów ludzkiej działalności ze świata rzeczywistego w cyberprzestrzeń wirtualny obszar powstały wewnątrz i w zasięgu oddziaływania urządzeń informatycznych oraz telekomunikacyjnych. Coraz więcej osób nie wyobraża sobie codziennego funkcjonowania bez korzystania z cyberprzestrzeni: różnorodnych portali, poczty elektronicznej, komunikatorów, cyfrowych bibliotek, powszechnej łączności bezprzewodowej oraz wirtualnych pieniędzy. Niestety, do cyberprzestrzeni przeniknęły również negatywne zjawiska typowe dla świata rzeczywistego.
Wszystkie cechy, które zadecydowały o powstaniu nowej jakości w komunikacji, handlu, czy usługach stały się również okolicznością sprzyjającą powstawaniu zupełnie nowych możliwości dla chuliganów, złodziei, terrorystów, czy szpiegów. Poczucie anonimowości, brak geograficznych granic, łatwość ukrywania i szyfrowania treści, ogromna prędkość zmian technicznych sprzyjająca wykorzystywaniu wynikających z niej ludzkich błędów i pomyłek powodują, że zagrożenia płynące z tej strony stają się coraz poważniejsze. Celem niniejszego artykułu jest ukazanie zagrożeń związanych z wykorzystaniem najnowszej technologii.

Słowa kluczowe:
informacja, cyberprzestrzeń, zagrożenie, prawo.

Prokopowicz Dariusz
Gwoździewicz Sylwia

1.4. Analiza bezpieczeństwa ochrony systemów informatycznych w kontekście globalnego cyberataku ransomware przeprowadzonego w dniu 27 czerwca 2017 r.

Streszczenie:
Realizujący się od końca ubiegłego wieku intensywny rozwój technologii informatycznej i teletransmisji danych wykorzystywany jest także do niezgodnej z normatywami prawa i zasadami etyki działalności hakerskiej i cyberprzestępczości. W ostatnich latach odnotowano wyraźny wzrost przypadków ataków hakerskich, w tym także skutecznych ataków z wykorzystaniem złośliwego oprogramowania ransomware tj. blokującego zainfekowane komputery poprzez szyfrowanie dostępu do systemu operacyjnego lub do danych zawartych na dyskach zainfekowanego wirusem komputera. W niniejszym artykule opisano problematykę zasad bezpieczeństwa oraz zagrożeń wynikających z cyberataku hakerskiego jaki został przeprowadzony 27 czerwca z użyciem wirusa ransomware Petya. Kluczową kwestią w kontekście skali rozprzestrzeniania się złośliwego oprogramowania jest sprawna i szybka reakcja mediów, w których podawane komunikaty ostrzegają obywateli o pojawiających się zagrożeniach. Kwestia ta dotyczy także odnotowanego z końcem czerwca 2017 roku ataku hakerskiego złośliwego oprogramowania typu ransomware Petya, za pomocą którego cyberprzestępcy blokowali działanie komputerów w wielu instytucjach publicznych, finansowych oraz firmach. Początkowo ten cyberatak dotyczył głównie instytucji i podmiotów funkcjonujących na Ukrainie jednak w kolejnych godzinach rozprzestrzeniania się wirusa Petya infekcje komputerów odnotowywane były także w nieco mniejszej skali w kilku innych krajach w Europie, w tym także w Polsce. Opisany cyberatak potwierdził potrzebę permanentnego aktywizowania procesów doskonalenia systemów i procedur bezpieczeństwa transferu, przetwarzania i archiwizowania danych niejawnych w systemach informatycznych podłączonych do internetu.

Słowa kluczowe:
bezpieczeństwo cybernetyczne, bezpieczeństwo informatyczne, bezpieczeństwo systemów informatycznych, wirus Petya, ransomware, cyberbezpieczeństwo, cyberprzestrzeń, cyberatak, WannaCry, złośliwe oprogramowanie, szkodliwe oprogramowanie, bezpieczeństwo informacji, systemy bezpieczeństwa, procedury bezpieczeństwa, phishing, Microsoft Windows

Krzemińska Beata

1.5. Automatyczny System Identyfikacji Daktyloskopijnej w policyjnej „cyberpodprzestrzeni"

Streszczenie:
Cyberprzestrzeń to drugi świat, równoległy do rzeczywistego, w którym funkcjonuje obecnie społeczeństwo. Zadaniem Policji jest zapewnienie bezpieczeństwa i porządku publicznego oraz zwalczanie zagrożeń płynących z obu tych obszarów. Skuteczność jej działania zależy w dużej mierze od sprawnego funkcjonowania zwłaszcza w tej wirtualnej przestrzeni, gdzie gromadzi i przetwarza ona wszystkie potrzebne danych. Priorytetem staje się wyizolowanie dedykowanej cybersfery, określonej mianem policyjnej „cyberpodprzestrzeni" na potrzeby niniejszego opracowania, w której mogą bezpiecznie pracować wszystkie kluczowe systemy informatyczne funkcjonujące w Policji.
Jednym z takich systemów jest Automatyczny System Identyfikacji Daktyloskopijnej (AFIS). W artykule ukazano rozwój tego system od początku jego funkcjonowania oraz wpływ tych zmian na ewolucję policyjnej cyberpodprzestrzeni. Przedstawiono także podstawowe założenia przyjęte do budowy systemu i zasady postępowania z przetwarzanymi transakcjami. Zaprezentowane podejście obrazuje środki prewencyjne podejmowane przez Policję w kierunku ochrony przed cyberatakami, podsłuchem, zniekształceniem lub skopiowaniem danych, dając tym samym gwarancje integralności, wiarygodności i niezawodności przetwarzanych informacji.

Słowa kluczowe:
AFIS, bezpieczeństwo, Eurodac, Pruem, daktyloskopia, cyberprzestrzeń, cyberpodprzestrzeń.

Frankowski Gerard
Miłostan Maciej
Meyer Norbert
Nowocień Tomasz Adam
Konieczny Radosław

1.6. Outsourcing cyberbezpieczeństwa w świetle problematyki współczesnych zagrożeń w cyberprzestrzeni

Streszczenie:
Dynamiczny rozwój technologii komunikacyjnych powoduje, że korzysta z nich coraz większa liczba użytkowników nieukierunkowanych technicznie – przez co mogą łatwo stać się ofiarą ataku. Z kolei organizacje są intensywnie atakowane z uwagi na posiadane zasoby i dane. W artykule chcemy przedstawić wieloaspektowość problemu cyberbezpieczeństwa, dokonać próby ogólnego podziału zagrożeń i nakreślić podstawowy punkt startowy strategii ochronnej, uwzględniającej zarówno elementy techniczne, jak i proceduralne, a także zgodnej z zasadami ekonomii bezpieczeństwa. Przedstawiamy możliwość zastosowania modelu outsourcingowego w odniesieniu do cyberbezpieczeństwa oraz wskazujemy, jakie problemy organizacja (w szczególności działająca w sektorze publicznym) może dzięki takiemu modelowi rozwiązać. Jednocześnie prezentujemy doświadczenia naszej instytucji macierzystej – Poznańskiego Centrum Superkomputerowo-Sieciowego – w zakresie badań nad bezpieczeństwem IT realizowanych na rzecz sektora publicznego. Przedstawiamy także możliwości współpracy w zakresie tworzenia innowacyjnych rozwiązań cyberbezpieczeństwa oraz centrów zarządzania bezpieczeństwem (SOC), zgadzając się z autorami Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, że instytucje naukowe oraz jednostki badawcze – finansowane przecież ze środków publicznych – powinny odgrywać istotną rolę w tworzeniu oraz realizacji założeń maksymalnie gwarantujących wysoki poziom zabezpieczeń polskiej cyberprzestrzeni.

Słowa kluczowe:
Cyberbezpieczeństwo, cyberprzestrzeń, zagrożenia, Security Operations Center, SOC, ochrona w głąb.

Gwoździewicz Sylwia
Prokopowicz Dariusz

1.7. Determinanty rozwoju cyberprzestępczych ataków na systemy informatyczne firm i klientów indywidualnych instytucji finansowych

Streszczenie:
W związku z dynamicznym rozwojem technologii informatycznej i bankowości internetowej sukcesywnie wzrasta znaczenie bezpieczeństwa elektronicznego przesyłania i przetwarzania danych za pośrednictwem globalnej sieci internet. Z rozwojem technik udostępniania informacji poprzez internet wiąże się wiele udogodnień dla beneficjentów, klientów i osób korzystających z usług informacyjnych instytucji finansowych i innych podmiotów. Dynamiczny rozwój bankowości internetowej zdeterminowany jest wygodą możliwości zdalnego przeprowadzania transakcji finansowych przez klientów usług finansowych. Dla banków oraz innych instytucji finansowych oraz przedsiębiorstw, w tym także dla podmiotów udostępniających elektronicznie informacje poprzez internet pojawia się możliwość znaczącej redukcji kosztów transakcyjnych przeprowadzanych operacji finansowych oraz elektronicznego transferu danych. Z drugiej strony proces udostępniania informacji poprzez internet i rozwój bankowości elektronicznej generuje wiele zagrożeń związanych z przestępstwami kradzieży danych niejawnych, przechwytywania przez cyberprzestępców danych osobowych i informacji poufnych oraz dokonywania malwersacji środków pieniężnych w systemach internetowej bankowości. W odpowiedzi na te zagrożenia poszczególne podmioty w tym instytucje sektora finansowego, publicznego i przedsiębiorstwa rozbudowują systemy bezpieczeństwa zdalnego udostępniania informacji oraz dokonywanych transakcji realizowanych za pośrednictwem internetu. Pojawiają się także nowe rodzaje zagrożeń i cyberprzestępstw jak np. wzrost aktywności cyberprzestępców dokonujących ataki z wykorzystaniem programów ransomware i botnetów, dokonywane na dużą skalę kradzieże danych osobowych z kont portali informacyjnych i społecznościowych, włamania

do oprogramowania ATM w bankomatach oraz rozsyłanie spamu zawierającego różne wersje złośliwego oprogramowania w załącznikach. Cyberprzestępcy aby włamać się do systemów informatycznych innych podmiotów wykorzystują luki w zabezpieczeniach powstających nowych wersji produkowanego oprogramowania, aplikacji i systemów informatycznych funkcjonujących w bankach, przedsiębiorstwach i podmiotach sektora publicznego. Wobec narastających zagrożeń ataków hakerskich, w tym rozsyłania spamu zawierającego złośliwe oprogramowanie typu ransomware coraz więcej firm tworzy dodatkowe zabezpieczenia systemów informatycznych i stale udoskonala pod tym względem działające w firmie oprogramowanie i infrastrukturę informatyczną.

Słowa kluczowe:
cyberprzestępczość, cyberataki, prawo karne, bezpieczeństwo systemów informatycznych, złośliwe oprogramowanie, ransomware, Business Email Compromise, raporty dotyczące zagrożeń, luki w zabezpieczeniach, oprogramowanie ATM, Adobe Acrobat Reader, Microsoft Windows, bonet Mirai, bankowość internetowa.

Łazarski Daniel

1.8. System dozoru elektronicznego w Polsce

Streszczenie:
Wprowadzenie do polskiego porządku prawnego systemu dozoru elektronicznego stało się niejako konieczne ze względu na rosnące przeludnienie więzień i wysokie koszty wykonywania kar izolacyjnych. Kara pozbawienia wolności stanowi najsurowszą reakcję prawną na naruszenie porządku prawnego. Powinna być stosowana w ostateczności – gdy orzeczenie innej kary nie jest możliwe z uwagi na przewidywaną niską skuteczność w zapobieganiu powrotności do przestępstwa. Jest to zgodne z zaleceniami podmiotów międzynarodowych odnośnie pierwszeństwa kar wolnościowych. Możliwość odbywania kary pozbawienia wolności w systemie dozoru elektronicznego sprawia, iż brak jest niekorzystnych efektów społecznych wynikających z izolacji. Osoba odbywająca tę karę w warunkach wolnościowych pozostaje w kontakcie z osobami bliskimi i nie jest zmuszona do przerwy w nauce lub pracy. Ryzyko demoralizacji skazanych oraz degradacji ekonomicznej jest tutaj mniejsze, niż gdyby kara była wykonywana w warunkach izolacji więziennej. Z drugiej strony, zapewnienie bezpieczeństwa dla ogółu społeczeństwa zdaje się być w takim przypadku trudniejsze.

Słowa kluczowe:
dozór elektroniczny, przestępczość, więziennictwo, kara pozbawienia wolności.

Wolaniuk Leszek

1.9. Wybrane problemy bezpieczeństwa systemów do zdalnej automatycznej identyfikacji opartej na RFID

Streszczenie:
W ostatnich latach nastąpił wzrost liczby zastosowań systemów do automatycznej identyfikacji wykorzystujących technikę RFID. Wykorzystują one komunikację radiową do bezprzewodowego zasilania układów, które pełnią rolę etykiet identyfikacyjnych obiektów oraz zdalnego odczytywania zawartych w nich danych. Doświadczenia z wdrożeń tej technologii wykazały wiele problemów związanych z możliwością nieautoryzowanego przechwytywania sygnałów identyfikacyjnych, ich fałszowania lub blokowania a także nieautoryzowanego kopiowania. Dodatkowy problem, co wykazały doświadczenia, stanowi brak jednoznacznego określenia odległości i warunków pracy układów techniki RFID. Nieznajomość prawidłowych wartości tych parametrów może znacząco przyczynić się do obniżenia poziomu bezpieczeństwa systemów wykorzystujących te układy.

Słowa kluczowe:
Systemy zdalnej automatycznej identyfikacji, RFID, bezpieczeństwo RFID.

Sztumski Janusz

2.1. Kilka uwag na temat koncepcji cyberprzestrzeni

Streszczenie:
Celem artykułu jest ukazanie procesu kształtowania się koncepcji cyberprzestrzeni oraz jej elementów składowych. Podjęto w nim również próbę prezentacji funkcjonowania Internetu jako istotnego czynnika w postępującej globalizacji współczesnego świata oraz uwarunkowań pojawienia się przestępczości popełnianej przez rozmaitych hakerów.
Wskazano w nim także na pewne trudności, które uniemożliwiają pojawienie się solidarności wszystkich państw w walce ze wspomnianą przestępczością popełnianą w sferze politycznej i militarnej. Wynikają one m.in. z dwoistej oceny działalności ofensywnej i defensywnej stosowanej w tej walce przez poszczególne państwa.

Słowa kluczowe: cyberprzestrzeń, przestrzeń, internet, komputer.

Tomaszycki Krzysztof

2.2. Proces migracji - realne czy wirtualne zagrożenie?

Streszczenie:
Przesiedlenia, migracja ekonomiczna czy też uchodźctwo, to w dobie informatyzacji zagadnienia, które przybierają zupełnie inny wymiar. Odchodzimy od realnego spostrzegania codzienności i wchodzimy w cyberprzestrzeń, w świat który daje inne wrażenia naszym zmysłom. Uzyskiwanie informacji o życiu codziennym, o warunkach przemieszczania się nie stanowi dziś wielkiego problemu. Nie wychodząc z domu jesteśmy w stanie poprzez informacje zawarte w intrenecie zaplanować ze szczegółami plan naszych podróży. Taki plan możemy sami ułożyć lub może być nam przedstawiony przez inne osoby. Migranci lub uchodźcy niejednokrotnie wykorzystują takie „ułożone plany podróży". Otrzymując takie informacje, stosując je w swoim postępowaniu stają się „ofiarami" zorganizowanych grup przestępczy, które bazują na naiwności tych ludzi. Czy w takim ujęciu proces migracji ma wymiar realny czy też wirtualny i jaki wymiar mają zagrożenia?

Słowa kluczowe:
migracja, uchodźctwo, zagrożenia, ochrona uchodźców, rzeczywistość realna, wirtualne zagrożenia

Nosov Vitalii
Rvachov Oleksii
Chernovol Valeriia

2.3. Szkolenie policjantów w aspekcie zastosowania kryminalistyki cyfrowej w dochodzeniu cyberprzestępstw

Streszczenie:
Na podstawie kierunku i zadań jednostek Cyberpolicji Ukrainy, aktualnej międzynarodowej naukowej, metodycznej i narzędziowej podstawy kryminalistyki cyfrowej określono treść i zakres specjalnych szkoleń dla policjantów w aspekcie zastosowania jej w dochodzeniu cyberprzestępstw. Na podstawie wyników praktycznego współdziałania z jednostkami policji zaproponowano uogólnienie metody poszukiwania cyfrowych śladów zaginionych dzieci.

Słowa kluczowe:
szkolenie policji, kryminalistyka cyfrowa, metoda poszukiwania cyfrowych śladów.

Kordaczuk – Wąs Marzena

2.4. Propaganda i świadomość w procesie radykalizacji - wzmacnianie i osłabianie czynników ryzyka w cyberprzestrzeni.

Streszczenie:
Aktualne procesy migracyjne, szczególnie zaś te związane z opuszczaniem przez jednostki społeczne terenów zdezintegrowanych politycznie czy też dotkniętych konfliktami, wymuszają na krajach europejskich podejmowanie działań zarówno zaspokajających podstawowe potrzeby migrujących osób, jak też zapobiegających rzeczywistym i potencjalnym zagrożeniom bezpieczeństwa wynikających ze wspomnianych wędrówek ludności. Wśród owych zagrożeń, obok tych związanych ze stanem zdrowia czy bezpieczeństwem socjalnym migrantów, szczególną uwagę zwraca konieczność zapobiegania zagrożeniom bezpieczeństwa wewnętrznego poszczególnych państw. I nie to nie tylko z perspektywy tzw. przestępczości pospolitej, ale również procesów związanych z nasilaniem się zachowań mogących prowadzić do radykalizacji zachowań zarówno samych migrantów, jak też Europejczyków. Działania te nabierają szczególnego znaczenia w obliczu udanych i nieudanych prób ataków terrorystycznych odnotowywanych w kolejnych europejskich krajach, które przekładają się na obniżanie poziomu poczucia bezpieczeństwa obywateli i nasilanie się niechęci wobec „przybyszów". Dlatego dostosowywanie środków prewencyjnych do diagnozowanych zagrożeń i jednostkowych potrzeb związanych z migracjami staje się priorytetem, a zarazem wyzwaniem dla podmiotów odpowiedzialnych za ich podejmowanie. Bezdyskusyjny wpływ na kształtowanie się, upowszechnianie i eskalację wspomnianych radyklanych zachowań może mieć wpływ wiele aktywności wzmacniających czynniki ryzyka diagnozowane w poszczególnych społecznościach i uwzględniane w systemach wczesnego ostrzegania. Jednakże w dobie cyfryzacji życia społecznego szczególnej uwagi wymaga bez wątpienia cyberprzestrzeń. Jej nieograniczony zasięg oraz powszechny dostęp do zasobów Sieci zwiększa bowiem możliwość upowszechniania treści o zabarwieniu radykalnym i wzmacniania zachowań o podłożu dyskryminacyjnym, co z kolei może prowadzić do zachowań

przestępnych. Dlatego tak ważną rolę w zapobieganiu radykalizacji, obok monitorowania treści zawartych w internecie, pełni również wykorzystanie potencjału zasobów internetowych w celu podnoszenia świadomości społecznej związanej z kształtowaniem bezpiecznych stosunków społecznych w dobie wzmożonych ruchów migracyjnych.

Słowa kluczowe:
Migracje, imigranci, uchodźcy, radykalizacja, internet, czynniki ryzyka, zagrożenia bezpieczeństwa, bezpieczeństwo wewnętrzne.

Krupa Monika

2.5. Patologia cyfrowego dzieciństwa

Streszczenie:
W nowym społeczeństwie wiedzy nikt już nie kwestionuje współczesnych przemian, jakie pojawiają się w cyberprzestrzeni i ich wpływu na kształtowanie oraz twórcze rozwijanie osobowości człowieka. Następujące przemiany cywilizacyjno – informatyczne, zwłaszcza w zakresie nowych funkcji mediów cyfrowych i technologii informacyjno – komunikacyjnych oraz wynikające z nich możliwości, pozwalają na realizację wielu zadań istotnych nie tylko dla edukacji ale także rozwiązywania prawnych i społecznych przemian, które mogą tworzyć problemy pojawiające się w cyberprzestrzeni.
Powszechnie uważa się, że wpływ mediów masowych nie jest niczym innym niż rodzajem oszustwa. Jako odbiorcy świadomi jesteśmy pozytywnych aspektów oddziaływania komunikacji medialnej na kształt i jakość życia współczesnego człowieka. Szybkość wymiany informacji, łatwość dostępu do nich, wspomaganie procesów edukacji i. t. p. Jednak mówiąc o oddziaływaniu mediów, używa się zwykle sformułowań w rodzaju: manipulacja, dominacja, władza, uprzedmiotowienie, kontrola społeczna – zwykle w pejoratywnym zakresie ich znaczeń. Niniejsze opracowanie nie ma na celu zaprzeczyć temu, co oczywiste na poziomie wiedzy powszechnej. W pewien sposób tekst ten próbuje uporządkować zakres zjawisk wpływu mediów, przenosząc jednakże problem tego zjawiska z obszaru mediów na jednostkę, czy raczej osobę wystawioną na ich wpływ.
Konsekwencje społeczne braków edukacji z zakresu komunikacji medialnej mogą być istotnie zaskakujące, zaś skutki zachodzących procesów praktycznie nieodwracalne, czego jaskrawym przykładem jest postępująca od końca XX wieku tabloidyzacja.
Psychologia internetu (Wallace 2001, s. 16), to nowa dziedzina dotycząca komunikowania się ludzi w cyberprzestrzeni. Od kilkunastu lat jesteśmy zależni, albo niektórzy nawet uzależnieni od internetu. Oprócz bezspornych korzyści dotyczących komunikowania się w cyberprzestrzeni dzieci i młodzieży (Turkle

2013, s. 6.), a także dorosłych występują jednak, i to często, bardzo poważne zagrożenia dla ich aktualnego oraz przyszłego rozwoju psychicznego i społecznego, a także rozwoju moralnego.
Życie społeczne, którego jedną z nadrzędnych wartości stało się istnieć w znaczeniu „być postrzeganym", nie daje zbyt wielu możliwości uniezależnienia się od wpływu mediów. Aby uniknąć wykluczenia ze sfery komunikacji masowej, jedyną drogą obrony jest samoregulacja i samokontrola środowisk dziennikarskich, prawo stanowione przez państwo oraz najistotniejsza w sferze wszelkich form porozumiewania się: kompetencja komunikacyjna. Niniejszy tekst tratuje przede wszystkim o znaczeniu i jakości kompetencji, ukazanej przez prezentacje najistotniejszych społecznych oraz prawnych środków wpływu wraz z ich potencjalnymi skutkami.

Słowa kluczowe:
cyberprzestrzeń, komunikacja medialna, społeczne środki wpływu mediów, prawne środki wpływu mediów, wpływ mediów na jednostkę.

Jureczka Marlena

2.6. Cyberprzestrzeń – miejsce spotkań migrantów i rodzin globalnych

Streszczenie:
W dobie coraz większych możliwości technologicznych i wolności społecznej, we współczesnym świecie pojawiają się coraz to nowsze zagrożenia XXI wieku – zamachy terrorystyczne, konflikty zbrojne, przestępczość, wyłudzenia, hackerstwo czy też rozłamy uporządkowanego świata rodzinnego. Już od najdawniejszych czasów, każda człowiek walczył o utrzymanie swoistego ładu i poczucia bezpieczeństwa swojego, jak i swoich najbliższych. W czasach, gdzie przekroczenie granicy terytorialnej stało się wyjątkowo proste, zaczyna się pojawiać nowy model rodziny, jakimi są rodziny globalne czy rodziny na odległość. Od momentu wejścia Polski do Unii Europejskiej można zaobserwować zjawisko emigracji – często zarobkowej, ale też emigracji naukowej czy związanej z poszukiwaniem miłości. W takich warunkach, jedyna możliwością kontaktu z rodziną, która często bywa oddalona o tysiące kilometrów jest cyberprzestrzeń. Zdominowany świat przez Facebook, WhatsApp, Skype czy wiele innych aplikacji stają się nowym domem, wygodnym dostępem do porzuconego świata, dostępnym w wygodnych godzinach, w wybranych dniach tygodnia. W takiej rzeczywistości bardzo łatwo stać się kimś obcym, dla rodziny, jak i dla siebie samego. Wiele rodzin staje się rodziną internetową, kończą się relacje ludzkie, a zaczyna się impuls puszczony w sieć cyberprzestrzeni, który może nigdy już nie wrócić. Celem niniejszego opracowania jest ukazanie i zestawienie dwóch zjawisk, które wzajemnie się przenikają na płaszczyźnie świata społecznego – wykorzystywanie cyberprzestrzeni do budowania pewnego rodzaju imitacji życia społecznego i migracja ludzi, którzy decydują się na życie z dala od swoich rodzin i przyjaciół.

Słowa kluczowe:
cyberprzestrzeń, migracja, bezpieczeństwo, rodziny globalne, procesy globalne, społeczeństwo ryzyka, kapitał społeczny.

Błażejczak Karina
Tomaszycki Krzysztof

2.7. „Papierowe małżeństwo" jako efekt kontaktów w cyberprzestrzeni

Streszczenie:
Wraz z wejściem Polski do Unii Europejskiej dla cudzoziemców z krajów trzecich atrakcyjny stał się pobyt w Polsce. Polska pozostaje krajem tranzytowym do „lepszego świata". Atrakcyjny jest pobyt na terenie Unii Europejskiej, korzystanie z prawa do swobodnego przemieszczenia się po całej strefie Schengen i korzystanie z zaopatrzenia socjalnego bogatych państw Unii Europejskiej. Jednym z najskuteczniejszych sposobów osiągnięcia tego celu jest stanie się członkiem rodziny obywatela jednego z krajów członkowskich. W tym właśnie celu zawierane są „papierowe małżeństwa". W ten sposób obywatel kraju trzeciego nie tylko stara się polepszyć swoje warunki bytowe, lecz także uniknąć konsekwencji nielegalnego pobytu na terenie Unii Europejskiej czy anulować procedury wydaleniowe.

Do zawierania znajomości i utrzymywania kontaktu z „przyszłą rodziną" najczęściej wykorzystywany jest internet i wszelkiego rodzaju komunikatory czy portale społecznościowe.

Takie spłycone, instrumentalne podejście do podstawowej komórki społecznej niesie za sobą poważne, pozytywne i negatywne, konsekwencje społeczne, kulturowe i polityczne. Jedną z nich może być również zagrożenie bezpieczeństwa społecznego państwa..

Słowa kluczowe:
fałszywe małżeństwo, legalizacja pobytu, bezpieczeństwo, internet, migracja, zagrożenia, kultura.

Popov Georgii
Amelin Oleksander

2.8. Typowe zagadnienia dochodzeniowe związane z cyberprzestępczością na Ukrainie.

Streszczenie:
Poniższy artykuł traktuje o braku stałego pojęcia „dowodu elektronicznego", który to prowadzi do szeregu problemów podczas zbierania dowodów, ich sprawdzania oraz ewaluacji. Ma na celu wyspecyfikowanie warunków, które mają znaczenie dla czynności kryminalnych. Analiza statystyki wskazuje na to, iż na Ukrainie dynamika przestępczości z wykorzystaniem urządzeń elektronicznych (w szczególności komputerów), różnorakich systemów automatycznych czy sieci telekomunikacyjnych, nie jest stała.
Problemy na tej płaszczyźnie mogą być rozwiązane przez: ukonstytuowanie definicji stałego pojęcia „dowodu elektronicznego" w oddzielnym paragrafie czwartego rozdziału Procedur Kryminalnych na Ukrainie (Dowody); implementacja oddzielnego aktu legislacyjnego, gdzie zebrane byłyby wszelkie pojęcia związane z szeroko pojętą „informacją" (dowód elektroniczny, cyberprzestrzeń, cyberbezpieczeństwo, cyberobrona, cyberatak, cyberterroryzm), wprowadzenie specjalnych kursów treningowych dla śledczych, prokuratorów i sędziów.

Słowa kluczowe:
dochodzenie w śledztwie, cyberzbrodnia, złośliwe oprogramowanie, cyberzagrożenia.

4. Abstract and keywords:

Garwol Katarzyna

1.1. Privacy on the Web in terms of legal regulations and research analyzes

Abstract:
Privacy is a value which seems to be important to every person. In today's world when digital media especially the internet play a vital role, privacy is changing its meaning. On the one hand technology causes that we are constantly pictured and located, but on the other hand people often share their lives on the internet and exceed the limits not only of their confidentiality but also of their intimacy. This article describes how the privacy is defined by investigators of this phenomena, what are the legal norms relating to the privacy protection and outlines recent researches of the privacy of the internet users.

Keywords:
privacy, internet, security, social media.

Prokopowicz Dariusz

1.2. Development of malware ransomware as a new dimension of cybercrime taking control of enterprise and banking systems

Abstract:
This article describes the issue of the strong growth in online activity of ransomware malware in 2016, by which cybercriminals block a computer, smartphone, or other device connected to a global network. An infected computer or other cyberattack victim device equipped with a microprocessor and the internet displays a message asking for a ransom payment to restore the infected device to work properly. In the face of growing threats of hacker attacks, including the spread of malware containing ransomware malware, more and more companies and banks create additional IT security and continually improve the software and IT infrastructure used in their operations. It is now prevailing that this process will never end, at least as long as technological progress is taking place, as new applications and web platforms are emerging, new versions of operating systems and IT infrastructure commonly used by users. Every imperfection of information systems, teleinformatic networks, internal security procedures is quickly detected and used by cybercriminals. So far, there has been a pattern of fixing vulnerabilities previously detected by hackers. Considering the strong increase in the activity of dangerous ransomware programs, this model should be changed to reverse the order of operations. Employees in companies, banks, and public IT organizations should anticipate cybercriminals as early as possible to detect vulnerabilities. As a result, the need for preventive, proactive prevention in the process of improving the risk management processes of information systems operating in financial institutions, enterprises and public sector entities is increasing.

Keywords:
Computer security, malware, ransomware, Business Email Compromise, cybercrime, cyberattack, internet, security reports, security vulnerabilities, banking services security, information security, security systems, internet banking

Orzechowska Anna
Gugulski Marcin

1.3. The development of cyberspace security threat databases.

Abstract:
The progressive development of the information society, combined with the improvement and dissemination of information and telecommunications solutions, transposes the facets of human activity from the real world into cyberspace, a virtual area created within and within the reach of IT and telecommunications. More and more people are not imagining their day to day operation without the use of cyberspace: a variety of portals, e-mail, instant messaging, digital libraries, universal wireless and virtual money. Unfortunately, cyberspaces have also infiltrated negative phenomena typical of the real world. All the qualities that have resulted in the emergence of new qualities in communication, commerce, or service have also become a factor in creating new opportunities for hooligans, thieves, terrorists and spies. The sense of anonymity, the lack of geographical boundaries, the ease of concealing and encrypting the content, the enormous speed of technical changes that make use of human errors and mistakes resulting from it, make the threats on this side more and more serious. The purpose of this article is to present the dangers of using the latest technology.

Keywords:
information, cyberspace, threat, law.

Prokopowicz Dariusz
Gwoździewicz Sylwia

1.4. An analysis of the security of information systems protection in the context of the global cyberatomy ransomware conducted on June 27, 2017

Abstract:
The intensive development of information technology and data transmission since the end of the last century has also been used to violate the laws and ethics of hacking and cybercrime. In recent years there has been a noticeable increase in hacker attacks, including successful attacks using ransomware malware, ie, blocking infected computers by encrypting access to the operating system or data contained on disks infected with a computer virus. This article describes the security issues and the risks of hacker cyber attacks that were conducted on June 27 with the Petya ransomware virus. The key issue in the context of the scale of malware spread is the efficient and rapid reaction of the media, in which messages are alerting citizens of emerging threats. This issue also applies to the Petya ransomware hacking attack by late June 2017, by which cybercriminals block the operation of computers in many public and financial institutions and businesses. Initially, this cyberatak was mainly about institutions and entities operating in Ukraine, but in the subsequent hours of the spread of the Petya virus, computer infections were also reported on a slightly smaller scale in several other European countries, including Poland. The described cyberatak confirmed the need to permanently activate the processes of system improvement and security procedures for the transfer, processing and archiving of classified data in internet-connected IT systems.

Keywords:
Cyber security, IT security, IT security, Petya virus, ransomware, cyber security, cyberspace, cyberattack, WannaCry, malware, malware, information security, security systems, security procedures, phishing, Microsoft Windows

Krzemińska Beata

1.5. Automated Fingerprint Identification System in police 'cybersubspace'

Abstract:
Cyberspace is the second world, parallel to real, in which the current society is functioning. However, there are different threats coming from both areas which constitute the main task for the Police to fight with, especially for the purpose of a safety assurance and public order. Police effectiveness depends of the smooth functioning, in this virtual space, where the needed information is collecting and processing. The main priority becomes to isolate the dedicated cybersphere, named as police 'cybersubspace' for the purposes of this study, in which all crucial information systems in the Police can work safely.
Automated Fingerprint Identification System (AFIS) is one of these kind of the applications. In the following paper the extension of the AFIS system, as well as the influence to the evolution of the police 'cybersubspace' have been presented. For instance, the fundamental assumptions of the system's design and the principles of data processing have been expressed. Moreover, all necessary procedures to prevent the cyberattacks, the listening, distorting and copying of data have been described. This behavior gave us the guarantee to the integrity, credibility and reliability of the processed information.

Keywords:
AFIS, security, Eurodac, Pruem, fingerprint, cyberspace, cybersubspace.

Frankowski Gerard
Miłostan Maciej
Meyer Norbert
Nowocień Tomasz Adam
Konieczny Radosław

1.6. Cybersecurity outsourcing in the context of contemporary cyberspace threat

Abstract:
Dynamic development of ICT systems causes rise of the number of users not technically oriented – which makes them relatively easier victims of attacks. On the other hand, organizations are attacked due to the value of their assets. In this paper we aim at introducing multiple facets of cybersecurity as well as to generally classify threats against system and against users and draw a starting point of the protection strategy. Such a strategy must be conformant with security economy principles and cover both technical and organizational points of view. We describe how to refer outsourcing to cybersecurity and point which problems of public sector organizations might be solved that way.
In parallel, we describe experience of our home institution – Poznań Supercomputing and Networking Center – concerning cybersecurity research led for the public sector purposes. We emphasize the opportunities of cooperation oriented towards development of innovative solutions for cybersecurity as well as Security Operations Center, following the authors of Cybersecurity Strategy for the years 2017-2022 in that research institutions – maintained also by public founds – should play an active role in shaping and realizing assumptions guaranteeing cybersecurity to the maximum available extent.

Keywords:
Cybersecurity, cyberspace, threats, Security Operations Center, SOC, defence-in-depth.

Gwoździewicz Sylwia
Prokopowicz Dariusz

1.7. Determinants of the development of cyber-attacks on IT systems of companies and individuals of financial institutions

Abstract:
Due to the dynamic development of information technology and internet banking, the importance of secure electronic transmission and processing of data through the global internet has gradually increased. With the development of information-sharing techniques through the internet, there are many facilities for beneficiaries, customers and users of information services of financial institutions and other entities. The dynamic development of internet banking is determined by the convenience of the ability to remotely conduct financial transactions by financial services clients. For banks and other financial institutions and enterprises, including those providing electronic information via the internet, there is the possibility of significant reduction of transaction costs of financial operations and electronic data transfer. On the other hand, the process of making information available via the internet and the development of e-banking generates many threats related to the crime of theft of classified data, the interception of confidential information by cybercriminals, and the scams of money in online banking systems. In response to these threats, individual entities including financial institutions, the public and the business sector expand security systems for remote access to information and transactions made via the internet. New types of cybercrime and cybercrime are emerging, including cybercriminals attacking ransomware and botnets, large-scale theft of personal information from social and information portals, hacking ATM software at ATMs, and spamming with various versions of malware. Software in attachments. Cybercriminals use vulnerabilities in emerging software releases, applications and IT systems in banks, businesses, and public sector to break into third party IT systems. With the increasing threat of hacker attacks, including the spread of malware containing ransomware malware, more and more companies

are making additional IT security and constantly improving the software and IT infrastructure of the company.

Keywords:
cybercrime, cyber attacks, criminal law, security of informatics systems, threat reports, vulnerabilities, ATM software, Adobe Acrobat Reader, Microsoft Windows, Mirai bonnet, online banking.

Łazarski Daniel

1.8. Electronic surveillance system in Poland

Abstract:
Introduction to polish legal electronic surveillance system it has become necessary due to rising overpopulation in prisons and high costs of execution disciplinary sanction. Sentence of imprisonment is the most severe legal response for violation of the legal order. It should be used in the last resort when the judgment of another penalty is not possible because of the expected low effectiveness in prevention of return to crime. It is in accordance with the recommendation of the international entities as regards priority penalties libertarian. The possibility of serving a prison sentence in the electronic surveillance system makes the lack of adverse social effects resulting from the isolation. The person that takes this punishment in libertarian conditions keeps in touch with family, relatives, friends and is not forced to take a break in work or studying. The risk of demoralizing the convicts and economic degradation is much smaller here, then if the punishment would be carried out in the conditions of prison isolation. On the other hand, to ensure security for the general public seems to be in this case more difficult.

Keywords:
electronic surveillance, criminality, penology, imprisonment.

Wolaniuk Leszek

1.9. Some security issues of RFID Remote Automatic Identification Systems

Abstract:
In recent years a growing number of applications systems for automatic identification based on RFID is observed. They use radio-communication to wirelessly supply power to system's components that act as identification labels and remotely read their identification data embedded in the labels. Experience drawn from many implementations of RFID technology indicates a lot of problems related to unauthorized capturing identification signals, blocking or counterfeiting, copying identification data. Additionally many experiments have shown the lack of precise information about the proper distance and necessary conditions for correct applying of RFID systems. Ignorance concerning proper values of these parameters could significantly reduce information security level of the system with RFID modules.

Keywords:
Automatic remote identification systems, RFID, RFID Security.

Sztumski Janusz

2.1. Couple issues about the conception of cyberspace

Abstract:
The goal of this article is to show the process of shaping of the conception of cyberspace and its elements. Also, there has been taken the effort of presentation of functioning of the Internet as a important factor of progressive globalization. Also, this article is to show the conditions of criminality committed by hackers.
Apart from that, the article shows different kinds of difficulties which unable the solidarity of all countries with counteraction of mentioned political and military criminality . They ensue from double evaluation of offensive and defensive activities performed by those countries.

Keywords:
Cyberspace, space, Internet, computer.

Tomaszycki Krzysztof

2.2. The proces of migration – real or virtual threat?

Abstract:
Resettlements, economical migration or emigration in the era of informatization are issues which get completely different dimension. We tend to quit from reality and come into cyberspace, which gives us senses different impressions. Gathering information about everyday life, about the conditions of migration, does not make a problem nowadays. Without leaving home, with the help of an Internet, we are able to plan our journeys with details. This plan can be figured out by ourselves or can be given to us by somebody else. Emigrants and refugees use those „prepared plans" very often. Being given those information, using it, they become victims of organized criminal groups, which base on naivete of those people. So, is the migration process real or virtual and what is the dimension of threats?

Keywords:
Migration, threats, protection of refugees, reality, virtual threats

Nosov Vitalii
Rvachov Oleksii
Chernovol Valeriia

2.3. Police training in the context of application of digital forensic in cybercrime investigations

Abstract:
The directions and tasks of the cyber policy units of Ukraine, the actual international scientific, methodical and instrumental base of digital forensics are analyzed. Special police training courses have been proposed and tested in the context of the use of digital forensics in investigations of cybercrime. A generalized methodology for searching digital traces of missing children is proposed, which is based on the results of practical interaction with the police units.

Keywords:
special police training, digital forensics, methodology for searching digital traces.

Kordaczuk – Wąs Marzena

2.4. Propaganda and consciousness in the process of radicalization - Strengthening and mitigating risk factors in cyberspace

Abstract:
Current migration processes, particularly those related to the departure of socially or politically disintegrated areas, force European countries to act to meet the basic needs of migrants as well as to prevent real and potential security threats resulting from these migrations. Among these threats, in addition to those related to the health or social security of migrants, particular attention is paid to the need to prevent threats to internal security in individual countries. And not only from the perspective of so-called common crime, but also processes related to the intensification of behavior that can lead to radicalization of behavior both migrants themselves and European citizens. These actions are gaining in importance due to successful and unsuccessful terrorist attacks which are increasingly common in European countries. Because they have the effect of reducing the level of citizens' sense of security and increasing the unwillingness of 'newcomers'. Due to it adapting preventive measures to diagnosed threats and individual needs related to migration becomes a priority and a challenge for entities responsible for organizing them. Undoubtedly, the impact on the development, spreading and escalation of mentioned radical behaviors can be influenced by many of the risk-enhancing activities (risk factors) that are being diagnosed in different communities and taken into account in early warning systems. However, in the age of digitizing social life, cyberspace requires special attention. Its unlimited operating reach and widespread access to the resources of the Network increases the possibility of disseminating radical content and strengthening discriminatory behavior which can lead to criminal acts. Therefore, an important role in the prevention of radicalization, in addition to monitoring the content of the Internet, has also use of the online resources potential that can raise public awareness related to the development of safe social relationships in times of increased migration.

Keywords:
Migrations, immigrants, refugees, radicalization, Internet, risk factors, security threats, internal security.

Krupa Monika

2.5. Digital childhood pathology

Abstract:
In the new knowledge society no one questions the present transformations which are appearing in cyberspace as well as their influence on shaping and creative development of human personality. Following civilization and IT transformation, especially in function range of new digital media, information and communication technologies and resulting from them opportunities permitting to realize many tasks which are cruicial for education and solving legal and social changes which could create problems in cyberspace.
It's commonly believed, that mass media impact is nothing but a kind of deception. As recipients we are aware of the positive aspects of media communication on form and quality of contemporary man's life. The speed of information exchange, the ease of access to them, support for educational process e.t.c. However talking about the impact of the media, usually used wording is: manipulation, domination, power, objectification, social control- usually in their pejorative meanings. This text is not intended to deny what is obvious at the level of universal knowledge. In a way, this text tries to sort out the range of media influences by moving the issue of the media from the media to the individual or rather to the person exposed to them.
The social consequences of lack of education in the field of media communication can be surprisingly significant and the effects of ongoing processes practically irreversible as evidenced by the progressive tabloidization that has been taking place since the late twentieth century.
internet psychology (Wallace 2001, s. 16) is a new field concerning communication between people in cyberspace. For dozen years we are dependent or addicted to the internet. Apart from the undisputed benefits of communicating in cyberspace to children and adolescents as well as adults often have very serious threats to their current and future mental, social and moral development. Social life where "exist" in the sense of "being perceived" has become one of the overriding values doesn't give too many opportunities to become independent

from the influence of the media. The only way to avoid exclusion from mass communication is self-regulation and self-control among journalists, law made by the state and most import ant in the sphere of all forms of communication: communication competence. This text deals primarily with the import_ance and the quality of the competencies shown by presentation of the most import_ant social and legal means of influence, together with their potential effects.

Keywords:
cyberspace, media communication, social means of media impact, legal means of media impact, impact of media on the individual.

Jureczka Marlena

2.6. Cyberspace: a meeting place for migrants and global families

Abstract:
In the era of a growing number of technological possibilities and increasing social freedom, the modern world is much exposed to a multitude of threats – terrorist attacks, armed conflicts, crime, extortion, hacking or breaks in family relations. Since the earliest times, people have struggled to maintain a certain order and sense of security for them and their families. In times when crossing territorial borders has become especially simple, there occurs a new family model, namely, a global family and long-distance family. Since Poland's accession to the European Union, there has been the phenomenon of emigration observed, and it is often an economic one, but it can be also related to scientific endeavours and searching for love. The only possible meeting place for a family in these conditions of thousands of kilometers distance is cyberspace. Facebook, WhatsApp, Skype and many other applications that have dominated the world are becoming a new home, an easy access to the once abandoned world used at one's convenience. In this reality, it is very easy to grow strange both to one's family and to oneself. Many families have become online families experiencing vanishing human relations with only an impulse sent to the network that may never be sent back. The essay juxtaposes two phenomena interlacing within the area of social life – using cyberspace to build a certain imitation of social life and migration of people who decide to live far from their families and friends.

Keywords:
cyberspace, security, global families, global processes, risk society, social capital.

Błażejczak Karina
Tomaszycki Krzysztof

2.7. „Paper marriage" as a result of contacts in cyberspace

Abstract:
Upon Poland's accession to the European Union, the stay in Poland became attractive to foreign nationals from third countries. Not literally, though. Poland remains a country of transit to a "better world". It is a stay within the territory of the European Union that is attractive, exercising the right of freedom of movement throughout the Schengen zone and the use of social welfare of the rich states of the European Union. One of the most effective ways of achieving this objective is to become a member of the family of a citizen of one of the Member States. "Paper marriage" are concluded for this very purpose. This way, a third country national not only seeks to improve their living conditions, but also to avoid the consequences of illegal stay on the territory of the European Union or cancel the extradition procedures.
To make acquaintances and to keep in contact with the "future family", internet is used the most often, as well as all kinds of instant messaging systems or social media.
Such shallow, instrumental approach to the fundamental social unit carries serious, positive and negative, social, cultural, and political consequences. One of them can also be a threat to the state security and the public order.

Keywords:
false marriage, legalization of residence, safety, internet, migration, threats, culture.

Popov Georgii
Amelin Oleksander

2.8. Topical issues on investigation of crimes connected with cybercrime in Ukraine

Abstract:
The article deals with the fact that the absence of fixed notion "electronic evidence" leads to a number of problems during collection, check and evaluation of evidence with the aim to define the conditions that have a meaning for the criminal proceedings. Analysis of the statistics indicates that in our country the dynamics of crime in the use of electronic computers (PCs), automated systems, computer or telecommunication networks is unstable.
Problems in this sphere could be solved by: placement of definition of the notion "electronic evidence" in a separate paragraph of Chapter 4 Criminal Procedure Code of Ukraine (Evidence and Proof); adoption of separate legal and regulatory act where all the notions connected with the information relationships would be defined ("electronic evidence", "cyberspace", "cybersafety", "cyberdefense", "cyberattack", "cyberterrorism"); introduction of training courses for investigators, prosecutors and judges.

Keywords:
investigation of crimes, cybercrime, malware, cyberthreads.

Bibliografia:

1. ABDEL-AZIZ A., ESLER J., 2009. *Intrusion Detection & Response. Leveraging Next Generation Firewall Technology*, SANS Institute, https://www.sans.org/reading-room/whitepapers/firewalls/intrusion-detection-response-leveraging-generation-firewall-technology-33053.
2. ABOUJAOUDE E., 2012. *Wirtualna osobowość naszych czasów. Mroczna strona e-osobowości*, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków.
3. ALI MIRI, 2013. *Advanced Security and Privacy for RFID Technologies*, IGI Global, USA.
4. Appendix 1. *Report on criminal offenses for the period of 2010 - 2016.*
5. ARTHUR C., 2013. *Internet slows down after DNS attack on Spamhaus*, artykuł internetowy, The Guardian, https://www.theguardian.com/technology/2013/mar/27/cyber-attack-spamhaus-slows-down-internet.
6. *Ataki złośliwego oprogramowania Petya*, 2017 *[w:]* Portal internetowy „CryptoNews.Pl", 28.06.2017, (https://cryptonews.pl/ataki-zlosliwego-oprogramowania-petya).
7. BAKKER E., DE LEEDE S., 2015. *European Female Jihadists in Syria: Exploring an Under-Researched Topic*, ICCT Background Note.
8. BALLEY M., 2016. *The Latest in Phishing: First of 2016*, artykuł internetowy, Wombatsecurity.com, https://info.wombatsecurity.com/blog/the-latest-in-phishing-first-of-2016.
9. BARAN L., MISIEWICZ M., 2014. *Cyberprzestrzeń – nowe miejsce spotkań. Teoretyczna i psychologiczna analiza wirtualnych społeczności,* (red.) WYSOCKA – PLECZYK M,. TUCHOLSKA K., *Człowiek zalogowany 2. Wirtualne społeczności,* Wydawnictwo Biblioteka Jagiellońska, Kraków.
10. BAUMAN Z., 1996. *Socjologia*, w przekładzie ŁOZIŃSKI J., ZYSK i S-KA Wydawnictwo, Poznań.
11. BAUMAN Z., 2016, *Obcy u naszych drzwi*, Wydawnictwo Naukowe PWN, Warszawa.

12. BECK U., 2002. *Społeczeństwo ryzyka. W drodze do innej nowoczesności*, Wydawnictwo Naukowe SCHOLAR, Warszawa.
13. BECK U., BECK – GERNSHEIM E., 2013. *Miłość na odległość. Modele życia w epoce globalnej*, Wydawnictwo Naukowe PWN, Warszawa.
14. BEDNAREK J., 2005. *Patologie społeczne. Zagrożenia w cyberprzestrzeni,* Wyższa Szkoła Humanistyczna, Pułtusk.
15. BEDNAREK S., OMELANIUK A.T., TYSZKA A., ZIELIŃSKI A., 2002. *DTSK*, Silesia, Wrocław-Warszawa.
16. BEETS G., WILLEKENS F., 2009. *The global economic crisis and international migration: An uncertain outlook,* Vienna Yearbook of Population Research.
17. BENDYK E., 2016. *Witajcie w antropocenie!,* (w:) Polityka nr 37, z dnia 7-13. IX 2016.
18. BERGER P., 1997. *Zaproszenie do socjologii*, Stawiński J. (tłum.), PWN, Warszawa.
19. BERSON I.R., BERSON, J., eds., 2010. *High-tech tots: Childhood in a digital world*, IAP.
20. BHATT S., MANADHATA P.K., ZOMLOT L., 2014. *The Operational Role of Security Information and Event Management Systems,* IEEE Security & Privacy, 12 (October).
21. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*. 2013. Biuro Bezpieczeństwa Narodowego, Warszawa.
22. *Billion-Dollar Scams: The Numbers Behind Business Email Compromise*, 2016 [w:] portal internetowy firmy analitycznej "Trend Micro Security News", 9 czerwiec 2016, (www.trendmicro.com/vinfo/us/security/news /cybercrime-and-digital-threats/billion-dollar-scams-the-numbers-behind-business-email-compromise).
23. BISSON D., 2016. *100,000 Bots Infected with Mirai Malware Behind Dyn DDoS Attack* [in] portal internetowy "Tripwire", 27 październik 2016, (www.tripwire.com/state-of-security/latest-security-news/100000-bots-infected-mirai-malware-caused-dyn-ddos-attack).
24. BIZINA M., GRAY D. H., 2014. *Radicalization of Youth as a Growing Concern for Counter-Terrorism Policy* (w:) 'Global Security Studies', Winter 2014, Volume 5, Issue I.

25. BLUMER H., 1951. *Collective Behavior* (w:) 'Principles of Sociology', Ed. by A. M. Lee, New York.
26. BOCZOŃ W., 2016. *Raport PRNews.pl: Rynek kont osobistych – IV kw.* artykuł internetowy, PRNews.pl 2017, http://prnews.pl/raporty/raport-prnewspl-rynek-kont-osobistych-iv-kw-2016-6553975.html.
27. BÓGDAŁ-BRZEŹIŃSKA A., GARYCKI M.F., 2003. *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, Wydawnictwo ASPRA-JS, Warszawa.
28. BONISŁAWSKA B., 2012. *Współczesne zagrożenia dla bezpieczeństwa publicznego*,[w:] Zeszyty Naukowe WSEI seria: Administracja, 2 (1/2012), Lublin.
29. BORUCH A., 2012. *Bankowość elektroniczna w Polsce*, wydanie II zmienione, Wydawnictwo CeDeWu, Warszawa.
30. BRUCE S., 2006. *Fundamentalizm*, Polity Press, Cambridge 2000, the Polish edition by Wydawnictwo Sic!, Warszawa.
31. BUNT G. R., 2004. *Rip. Burn. Pray: Islamic Expression Online* (w:) Ed. by L. L. Dawson D.E. Cowan, 'Religion Online. Finding Faith on the Internet', Routledge, New York and London.
32. BYRON T., 2008. *Safer Children in a Digital World. The Report of the Byron Review*, Department for Children, Schools and Families, http://dera.ioe.ac.uk/7332/7/Final%20Report%20Bookmarked_Redacted.pdf
33. CASTLES S., MILER M.J., 2011. *Migracje we współczesnym świecie*. Wydawnictwo Naukowe PWN, Warszawa.
34. CBOS, Komunikat z badań, 2008. *Praca Polaków za granicą– doświadczenia i plany*, Warszawa.
35. CBOS, Komunikat z badań, 2014. *Jak nam się żyje? Materialny wymiar życia rodzin*, Warszawa.
36. CHARAKTERY, wrzesień 2013.
37. CHYROWICZ B., 2009. *Jawność i prywatność* (w:) *Prywatyzacja w dobie globalizacji*, (red.) Chyrowicz B., SSpS, Wydawnictwo Towarzystwo Naukowe KUL, Lublin.
38. *Cisco 2017 Annual Cybersecurity Report: Chief Security Officers Reveal True Cost of Breaches and the Actions Organizations are Taking* [in] "the

network. Cisco's Technology News Site", portal "Newsroom.Cisco", 31.01.2017, (https://newsroom.cisco.com/press-release-content?articleId=1818259, za: http://thenetwork. cisco.com).
39. ComCERT,2016. *Koncepcja SOC dla centralnego urzędu administracji publicznej*, artykuł internetowy, ComCERT, https://www.comcert.pl/koncepcja-soc-dla-centralnego-urzedu-administracji-publicznej/.
40. *Criminal Code of Ukraine from 05.04.200, № 2341-III.*
41. *Criminal Procedure Code of Ukraine from 13.04.2012, № 4651-VI.*
42. CZECHOWICZ B., 2017. *Microsoft: ransomware Petya wyrządził szkody głównie wśród użytkowników Windowsa 7* [w:] Portal internetowy „PC Lab", 2.07.2017 r. (http://pclab.pl/news74755.html).
43. DANES L., *Wirus Petya. Jak się go pozbyć?*, 2016. [w:] Witryna internetowa „Usuń Wirusa", 15.04.2016, (https://usunwirusa.pl/wirus-petya).
44. DŁUGOSZ D., *Microsoft: Petya wyrządziła mniej szkód niż WannaCry. Ofiarami głównie komputery z Windows 7*, 2017 *[w:]* Portal internetowy czasopisma „Komputer Świat", 2.07.2017 r. (www.komputerswiat.pl/nowosci/bezpieczenstwo/2017/26/microsoft-petya-wyrzadzila-mniej-szkod-niz-wannacry-ofiarami-glownie-komputery-z-windows-7.aspx).
45. DMOWSKI A., PROKOPOWICZ D., 2006. *Przestępczość elektroniczna i kradzież poufnych informacji – dynamicznie rozwijająca się gałąź szarej strefy* (w:) „*Szara strefa gospodarcza w dobie globalizacji*" - monografia naukowa, Seria wydawnicza: Konferencje i seminaria nr 19, Publikacja pokonferencyjna dla Konferencji naukowej pt.: „*Szara strefa gospodarcza w dobie globalizacji*", Konferencja naukowa w PWSBiA w dniu 06.10.2006 r., Prywatna Wyższa Szkoła Businessu i Administracji w Warszawie, Warszawa 2006, s. 76-96.
46. DMOWSKI A., PROKOPOWICZ D., 2010. *Rynki finansowe*, Wydawnictwo Centrum Doradztwa i Informacji Difin sp. z o.o., Warszawa.
47. DOMAŃSKA-SZARUGA B., 2013. *Common banking supervision within the financial safety net* [w:] K. Raczkowski, F. Schneider (red.), *The*

economic security of business transactions. *Management In Business*, Chartridge Books Oxford, Oxford 2013.
48. DOMAŃSKA-SZARUGA B., PROKOPOWICZ D., 2015. *Makroekonomiczne zarządzanie antykryzysowe* (w:) 34_Zeszyty Naukowe Uniwersytetu Przyrodniczo – Humanistycznego w Siedlcach, nr 107, Seria: Administracja i Zarządzanie (34) 2015, UPH Wydział Nauk Ekonomicznych i Prawnych, Siedlce.
49. DOPIERAŁA R., 2013. *Prywatność w perspektywie zmiany społecznej*, Zakład Wydawniczy NOMOS, Kraków.
50. DUAN E., 2016. *FLocker Mobile Ransomware Crosses to Smart TV* [in] blog internetowy "TrendLabs Security Intelligence Blog", 13 czerwca 2016, (http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv).
51. DUTKO M., KARCIARZ M., 2011. *Informacja w Internecie*, Wydawnictwo Naukowe PWN, Warszawa.
52. DZIADZIA B., 2007. *Wpływ mediów. Konteksty społeczno-edukacyjne*, Oficyna Wydawnicza „Impuls", Kraków.
53. EINSTEIN A., 1958. *Istota teorii względności,* PWN, Warszawa.
54. ELLUL J., 1973. *Propaganda: The Formation of Men's Attitudes*, Random House Vintage Books, 1973.
55. ENISA, 2006. *A step-by-step approach on how to set up a CSIRT*, ENISA, https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/ENISA%20-%20CSIRT%20setting%20up%20guide.pdf.
56. FELIKSIAK M., 2015. *Bezpieczeństwo w internecie*, *Komunikat z badań*, CBOS, Warszawa, nr 109/2015.
57. Foresite.com, 2015. *New study makes a case for Cyber Security-As-a-Service*. Artykuł internetowy, Foresite.com, https://foresite.com/blog/new-study-makes-a-case-for-cyber-security-as-a-service/.
58. *Forex - jak uniknąć oszustwa*, 2006. [in] portal internetowy „Gospodarka.pl. Poradnik Internetu dla Twojej Firmy", za: Skarbiec.Biz, 30.05.2006 (www.egospodarka.pl).
59. FRANKOWSKI G., JERZAK M., 2012. *Advanced Architecture of the Integrated IT Platform with High Security Level*, [w:] A. Dziech, A. Czyżewski, MCSS', *Conference Proceedings, Communications in*

Computer and Information Science Vol. 287, Springer-Verlag 2012, http://link.springer.com/content/pdf/10.1007/978-3-642-30721-8_11.pdf.
60. FRANKOWSKI G., JERZAK M., MIŁOSTAN M., NOWAK T., PAWŁOWSKI M., 2015. *Application of the Complex Event Processing system for anomaly detection and network monitoring*, Computer Science Journal Vol. 16, No. 4, str. 351-372, AGH Kraków, http://journals.agh.edu.pl/csci/article/view/1278/1379.
61. GACKI G., 2006. *Przestępczość internetowa*, [in] Portal internetowy „*Gospodarka.pl. Poradnik Internetu dla Twojej Firmy*", 07.09.2006, (www.egospodarka.pl).
62. GAŚ Z., 1994. *Kierunki działań profilaktycznych*, Pracownia Wydawnicza Fundacji "Masz Szansę", Lublin.
63. GĄSIOROWSKI J., PODSIEDLIK P., 2015. *Przestępstwa w bankowości elektronicznej w Polsce. Próba oceny z perspektywy prawno-kryminalistycznej - Bankowość elektroniczna – typologia*, Dystrybutor Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza.
64. GIBSON W., 1999, *Neuromancer*, Wydawnictwo Książnica, Poznań.
65. GIBSON W., 2009. *Neuromancer*, Wydawnictwo Książnica, Warszawa.
66. GIDDENS A., 2010. *Nowoczesność i tożsamość*. PWN, Warszawa.
67. *Globalne dochody bitcoin wirusa petya*, 2017 [w:] Portal internetowy „CryptoNews.Pl", 29.06.2017, (https://cryptonews.pl/10-200-globalne-dochody-bitcoin-wirusa-petya).
68. GOODIN D., 2014. *PoC Hack on Data Sent Between Phones and Smartwatches (Updated)* [in] portal internetowy "arsTechnica", 10 grudnia 2014, (http://arstechnica.com/security/2014/12/connections-between-phones-and-smartwatches-wide-open-to-brute-force-hacks).
69. GÓRKA M., (red.) 2014. *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Wydawnictwo Difin, Warszawa.
70. GRACZ K., 2007. *Przymusowe migracje a perspektywa wielokulturowości w Polsce*, (w:) Gutowska A., (red.) *Uchodźcy w Polsce. Kulturowo-prawne bariery w procesie adaptacji*. Stowarzyszenie Interwencji Prawnej. Warszawa.
71. GRZELAK A., 2008. *Trzeci filar Unii Europejskiej*, Wydawnictwo Sejmowe, Warszawa.

72. GRZELAK M., 2011. *Międzynarodowa strategia USA dla cyberprzestrzeni*, (w:) *Bezpieczeństwo Narodowe*. Kwartalnik wyd. przez Biuro Bezpieczeństwa Narodowego, Warszawa 2011, nr II - 2011/18.
73. GRZELAK M., 2014. *Szpiegostwo i inwigilacja w internecie* (w:) „*Socjotechniczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji"*, (red.) Liedel K., Piasecka P., Aleksandrowicz T.R., Wydawnictwo Delfin, Warszawa.
74. GRZELAK M., RIEDEL K., 2012. *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „Bezpieczeństwo Narodowe" nr 22.
75. GRZYWACZ J., 2016. *Bankowość elektroniczna w przedsiębiorstwie*, Wydawnictwo SGH, Warszawa.
76. GRZYWAK A., WIDENKA G., 2015. *Bezpieczeństwo rozproszonych systemów informatycznych - Kryptografia w zastosowaniu do podpisu cyfrowego i identyfikacji użytkownika w sieci Internet,* Wydawnictwo Wyższa Szkoła Biznesu w Dąbrowie Górniczej, Dąbrowa Górnicza.
77. GUERRESCHI C., 2010. *Nowe uzależnienia*, Salwator, Kraków.
78. GUS, 2017. *Społeczeństwo informacyjne w Polsce w 2016 r.*, GUS,http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5497/2/6/1/si__sygnalna_2016.pdf.
79. GWÓŹDŻ M., 2016. *Liczby polskiego Internetu 2016*, artykuł internetowy, SMMeasure.eu, http://smmeasure.eu/liczby-polskiego-internetu-2016/.
80. GWOŹDZIEWICZ S., 2016. *Problemy prawnokarne cyberstalkingu w polskim systemie prawnym* [in] „Medzinarodny Vedecky Zbornik III", Srbske Rozvojove Združenie, Bačsky Petrovec, Serbia.
81. GWOŹDZIEWICZ S., JAKUBOWSKI J., 2017. *The tasks of the national administration within the protection of the Polish Cyberspace* [in] Public Mamagement - Публічне Урядування - Collection is trained in scientific partnership with the Ukrainian Technological Academy - № 2 (7) – May 2017, Kijów.
82. GWOŹDZIEWICZ S., PROKOPOWICZ D., 2015. *Administrative, supervisory and legal determinants of globalization of financial markets and the banking system in Poland* [in] "International Journal of New Economics and Social Sciences", nr 2 (2) 2015.

83. GWOŹDZIEWICZ S., PROKOPOWICZ D., 2015. *Administrative, supervisory and legal determinants of globalization of financial markets and the banking system in Poland [w:]* "International Journal of New Economics and Social Sciences", nr 2 (2) 2015.
84. GWOŹDZIEWICZ S., PROKOPOWICZ D., 2016a. *Bezpieczeństwo bankowości internetowej i uwarunkowania elektronicznego transferu danych w technologii Big Data w Polsce* [w:] Vlastimil V. (red.), "Međunarodni naučni zbornik. Pravo Ekonomija Menadžment I" /Międzynarodowe zeszyty naukowe. Zarządzanie Prawo Gospodarka I/ International scientific books. Right, Economy and Management I/, Wydawnictwo [Izdavač:] Srpsko Razvojno Udruženje /Stowarzyszenie Rozwoju Serbii/ Bački Petrovac.
85. GWOŹDZIEWICZ S., PROKOPOWICZ D., 2016b. *Prawo do ochrony informacji i danych osobowych w cyberprzestrzeni w dobie rozwoju bankowości internetowej - The Right to Protection of Information and Personal Data in the Cyberspace in the Age of the Internet Banking Development* [w:] D. Gałuszka, G. Ptaszek, D. Żuchowska-Skiba (red.), "Technologiczno-społeczne oblicza XXI wieku", Wydawnictwo LIBRON Filip Lohner, Kraków.
86. GWOŹDZIEWICZ S., PROKOPOWICZ, D., 2016c. *System and normative adaptation of the financial system in Poland to the European Union Standards - The Next Stage* [in] *Globalization, the State and the Individual*, "International Scientific Journal", Free University of Varna "Chernorizets Hrabar", Chayka, Bułgaria, Varna 2016, nr 4 (12) 2016.
87. HABRAJSKA G., 2005. *Nakłanianie, perswazja, manipulacja językowa*, Acta Universitatis Lodziensis, nr 7.
88. HASEBRINK U., LIVINGSTONE S., HADDON L., OLAFFSON K., 2009. *Comparing children's online opportunities and risks across Europe: cross-national comparisons for EU Kids Online*, 2nd edition, EU Kids Online, http://eprints.lse.ac.uk/24368/1/D3.2_Report-Cross_national_comparisons-2nd-edition.pdf
89. HEYDT-BENJAMIN T.S., BAILEY D.V., KEVIN FU, JUELS A., O'HARE T., 2006. *RFID Payment Card Vulnerabilities Technical Report*, www.nytimes.com, 23 Oct 2006.

90. Incapsula.com, *Botnet DDoS Attacks*, artykuł internetowy, Incapsula.com https://www.incapsula.com/ddos/ddos-attacks/botnet-ddos.html.
91. Integrated Solutions, 2015. *Oszczędności kontra bezpieczeństwo*. Artykuł internetowy, Integrated Solutions, http://www.integratedsolutions.pl/pl/firma/aktualnosci/nowe-zycie-outsourcingu-it-w-polsce/.
92. JAWŁOWSKA A., (red.) 2001. *Wokół problemów tożsamości*, Wydawnictwo Naukowe LTW, Warszawa.
93. JĘDRUSZCZAK K., 2005, *Modele i koncepcje prywatności w psychologii* (w:) *Przegląd psychologiczny*, Bydgoszcz, tom 48, nr 2.
94. JESSEL A.D., MOIR A., 2010. *Płeć mózgu. O prawdziwej różnicy między mężczyzną i kobietą*, Państwowy Instytut Wydawniczy, Warszawa.
95. JUEL A., MOLNAR D., WAGNER D., 2005. *Security and Privacy Issues in E-passports*, Cryptology ePrint Archive: Report 2005/095,
96. JUELS A., 2005. *RFID Security and Privacy: A Research Survey*, RSA Laboratories.
97. KAŁUŻA-KOPIAS D., 2014. *Demograficzne skutki międzynarodowych migracji w wybranych krajach Unii Europejskiej ze szczególnym uwzględnieniem Polski* (w:) „*Polityka społeczna wobec przemian demograficznych. Studia Ekonomiczne*", Zeszyty Naukowe Wydziałowe Uniwersytetu Ekonomicznego w Katowicach, (red.) Rączaszek A., Koczur W., nr 167.
98. KANNOUF N., DOUZI Y., BENABDELLAH M., 2015. *Security on RFID technology. 2015 International Conference on Cloud Technologies and Applications*, IEEE, 30 November.
99. KARMAKAR N.C., 2013. *Advanced RFID Systems, Security, and Applications*, IGI Global, USA.
100. Kaspersky Lab, 2015. *Damage Control: The cost of security breaches. IT Security Special Report Series*, Kaspersky Lab, http://media.kaspersky.com/pdf/it-risks-survey-report-cost-of-security-breaches.pdf.
101. KASPRZAK R., MAJ M., TARAPATA Z., 2015. *Przestępstwa w cyberprzestrzeni. Aspekty technologiczne i prawne* (w:) praca zbiorowa pod redakcją naukową: PŁYWACZEWSKI E.W., FILIPOWSKI W., RAU

Z., *PRZESTĘPCZOŚĆ W XXI WIEKU ZAPOBIEGANIE I ZWALCZANIE Problemy technologiczno-informatyczne*, Wolters Kluwer SA, Warszawa.
102. KAWCZYŃSKA – BUTRYM Z., 2008. *Migracja: Perspektywa mikrospołeczna – indywidualne i rodzinne zyski, koszty i straty*, [w:] *Migracja – wyzwanie XXI wieku*, (red.) ZIĘBA M., Katolicki Uniwersytet Lubelski Jana Pawła II, Lublin.
103. KIRSCHENBAUM I., WOOLY A., 2006. *How to Build a Low-Cost, Extended-Range RFID Skimmer*, School of Electrical Engineering Systems; Tel Aviv University, Israel.
104. KLIARSKY A., ATLASIS A., 2011. *Responding to Zero Day Threats*, SANS Institute, http://www.sans.org/reading-room/whitepapers/incident/respondingzero-day-threats-33709.
105. *Kogo zaraził wirus Petya? Polska w czołówce,* 2017 *[w:]* Portal internetowy czasopisma „Rzeczpospolita", 28.06.2017 r. (www.rp.pl/Spoleczenstwo/170629060-Kogo-zarazil-wirus-Petya-Polska-w-czolowce.html).
106. KOŁODZIEJCZYK Ł., 2014. *Prywatność w Internecie*, Wydawnictwo SBP, Warszawa.
107. KONIECZNA E.J., (red.), 2005. *Biblioterapia w praktyce. Poradnik dla nauczycieli, wychowawców, terapeutów*, Impuls, Kraków.
108. *Konsekwencje ataku Petya,* 2017 [w:] Portal internetowy „Speedtest.Pl", 28.06.2017 r. (http://www.speedtest.pl/wiadomosci/polecane/konsekwencje-ataku-petya).
109. KORCZAK J., KIJEWSKA K., 2009. *Automatyczna identyfikacja w logistyce- szanse i zagrożenia,* Instytut Ekonomii i Zarządzania; Politechnika Koszalińska, Koszalin.
110. KORDACZUK-WĄS M., 2017. *Policyjne działania w obszarze profilaktyki społecznej* (w:) KORDACZUK-WĄS M., MAZUR J., STAWNICKA J., (red.) *Działania profilaktyczne. Planowanie-projektowanie-realizacja,* (manuskrypt).
111. KORDACZUK-WĄS M., DE JONGH L.-A., 2017. *Breaking the process of violent radicalisation in Juvenile Justice Systems. A manual on how to protect children at risk of radicalisation through alternatives to detention*

and prevention measures, International Juvenile Justice Observatory, Brussels (manuscript).
112. KOSIŃSKI J., 2015. *Paradygmaty cyberprzestępczości*, Wydawnictwo Difin, Warszawa.
113. KOT E., TOMASZYCKI K., 2015. *Funkcjonowanie automatycznego systemu identyfikacji daktyloskopijnej AFIS* (w:) praca zbiorowa pod redakcją naukową: PŁYWACZEWSKI E.W., FILIPOWSKI W., RAU Z., *PRZESTĘPCZOŚĆ W XXI WIEKU ZAPOBIEGANIE I ZWALCZANIE Problemy technologiczno-informatyczne*, Wolters Kluwer SA, Warszawa.
114. KOT E., TOMASZYCKI K., 2017. *Biegły daktyloskopii wobec problemu migracyjnego*, (w:) KUŹNIAR Z., ŁAPIŃSKA A., TOMASZYCKI K., (red.) *Zagrożenia bezpieczeństwa w XXI wieku – I. Terroryzm a bezpieczeństwo kulturowe*, WSO WL Wydawnictwo Uczelniane, Wrocław.
115. KOTOWSKI W., KURZĘPA B., 2009. *Dozór elektroniczny. Komentarz praktyczny*, Wydanie 1, Wydawnictwo LexisNexis, Warszawa.
116. KOZAK S., 2011. *Patologie komunikowania w Internecie*, Difin, Warszawa.
117. KOZAK S., 2013. *Patologia fonoholizmu. Przyczyny, skutki i leczenie uzależnienia dzieci i młodzieży od telefonu komórkowego*, Difin, Warszawa.
118. KOZAK S., 2014. *Patologia cyfrowego dzieciństwa i młodości*, Difin, Warszawa.
119. KRAJOWE BIURO PRZECIWDZIAŁANIA NARKOMANII, 2016. *Metody i strategie profilaktyczne* [online]. Dostęp na: www.kbpn.gov.pl. Data korzystania: [listopad 2016].
120. KREBS B., 2016. *Microsoft: No More Pick-and-Choose Patching* [in] portal internetowy "Krebs on Security", 11 październik 2016, (https://krebsonsecurity.com/2016/10/microsoft-no-more-pick-and-choose-patching).
121. KRÓL A., 2017. *Pesymistyczne prognozy* [in] „*Bank. Miesięcznik Finansowy"*, Raport specjalny: „*Cyberprzestępstwa. Bezpieczeństwo banków 2017*", nr 04 (287), kwiecień 2017.
122. KRYWKO J., 2014. (artykuł) *Uśmiech, czy ciąg znaków*, „Gazeta wyborcza", 10.04.2014.

123. KRZEMIŃSKA B., 2008. *Kompetencje Wydziału Daktyloskopii CLK KGP we współpracy międzynarodowej* (w:) Problemy Kryminalistyki, nr 262
124. KRZEMIŃSKA B., 2009. *Koncepcja automatycznej wymiany danych daktyloskopijnych* (w:) praca zbiorowa pod redakcją naukową: podinsp. RYBICKI P., TOMASZEWSKI T., *Daktyloskopia 100 lat na ziemiach polskich*, Stowarzyszenie Absolwentów Wydziała Prawa i Administracji UW, Warszawa.
125. KRZEMIŃSKA B., TOMASZYCKI K., 2017. *Migracja do Unii Europejskiej a poczucie bezpieczeństwa.* (w:) KUŹNIAR Z., ŁAPIŃSKA A., TOMASZYCKI K., (red.) *Zagrożenia bezpieczeństwa w XXI wieku – I. Terroryzm a bezpieczeństwo kulturowe*, WSO WL Wydawnictwo Uczelniane, Wrocław.
126. KUBITSKY J., 2012. *Psychologia migracji*, Wydawnictwo Difin, Warszawa.
127. LAWRENCE B.B., 2002. *Allah On-Line: The Practice of Global Islam in the Information Age* (w:) Practicing Religion in the Age of The Media Ed. by Hoover S. M., Clark L.S., Columbia University Press, New York.
128. LE BON G., 1986. *Psychologia tłumu*, Wydawnictwo Naukowe PWN, Warszawa.
129. LECIEJEWICZ L., 2006. *Migracje w pradziejach i starożytności. Wprowadzenie do dyskusji* (w:) FURDALA A., WYSOCZAŃSKI W., (red.) *Migracje: dziej, typologia, definicje*, Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław.
130. LEOPANDO J., 2016. *Patch Your Flash: Another Zero-Day Vulnerability Hits Adobe Flash* [in] blog internetowy "TrendLabs Security Intelligence Blog", 27 październik 2016, (http://blog.trendmicro.com/trendlabs-security-intelligence/patch-flash-another-zero-day-vulnerability-hits-adobe-flash).
131. LIMANÓWKA A., 2007. *Cyberprzestrzeń a rzeczywistość wirtualna,* (red.) SOKOŁOWSKI M., *Oblicza Internetu: architektura komunikacyjna sieci*, Wydawnictwo Państwowej Wyższej Szkoły Zawodowej w Elblągu, Elbląg.
132. MACIEJEWSKI J., 2006, *Grupy dyspozycyjne społeczeństwa polskiego,* Socjologia XXXVIII, [w:] red. MACIEJEWSKI J., Wydawnictwo Uniwersytetu Wrocławskiego, Wrocław.

133. MALAK P., 2017. *Przejęcie kontroli nad użytkownikiem* [in] „*Bank. Miesięcznik Finansowy"*, Raport specjalny: „*Cyberprzestępstwa. Bezpieczeństwo banków 2017*", nr 04 (287), kwiecień 2017.
134. MASSY D., 2014. *What Does the End of Support of Windows XP Mean for Windows Embedded?* [in] portal internetowy firmy informatycznej "Microsoft Developer Network", 17 luty 2014, (https://blogs.msdn.microsoft.com/windows-embedded/2014/02/17/what-does-the-end-of-support-of-windows-xp-mean-for-windows-embedded).
135. MATOSEK M.,2009. *Kultura innowacyjna jako czynnik realizacji strategii zrównoważonego rozwoju Asea Brown Boveri* [in] Grądzki R., Matejn M., (red.), „*Rozwój zrównoważony – zarządzanie innowacjami ekologicznymi*", Katedra Podstaw Techniki i Ekologii Przemysłowej Politechniki Łódzkiej, Łódź.
136. MAYER-SCHONBERGER V., 2015. *Big Data. Rewolucja, która zmieni nasze myślenie, pracę i życie*, Wydawnictwo MT Biznes, Warszawa.
137. McAfee® Foundstone® Professional Services,2015. *Creating and Maintaining a SOC. The details behind successful security operations centers.* McAffee/Intel Security, http://www.mcafee.com/de/resources/white-papers/foundstone/wp-creating-maintaining-soc.pdf.
138. McFARLAND CH., PAGET F., SAMANI R., 2015. *The Hidden Data Economy. The Marketplace for Stolen Digital Information*, McAfee Labs/Intel Security http://www.mcafee.com/us/resources/reports/rp-hidden-data-economy.pdf.
139. MERKWA M., 2011. *Prawo dostępu do Internetu jako prawo człowieka w kontekście wyzwań współczesnego świata* (w:) „*Era globalizacji. Współczesne zagrożenia i wyzwania w zakresie bezpieczeństwa"* (red.) Oleksiewicz I., Polinceusz M., Pomykała M., Rajchel J., Wydawnictwo Amelia, Rzeszów-Warszawa.
140. MICHALCZYK S., 2015. *Jednostka i społeczeństwo w świecie mediów. Klasyczne i współczesne idee w teoriach średniego zasięgu*, Wydawca: Stowarzyszenie Thesaurus Silesiae – Skarb Śląska, Katowice.
141. *Michigan State University Confirms Data Breach of Server Containing 400,000 Student, Staff Records*, 2016.[in] portal internetowy *"WXYZ*", 18

listopad 2016, (www.wxyz.com/news/michigan-state-university-confirms-data-breach-of-server-containing-400000-student-staff-records).

142. MICZKOWSKA A., 2009. *Problematyka przestępczości zorganizowanej*, (w:) SADOWSKI M., SZYMANIEC P., (red.) WROCŁAWSKIE STUDIA ERAZMIAŃSKIE. ZESZYTY STUDENCKIE, *Prace prawnicze, administratywistyczne i historyczne*, Katedra Doktryn Politycznych i Prawnych WPAiE UWr, Wrocław.
143. MILLER M., BURRELL T., HOWARD M., 2011. *Mitigating Software Vulnerabilities. How exploit mitigation technologies can help reduce or eliminate risk, prevent attacks and minimize operational disruption due to software vulnerabilities*, Microsoft Corporation.
144. Ministerstwo Cyfryzacji, 2017. *Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017-2022*, Ministerstwo Cyfryzacji, https://mc.gov.pl/files/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf.
145. MŁYNARSKA-SOBACZEWSKA A., 2013, T*rzy wymiary prywatności. Sfera prywatna i publiczna we współczesnym prawie i teorii społeczne*j (w:) *Przegląd Prawa Konstytucyjnego*, Toruń, nr 1 (13)/2013.
146. MŁYŃSKA K., 2004/2005. *Cyber-granice nieskończoności* (w:) „Kwadratura Koła", Rocznik Kół Naukowych, Katowice.
147. MOCZYDŁOWSKI P., 2006.*Przestępca na uwięzi. Elektroniczny monitoring sprawców przestępstw*, Wydawnictwo Ius et Lex, Warszawa.
148. MODRZEJEWSKA D., 2008. *Kompleksowe podejście w działaniach profilaktycznych* (w:) SZCZEPANIK J., (red.) *Różne spojrzenia na przemoc,* Wydawnictwo WSHE, Łódź 2008, s. 214;
149. NEUMANN P., 2015. *Foreign fighter total in Syria/Iraq now exceeds 20,000; surpasses Afghanistan conflict in the 1980s*, ICSR, King's College London. Dostęp na: http://icsr.info/2015/01/foreign-fighter-total-syriairaq-nowexceeds-20000-surpasses-afghanistan-conflict-1980s/ [30 January 2017].
150. NOWOTNIK D., 2011. *Migracje zagraniczne w krajach Unii Europejskiej w warunkach kryzysu gospodarczego* (w:) *„Prace Komisji Geografii Przemysłu",* Warszawa-Kraków 2011, nr 18.

151. NYDELL (OMAR) M.K., 2001. *Zrozumieć arabów*. Wydawnictwo Studio Emka, Warszawa.
152. OŚRODEK BADAŃ NAD MIGRACJAMI, 2015. *Kryzys I co dalej?*, „Biuletyn Migracyjny", Nr 53/2015.
153. PACEK B., HOFFMAN R., 2013. .*Działania sił zbrojnych w cyberprzestrzeni*, Warszawa.
154. PASSERI P.,2017. *February 2017 Cyber Attacks Statistics.* Artykuł internetowy, Hackmageddon.com, http://www.hackmageddon.com/2017/03/20/february-2017-cyber-attacks-statistics/.
155. PAULI D., 2016. *IoT Worm Can Hack Philips Hue Lightbulbs, Spread Across Cities* [in] portal internetowy "The Register", 10 listopada 2016, (www.theregister.co.uk/2016/11/10/iot_worm_can_hack_philips_hue_lightbulbs_spread_across_cities).
156. PERRAUDIN F., 2015. *UK Launches Twitter Account to Combat Islamic State Propaganda*, 'Guardian', August 28.
157. PESCATORE J., TOUNG G., 2009. *Defining the Next-Generation Firewall*, Gartner RAS Core Research Note G00171540, https://www.gartner.com/doc/1204914/defining-nextgeneration-firewall.
158. PIASECKA P., 2017. *Cyberprzestrzeń jako źródło zagrożeń asymetrycznych – wyzwania i rekomendacje* (w:) praca zbiorowa pod redakcją naukową: LIEDEL K., PIASECKA P., *BEZPIECZEŃSTWO ANTYTERRORYSTYCZNE Świadomość społeczna i edukacyjna*, Difin SA, Warszawa.
159. PLESZKUN-OLEJNICZAK E., BACHURA J., WORSOWICZ M., (red.), 2010. *O mediach i komunikacji*, Wydawnictwo UŁ, Łódź.
160. *Podsumowanie Ransomware: Analiza WannaCry Surze*, 2017 [in] portal internetowy "Trend Micro", Analiza firmy analitycznej Trend Micro,, Dział: „Aktualności – Bezpieczeństwo, 30.05.2017 r., (www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-business-as-usual-after-wannacry-surge).
161. POLASIK M., 2008. *Bankowość elektroniczna. Istota - stan – perspektywy*, Wydawnictwo CeDeWu, Warszawa.

162. PROKOPOWICZ D., 2005. *Ewolucja procesu doskonalenia zarządzania ryzykiem kredytowym w polskiej bankowości [w:]* Zeszyty Naukowo-Teoretyczne PWSBiA „Wiek XXI. The 21st Century", Nr 4 (14) 2004 / 1 (15) 2005, Prywatna Wyższa Szkoła Businessu i Administracji w Warszawie, Warszawa.
163. PROKOPOWICZ D., 2009. *Zagrożenia rozwoju i bezpieczeństwo bankowości elektronicznej* [w:] Zeszyty Naukowe Wyższa Szkoła Zarządzania i Prawa im. Heleny Chodkowskiej w Warszawie. Rok XIV. Nr 1 (30)/2009.
164. PROKOPOWICZ D., 2011. *Rozwój bankowości elektronicznej w Polsce [w:]* "Przedsiębiorstwo przyszłości". Kwartalnik Wyższej Szkoły Zarządzania i Prawa im. Heleny Chodkowskiej. Warszawa, Nr 2 (7) 2011, Kwiecień 2011, Rok wyd. III.
165. PROKOPOWICZ D., 2013. *Zintegrowane zarządzanie ryzykiem kredytowym w bankach komercyjnych [w:]* "Ekonomika i Organizacja Przedsiębiorstwa. Economics and Organization of Enterprise" Zeszyty Naukowe. Wydawnictwo Instytut Organizacji i Zarządzania w Przemyśle „ORGMASZ", Indeks 357022, nr 8 (763) 2013, sierpień 2013.
166. PROKOPOWICZ D., 2017. *Bezpieczeństwo udostępniania informacji przez instytucje sektora publicznego oraz transferu danych niejawnych poprzez sieć Internet* [w:] GOŁĘBIOWSKA A., ZIENTARSKI B., (red.), „*Ponowne wykorzystywanie informacji sektora publicznego w administracji*", Senat Rzeczypospolitej Polskiej, Kancelaria Senatu, Warszawa.
167. PROKOPOWICZ D., DMOWSKI A., 2010. *Rynki finansowe*, Wydawnictwo Centrum Doradztwa i Informacji Difin sp. z o.o., Warszawa.
168. PROKOPOWICZ D., DMOWSKI A., SARNOWSKI J., 2005. *Podstawy finansów i bankowości,* Wydawnictwo Centrum Doradztwa i Informacji Difin sp. z o.o., Warszawa.
169. PRYCIAK M., 2010, *Prawo do prywatności* (w:) Wrocławskie Studia Erazmiańskie, Wrocław, Rocznik 10, tom IV.
170. *Przewidywania dotyczące bezpieczeństwa. Następny poziom. Płaskowyż ransomware, większy kompromis z procesem biznesowym i boom cyberpropagandy - jakie powinnyśmy spodziewać się w 2017 roku?* [in] portal internetowy "Trend Micro", Raport firmy analitycznej Trend

Micro, 6.12.2016, (www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2017).
171. PURDY G., 2010. *ISO 31000:2009—Setting a New Standard for Risk Management*, Risk Analysis, Vol. 30, No. 6.
172. PYŻALSKI J., 2009. *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska*, „*Dziecko Krzywdzone*", nr 1.
173. RADZEWICZ Sz., 2017. *FAQ: ransomware Petya – odpowiedzi na najpopularniejsze pytania* [w:] blog internetowy „Spiders Web. Blog blisko technologii", 28.06.2017, (www.spidersweb.pl/2017/06/faq-ransomware-petya.html).
174. *Ransomware Recap: Petya Ransomware Outbreak Shakes Europe*, 2017 [w:] Portal internetowy analitycznej firmy technologicznej „TrendMicro", 28.06.2017 (www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-recap-petya-ransomware-outbreak-shakes-europe).
175. *Raport Trend Micro: wzrost liczby ataków ransomware w 2016 r.* [in] Portal „AleBank.pl", za: *Analiza firmy analitycznej Trend Micro*, 22.03.2017, (https://alebank.pl/trend-micro-wzrost-liczby-atakow-ransomware-w-2016-r/?id=225760&catid=361).
176. *Raport Trend Micro: wzrost liczby ataków ransomware w 2016 r. [w:]* Portal "AleBank.pl", za: Analiza firmy analitycznej Trend Micro, 22.03.2017, (https://alebank.pl/trend-micro-wzrost-liczby-atakow-ransomware-w-2016-r/?id=225760&catid=361).
177. *Report on the number of people who were convicted, justified, closed cases, non-triable persons, use of compulsory measures of medical character and criminal penalty types for the period of 2010 - 2016.*
178. SHAVIT S., 2004. *Contending with International Terrorism*, 'Journal of International Security Affairs'.
179. SIENKIEWICZ P., 2009. *Terroryzm w cybernetycznej przestrzeni* (w:) JEMIOŁA T., KISIELNICKI J., RAJCHEL K., (red.) *Cyberterroryzm – nowe wyzwania XXI wieku*, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa.
180. SIMM M., WĘGRZYN-JONEK E., 2002. *Budowanie szkolnego programu profilaktyki*, „Rubikon", Kraków.

181. SIMON P., 2017. *Czy multikulturalizm jest wspólnotowy?* (w:) THIOLLET H., (red.) *Migranci, migracje. O czym warto wiedzieć, by wyrobić sobie własne zdanie*. Wydawnictwo Karakter, Kraków.
182. *Słownik terminów z zakresu bezpieczeństwa narodowego*, 2002. Wydawnictwo AON, Warszawa.
183. SPITZER M., 2013. *Cyfrowa demencja. W jaki sposób pozbawiamy rozumu siebie i swoje dzieci*, (przeł.) LIPIŃSKI A., Dobra Literatura, Słupsk.
184. STECH G., 2017. *Petya Wielki… Problem*, [w:] portal internetowy „Computerworld", 28.06.2017, (www.computerworld.pl/news/Petya-Wielki-Problem,408326.html).
185. STOJER-POLAŃSKA J., 2015. *Kryminalistyczne aspekty cyberterroryzmu* (w:) praca zbiorowa pod redakcją naukową: PŁYWACZEWSKI E.W., FILIPOWSKI W., RAU Z., *Przestępczość w XXI wieku zapobieganie i zwalczanie. Problemy technologiczno-informatyczne*, Wolters Kluwer SA, Warszawa.
186. STROIŃSKI M., WĘGLARZ J., 2008. *Znaczenie e-infrastruktury dla nauki*, Biuro Upowszechniania i Promocji Nauki PAN.
187. STRZAŁKO J. (red.), 2006. *Słownik terminów biologicznych*, Wydawnictwo Naukowe PWN, Warszawa.
188. SUCHOCKA R., 2014. *Dwa oblicza życia imigrantów w enklawie etnicznej,* (w:) RUCH PRAWNICZY, EKONOMICZNY I SOCJOLOGICZNY, Rok LXXVI – zeszyt 1 – 2014, Poznań.
189. SUCHORZEWSKA A., 2010. *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Oficyna a Wolters Kluwer business, Warszawa.
190. SYED AHSON, MOHAMMAD ILYAS (red.), 2008. *RFID HANDBOOK.Applications, Technology, Security, and Privacy*, CRC Press.
191. SZACKA B., 2003. *Wprowadzenie do socjologii*. Oficyna Naukowa, Warszawa.
192. SZACKI J., 2002. *Historia socjologii*, Wydawnictwo Naukowe PWN, Warszawa.
193. SZAFRAŃSKI J., 2009. *Cyberterroryzm – rzeczywiste zagrożenie w wirtualnym świecie?* (w:) JEMIOŁA T., KISIELNICKI J., RAJCHEL K.,

(red.), *Cyberterroryzm – nowe wyzwania XXI wieku*, Wyższa Szkoła Informatyki, Zarządzania i Administracji, Warszawa.

194. SZCZURKOWSKI M., 2010. *Wytwarzanie i sterowanie polami magnetycznymi dla radiowej identyfikacji obiektów RFID oraz indukcyjnego przekazu energii*. ROZPRAWA DOKTORSKA, Akademia Górniczo-Hutnicza Stanisława Staszica w Krakowie. Wydział Elektrotechniki, Automatyki, Informatyki i Elektroniki. Kraków.
195. SZKODZIN B., 2006. *Oszustwa internetowe IX 2006*, [in] portal internetowy „*Gospodarka.pl. Poradnik Internetu dla Twojej Firmy",* 11.10.2006 (www.egospodarka.pl).
196. SZPOR G. (red.), 2013. *Internet Cloud computing Przetwarzanie w chmurach*, Wydawnictwo C.H. Beck, Warszawa.
197. SZTOMPKA P., 2005. *Socjologia zmian społecznych.* Wydawnictwo Znak, Kraków.
198. SZYMANEK K., 2005. *Sztuka argumentacji. Słownik terminologiczny*, Warszawa.
199. SZYMAŃSKA J., ZAMECKA J., 2002. *Przegląd koncepcji i poglądów na temat profilaktyki* (w:) ŚWIĄTKIEWICZ G., (red.) *Profilaktyka w środowisku lokalnym*, KBPN, Warszawa.
200. TABI B., 1995. *Fundamentalizm religijny*, Bibliographisches Institut & F.A. Brockhaus AG, Mannheim, the Polish edition by Państwowy Instytut Wydawniczy, Warszawa.
201. TATARKIEWICZ W., 1948. *Historia filozofii,* t. I., „Czytelnik". Warszawa.
202. Teamquest.pl, 2016. *Boom na specjalistów od bezpieczeństwa IT*, artykuł internetowy, Teamquest.pl,https://teamquest.pl/blog/199_boom-na-specjalistow-od-bezpieczenstwa-it.
203. THIOLLET H., 2017. *Czy ludzie migrują z krajów biednych do bogatych?* (w:) THIOLLET H., (red.) *Migranci, migracje. O czym warto wiedzieć, by wyrobić sobie własne zdanie*. Wydawnictwo Karakter, Kraków.
204. TOŁPA T., PROTASIEWICZ J., KOZŁOWSKI M., BUŁKSZAS B., 2015. *Zagrożenia, nadużycia i bezpieczeństwo w systemach informatycznych a granice ochrony praw podstawowych* (w:) praca zbiorowa pod redakcją naukową: PŁYWACZEWSKI E.W., FILIPOWSKI W., RAU Z.,

PRZESTĘPCZOŚĆ W XXI WIEKU ZAPOBIEGANIE I ZWALCZANIE Problemy technologiczno-informatyczne, Wolters Kluwer SA, Warszawa.

205. TOMASZYCKI K., KUŹNIAR Z., ŁAPIŃSKA A., 2017. *Kontrola migracji a terroryzm*, (w:) KUŹNIAR Z., ŁAPIŃSKA A., TOMASZYCKI K., (red.) *Zagrożenia bezpieczeństwa w XXI wieku – I. Terroryzm a bezpieczeństwo kulturowe*, WSO WL Wydawnictwo Uczelniane, Wrocław.
206. TREJDEROWSKI T., 2013. *Kradzież tożsamości. Terroryzm informatyczny*, Wydawnictwo Eneteia, Warszawa.
207. *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats*, 2017[in] portal internetowy "Trend Micro", Raport firmy analitycznej Trend Micro, 28.02.2017,(www.trendmicro.com/vinfo /us/security/research-and-analysis/threat-reports/roundup).
208. *TrendLabs 2016 Annual Security Roundup: A Record Year for Enterprise Threats*, 2017 *[w:]* portal internetowy "Trend Micro", Raport firmy analitycznej Trend Micro, 28.02.2017, (www.trendmicro.com/vinfo /us/security/research-and-analysis/threat-reports/roundup).
209. TREVERTON G.F., 2011. *Comparing Early Warning Across Domains*, The Swedish National Defence College.
210. TURKLE S., 2010. *Samotni razem, Dlaczego oczekujemy więcej od zdobyczy techniki, a mniej od siebie nawzajem* (przekład) CIERPISZ M., Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków
211. TURNER R., KILLIAN L., 1972. *Collective behavior*, Englewood Cliffs.
212. *Twórca wirusa Petya zaoferował swoją pomoc*, 2017 [w:] Portal internetowy „Sputnik News", 30.06.2017 r. (https://pl.sputniknews.com/swiat/201706305785339-sputnik-wirus-petya).
213. VIEGA,, J., Mc GRAW G., 2002. *Building Secure Software: How to Avoid Security Problems the Right Way*, Boston, MA: Addison-Wesley.
214. WALLACE P., 2001. *Psychologia Internetu,* Dom Wydawniczy Rebis, Poznań.
215. WASZCZUK P., 2015. *Dodatkowy wymiar bezpieczeństwa IT,* artykuł internetowy, ITWiz http://itwiz.pl/dodatkowy-wymiar-bezpieczenstwa/.
216. WEIMANN, G., 2006. *Terror on the Internet. The New Arena, the New Challenges*, United States Institute of Peace Press, Washington.

217. WINTER CH., 2015 (a). *Documenting the Virtual Caliphate*, Quilliam Foundation.
218. WINTER CH., 2015 (b). *Islamic State Propaganda: Our Response to the Competition* (w:) Cyber Propaganda From how to start a revolution to how to beat ISIS, 'BEYOND PROPAGANDA'.
219. WINTER CH., 2015 (c). *Experts Weigh In (part 4): Can the United States Counter ISIS Propaganda?*, Brookings Institution Markaz.
220. *Wirus Petya zaatakował Polskę. Zobacz, jak go usunąć i zabezpieczyć komputer,* 2017 [w:] Portal internetowy „Fpiec", 28.06.2017 r. (www.fpiec.pl/post/2017/06/28/gloalntyatakghakersdd).
221. *Wirus Petya. Jak działa i czy naprawdę zagraża Polsce?,* 2017 *[w:]* Portal internetowy „Superbiz.se.pl", 28.06.2017, (http://superbiz.se.pl/wiadomosci-biz/wirus-petya-jak-dziala-i-czy-naprawde-zagraza-polsce_1006354.html).
222. WOJTASIK K., 2016. *Życie codzienne na terenach tzw. Państwa Islamskiego w przekazie jego oficjalnych mediów,* (w:) Media i Społeczeństwo. Medioznawstwo - komunikologia - semiologia - socjologia mediów - media a pedagogika, nr 6/2016, Bielsko-Biała.
223. WOJTASIK Ł.(red.) 2013. Biblioteka programu „Dziecko w Sieci" Fundacji Dzieci Niczyje, *Jak reagować na cyberprzemoc*. Poradnik dla szkół, wyd. II (dostęp: 2013 rok).
224. WOLANY L., 2016. *Informatyka najbardziej perspektywicznym kierunkiem studiów. W Polsce brakuje ok. 50 tys. specjalistów IT, a w UE ponad 270 tys.*, artykuł internetowy, newseria.pl. https://lifestyle.newseria.pl/newsy/kariera/informatyka_najbardziej,p1349645937.
225. WORONOWICZ B., 2012. *Uzależnienia. Geneza, terapia, powrót do zdrowia*, Rebis, Poznań.
226. *Yahoo Discloses 2013 Breach that Exposed Over One Billion Accounts,* 2016[in] portal internetowy firmy analitycznej "Trend Micro Security News", 15 grudnia 2016, (www.trendmicro.com/vinfo/us/security/news/cyber-attacks/yahoo-discloses-2013-breach-exposed-over-1billion-accounts).

227. YORK K., 2016. *Dyn Statement on 10/21/2016 DDoS Attack* [in] portal internetowy "Dyn", 22 październik 2016, (http://dyn.com/blog/dyn-statement-on-10212016-ddos-attack).
228. YOSSI O., 2006. *Remote Power Analysis of RFID Tags*, Scientific Council of the Weizmann Institute of Science Rehovot, Israel.
229. YOUNG B., 2016. *Data Breach Exposes Info for 400,000 Community Health Plan Members* [in] portal internetowy "The Seattle Times", 21 grudnia 2016, (www.seattletimes.com/seattle-news/health/data-breach-exposes-info-for-400000-community-health-plan-members).
230. ZIÓŁKOWSKI A., 2009. *Historia powszechna. Starożytność.* Wydawnictwo Naukowe PWN. Warszawa.
231. Наказ Національної поліції України № 85 від 10.11.2015. *Положення про Департамент кіберполіції Національної поліції України*, https://www.npu.gov.ua/uk/publish/article/1816252, доступ від 10.02.2017.
232. Повідомлення Департаменту комунікації Національної поліції України. *Поліція посилює заходи щодо розшуку зниклих дітей*, https://www.npu.gov.ua/uk/publish/article/2128566, доступ від 10.03.2017.

Netografia:

1. http://ec.europa.eu/COMMFrontOffice/publicopinion/index.cfm/Survey/getSurveyDetail/instruments/FLASH/surveyKy/2124.
2. http://gis.gov.pl/images/%C5%9Brodki_zast%C4%99pcze/%C5%9Bz/raport_eur._nar_2016.pdf.
3. http://man-ha.pionier.net.pl/pl/
4. http://mkuliczkowski.pl/static/pdf/slownik.pdf
5. http://orka.sejm.gov.pl/wydbas.nsf/0/aa1e06213f088c33c1257d0e00491563/$file/infos_173.pdf.
6. http://pbi.org.pl/patronaty/prywatnosc-w-sieci-raport-iab-polska/.
7. http://pbi.org.pl/raporty/polscy-internauci-kwietniu-2017-analiza/.
8. http://pl.blastingnews.com/polityka/2017/01/imigranci-przywlekli-grozne-choroby-gdy-kaczynski-ostrzegal-mowiono-to-rasizm-001438649.html.
9. http://pl.wikipedia.org/wiki/Informacja,
10. http://prawo.gazetaprawna.pl/artykuly/1030778,nowa-ustawa-o-ochronie-danych-osobowych.html.
11. http://prawo.gazetaprawna.pl/artykuly/921582,co-moga-sluzby-specjalne-ustawa-inwigilacyjna-ustawa-o-policji.html.
12. http://sde24.pl/Repozytorium/PolitykaCertyfikacjiSDE.pdf - dostęp 16.06.2017.
13. http://www.cbos.pl/SPISKOM.POL/2014/K_044_14.PDF
14. http://www.dozorelektroniczny.gov.pl/
15. http://www.dw.com/pl/europol-handlarze-narkotykami-aktywni-w-przemycie-ludzi/a-36999394.

16. http://www.dw.com/pl/niemcy-migranci-i-przest%C4%99pczo%C5%9B%C4%87/a-38446517.
17. http://www.ecteg.eu/courses.html.
18. http://www.europarl.europa.eu/poland/pl/strona_glowna/eurobarometr_1.html.
19. http://www.giodo.gov.pl/144/id_art/112/j/pl/.
20. http://www.info-migrator.pl/informacje-prawne/opisy-ustaw/3428-konwencja-genewska-z-28-lipca-1951-r-dotyczaca-statusu-uchodzcow.
21. http://www.pionier.net.pl/online/pl/jednostki/
22. http://www.platon.pionier.net.pl/online/.
23. http://www.polskatimes.pl/fakty/swiat/a/przemytnicy-pomagaja-uchodzcom-dostac-sie-do-europy-to-biznes-lepszy-niz-handel-bronia,9441109/.
24. http://www.ppbw.pl.
25. http://www.pulshr.pl/rekrutacja/bezrobocie-imigranci-emigracja-jak-wygladal-polski-rynek-pracy-w-2016-r,40236.html.
26. http://www.rp.pl/Uchodzcy/160119321-Grecja-oskarza-Turcje-o-przemyt-imigrantow.html.
27. http://www.rp.pl/Uchodzcy/304249891-Niemcy-Wzrost-przestepczosci-wsrod-mlodych-imigrantow.html.
28. http://www.sejm.gov.pl/prawo/konst/polski/2.htm.
29. http://www.sw.gov.pl/assets/22/14/77/288103de1e84b021bbd946b0f0a063a650bbda89.pdf
30. http://www.sw.gov.pl/assets/37/63/62/bf088ac03b4beb5926f552752e690b9faaa0651f.pdf

31. http://www.sw.gov.pl/assets/37/63/62/bf088ac03b4beb5926f552752e690b9faaa0651f.pdf
32. http://www.sw.gov.pl/assets/48/00/89/4da5d51548c25fb796040f4fc45b5e431bfa56f1.pdf
33. http://www.sw.gov.pl/assets/85/57/82/cb633cd8b291b9c58b80ddf40f7d597a7d91007f.pdf
34. http://www.sw.gov.pl/jednostka/biuro-dozoru-elektronicznego - dostęp 16.06.2017.
35. http://www.ucd.ie/cci/education/prospective_students/fcci_programmes.html.
36. http://www.unhcr.org/globaltrends2016/.
37. http://www.unhcr.org/pl/2858-wojny-przemoc-i-przesladowania-przyczyna-rekordowej-liczby-przymusowych-przesiedlen.html.
38. http://www.unhcr.org/pl/363-plwiadomosci2016653-mln-osob-przymusowo-przesiedlonych-kolejny-rekord-w-statystykach-html.html
39. http://www.unic.un.org.pl/unic-activities/spotkanie-wysokiego-szczebla-na-forum-zgromadzenia-ogolnego-na-temat-migracji-miedzynarodowych-i-rozwoju/862.
40. https://amnesty.org.pl/niemcy-wzrost-przestepstw-z-nienawisci/.
41. https://documents. trendmicro.com/assets/rpt-2016-annual-security-roundup-a-record-year-for-enterprise-threats.pdf
42. https://mc.gov.pl/aktualnosci/projekt-ustawy-o-ochronie-danych-osobowych.
43. https://mc.gov.pl/files/projekt_ustawy_o_ochronie_danych_osobowych_28.03.2017.pdf.

44. https://mc.gov.pl/files/strategia_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf.
45. https://panoptykon.org/wiadomosc/badania-co-polki-i-polacy-mysla-o-prywatnosci-w-sieci.
46. https://pl.wikipedia.org/wiki/Historia_Internetu_w_Polsce.
47. https://wiadomosci.wp.pl/inwigilacja-internetu-nie-tylko-w-polsce-jak-wyglada-kontrola-dzialan-sluzb-w-europie-6025256964621441a.
48. https://wiadomosci.wp.pl/migracja-w-skali-swiatowej-jest-zjawiskiem-pozytywnym-6036386656195713a.
49. https://wiadomosci.wp.pl/onz-migracja-szansa-na-polepszenie-zycia-6078989422130305a.
50. https://wp.tv/i,gigantyczny-przemyt-broni-do-ue-udaremniony,mid,1828277,cid,4051,klip.html?ticaid=619888.
51. https://www.cfreds.nist.gov/dfr-test-images.html.
52. https://www.cfreds.nist.gov/utf-16-russ.html.
53. https://www.europol.europa.eu/publications-documents/migrant-smuggling-in-eu.
54. https://www.facebook.com/cybercopua/.
55. https://www.honeynet.org/challenges/2010_2_browsers_under_attack.
56. https://www.honeynet.org/challenges/2011_7_compromised_server.
57. https://www.honeynet.org/node/504.
58. https://www.iab.org.pl/wp-content/uploads/2017/03/IAB_Polska_Prywatnosc_w_sieci_2016_2017_raport.pdf.
59. https://www.mr.gov.pl/media/36848/SOR_2017_maly_internet_03_2017_aa.pdf.

60. https://www.rootme.org/en/Challenges/Forensic/Logs-analysis-web-attack.
61. https://www.wprost.pl/529961/Grozna-choroba-wykryta-w-Danii-Zakazeni-to-imigranci.
62. www.aliexpress.com/price/long-range-rfid-reader_price.html.
63. www.atlasrfidstore.com/active-rfid/.
64. www.blackhat.com/us-13/briefings.html#Brown.
65. www.blackhat.com/us-15/briefings.html#breaking-access-controls-with-blekey.
66. www.gaorfid.com/devices/readers-by-feature/long-range-rfid-readers.
67. www.rfdump.org/.
68. www.rfidjournal.com/articles/view?2167.
69. www.technovelgy.com/ct/Technology-Article.asp?ArtNum=20.
70. www.trendmicro.com/vinfo /us/security/research-and-analysis/threat-reports/roundup
71. www.youtube.com/watch?v=BR-JXDdzCko.

Akty prawne:

1. Konwencja Dotycząca Statusu Uchodźców, sporządzona w Genewie dnia 28 lipca 1951 r. (Dz. U. z 1991 r. Nr 119, poz. 515 i 517).
2. Protokół dotyczący statusu uchodźców, sporządzony w Nowym Jorku dnia 31 stycznia 1967 r. (Dz.U. z 1991 r. Nr 119, poz. 517).
3. Konwencja Dublińska – podpisana 15 czerwca 1990 w Dublinie konwencja, wskazuje państwo odpowiedzialne za rozpatrywanie wniosków o azyl złożonych w jednym z PC UE.
4. Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. *w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej* - DU UE L210/1 z 2008 r.
5. Decyzja Rady 2008/616/WSiSW z dnia 23 czerwca 2008 r. *w sprawie wdrożenia* DECYZJI 2008/615/WSiSW *w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (zawierająca załącznik precyzujący parametry techniczne wymiany danych daktyloskopijnych, DNA i danych rejestracyjnych pojazdów)* – DU UE L210/12 z 2008 r.
6. Ustawa z dnia 25 lutego 1964 r. - Kodeks rodzinny i opiekuńczy (Dz.U. z 2017 r. poz.682.).
7. Ustawa z dnia 12 grudnia 2013 r. *o cudzoziemcach* (Dz.U. 2016 poz. 1990).
8. Ustawę z dnia 7 września 2007 r. *o wykonywaniu kary pozbawienia wolności poza zakładem karnym w systemie dozoru elektronicznego*. (Dz. U. z 2010 r. Nr 142, poz. 960, z późn. zm,).
9. Ustawie z dnia 29 stycznia 2004 r. *Prawo zamówień publicznych* (Dz.U. z 2015 t. poz. 2164 z późn. zm,)
10. Ustawa z dnia 27 lipca 2001 r. *o kuratorach sądowych* (Dz.U. 2001 nr 98 poz. 1071 z późn. zm.).
11. Ustawa z dnia 29 sierpnia 1997 r. *o ochronie danych osobowych* (Dz.U. 1997 nr 133 poz. 883 z późn. zm.)
12. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny* (Dz.U. 1997 nr 88 poz. 553 z późn. zm.).
13. Ustawa z dnia 6 czerwca 1997 r. *Kodeks karny wykonawczy* (Dz.U. 1997 nr 90 poz. 557 z późn. zm.).

Ustawa z dnia 29 sierpnia 1997 r. *Prawo bankowe* (Dz.U. 1997 nr 140 poz. 939 z późn. zm.)

14. Rozporządzenie Ministra Sprawiedliwości z dnia 10 października 2016 r. *w sprawie sposobu oraz szczegółowych warunków wykonywania kar, środków karnych i środków zabezpieczających w systemie dozoru elektronicznego* (Dz.U. 2016 poz. 1698).
15. Rozporządzenie Ministra Sprawiedliwości z dnia 10 października 2016 r. *w sprawie wzoru pisemnego pouczenia o przysługujących skazanemu prawach i ciążących na nim obowiązkach związanych z dozorem elektronicznym, jak również o konsekwencjach naruszenia tych obowiązków* (Dz.U. 2016 poz. 1692)
16. Rozporządzenie Ministra Sprawiedliwości z dnia 10 października 2016 r. *w sprawie sposobu i trybu sprawowania nadzoru nad wykonywaniem dozoru elektronicznego* (Dz.U. 2016 poz. 1700).
17. Rozporządzenie Ministra Sprawiedliwości z dnia 26 maja 2015 r. *w sprawie określenia szczegółowych warunków technicznych i wymagań funkcjonalnych, jakie powinny spełniać środki techniczne służące do wykonywania dozoru elektronicznego, oraz sposobu funkcjonowania systemu komunikacyjno-monitorującego* (Dz.U. 2015 poz. 797).
18. Rozporządzenie Ministra Sprawiedliwości z dnia 28 maja 2015 r. *w sprawie sposobu archiwizowania oraz sposobu i trybu usuwania danych osobowych i informacji zarejestrowanych w związku z wykonywaniem dozoru elektronicznego* (Dz.U. 2015 poz. 800).
19. Rozporządzenie Ministra Sprawiedliwości z dnia 3 czerwca 2015 r. *w sprawie wysokości opłaty wyrównawczej dla nadajnika i rejestratora stacjonarnego lub przenośnego służących do wykonywania dozoru elektronicznego* (Dz.U. 2015 poz. 813).
20. Rozporządzenie Parlamentu Europejskiego i Rady (UE) Nr **603/2013**z dnia 26 czerwca 2013 r. *w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania* rozporządzenia (UE) NR 604/2013 *w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego*

lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego oraz zmieniające Rozporządzenie (UE) NR 1077/2011 *ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości* - DU UE L180 z 2013 r.

21. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. *w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych* (Dz.U. 2012 poz. 526)
22. Komisja Nadzoru Finansowego, 2013. *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*.

Wykaz rysunków:

Wykaz tabel:

Sylwia Gwoździewicz doktor prawa (Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie), absolwentka menedżerskich studiów podyplomowych w zakresie zarządzania zasobami ludzkimi (Uniwersytet Warszawski) i menadżera innowacji (Szkoła Główna Handlowa). Przez wiele lat pełniła funkcję Kanclerza Wyższej Szkoły Nauk Społecznych w Mińsku Mazowieckim; dyrektora Instytutu Nauk Medycznych, Dyrektor Instytutu Nauk Społecznych Wyższej Szkoły Przedsiębiorczości w Warszawie; dyrektora Wyższej Szkole Gospodarki Euroregionalnej w Józefowie. Organizator i inicjator wielu konferencji naukowych w tym międzynarodowych z jednostkami naukowymi, samorządowymi i biznesowymi na terenie województwa mazowieckiego. Koordynator pierwszego Forum Gospodarczego Powiatu Otwockiego. Redaktor naczelna czasopisma pt. "International Journal of Legal Studies"; zastępca redaktora naczelnego czasopisma pt. "International Journal of New Economics and Social Sciences", recenzent uniwersyteckiego czasopisma pt. „Kortowski Przegląd Prawniczy" oraz członek rady naukowej czasopisma Ukraińskiej Akademii Technologicznej w Kijowie pt. „Public management". Zainteresowania naukowe: cyberbezpieczeństwo i cyberprzestępczość; prawne aspekty bezpieczeństwa i cyberbezpieczeństwa oraz przestępstw przeciwko ochronie informacji, danych osobowych, własności intelektualnej oraz tajemnicy przedsiębiorstwa.

Krzysztof Tomaszycki – młodszy inspektor doktor inżynier, doktor nauk społecznych w zakresie socjologii (Wydział Nauk Społecznych Uniwersytetu Wrocławskiego), absolwent studiów podyplomowych: Analityk zarządzania (Instytut Organizacji i Zarzadzania w Przemyśle „Orgmasz") i Zarządzanie jednostką organizacyjną w administracji publicznej (Wyższa Szkoła Policji w Szczytnie). Wieloletni kierownik Zakładu Daktyloskopii Centralnego Laboratorium Kryminalistycznego Policji, obecnie radca w Wydziale Zarządzania Projektami Biura Łączności i Informatyki Komendy Głównej Policji w Warszawie. Organizator i inicjator wielu konferencji naukowych w tym międzynarodowych: 100 lat daktyloskopii na ziemiach polskich, Bezpieczeństwo kulturowe a zagrożenia terroryzmem. Członek rad naukowych konferencji międzynarodowych i krajowych: Zadania jednostek administracyjnych samorządu terytorialnego z wykorzystaniem potencjału grup dyspozycyjnych w przezwyciężaniu zagrożeń bezpieczeństwa publicznego, Współpraca samorządu terytorialnego oraz grup dyspozycyjnych w zapewnianiu bezpieczeństwa społeczności lokalnych, Handel ludźmi. Zagrożenie współczesnego bezpieczeństwa. Redaktor tematyczny „International Journal of New Economics and Social Sciences", recenzent czasopism: Security, economy & law, Ekonomika i organizacja przedsiębiorstwa oraz członek rady naukowej czasopisma Kultura bezpieczeństwa Nauka-Praktyka-Refleksje. Zainteresowania naukowe: socjologia grup dyspozycyjnych, kryminalistyka, kryminologia, społeczne aspekty bezpieczeństwa, migracja, zwalczanie terroryzmu oraz cyberbezpieczeństwo i cyberprzestępczość. Praktyk, kryminalistyk, biegły z zakresu badań daktyloskopijnych.

ISBN 978-83-945923-2-5