ROCZNIKI NAUK SPOŁECZNYCH
Tom 16(52), numer 1 – 2024
DOI: https://doi.org/10.18290/rns2024.0005

WALDEMAR SCHEFFS

BEZPIECZEŃSTWO UŻYTKOWANIA URZĄDZEŃ MOBILNYCH PODCZAS KONFLIKTU ZBROJNEGO*

SAFETY OF USING MOBILE DEVICES DURING ARMED CONFLICT

A b s t r a c t. The study presents the problem of the lack of safety rules for using mobile telecommunications devices, i.e. smartphones, smartwatches, mobile phones during military operations. Despite its many advantages, the mobile phone also poses a threat to people and their surroundings during military operations. Attention was focused on the lack of developed safety rules and on available methods of locating the device. At the same time, attention was paid to how easy it is to track a phone and a person during an armed conflict. The advisability of owning and using secured mobile devices by persons responsible for managing state and military administration was indicated. A separate place was devoted to the awareness of people using mobile devices who may, through unintentional correspondence, provide important information to the opposing party. Practical solutions and conclusions resulting from a similar situation in Ukraine during the ongoing armed conflict were also indicated.

Keywords: Mobile telecommunications devices; GPS location; armed conflict; mobile telephony security.

WPROWADZENIE

Szeroki kontekst postrzegania wielu kwestii związanych z zagrożeniami, odnoszący się do bezpieczeństwa obywateli podczas konfliktu zbrojnego, podlega ciągłym przeobrażeniom. Zauważalne zmiany wynikają ze stylu życia obywateli, ich swobód, postępujących procesów globalizacyjnych, procesów rozwoju i wdrażania nowych technologii, szczególnie informatycznych, oraz

Dr hab. WALDEMAR SCHEFFS – Uniwersytet Kaliski im. Prezydenta Stanisława Wojciechowskiego, Instytut Nauk o Bezpieczeństwie; adres do korespondencji: ul. Nowy Świat 4, 62-800 Kalisz; e-mail: w.scheffs@uniwersytetkaliski.edu.pl; ORCID: https://orcid.org/0000-0002-3720-5806.

* W całym opracowaniu pojęcia: telefon komórkowy, smartfon, smartwatch będą stosowane zamiennie i traktowane ogólnie jako mobilne urządzenia telekomunikacyjne.

umiędzynarodowienia zjawisk społeczno-ekonomicznych, które wpływają na wiele kwestii związanych z postrzeganiem zagadnień bezpieczeństwa i obronności kraju w różnych jej aspektach.

Kwestie bezpieczeństwa społeczeństwa podczas konfliktu zbrojnego od dawna uważane są jako priorytetowe, ale nie zawsze dostatecznie eksponowane. Przykładem jest edukacja społeczeństwa mająca odnosić się do właściwych postaw i reakcji społecznych na zagrożenia podczas trwania konfliktu zbrojnego, która właściwie jest marginalizowana. Można postawić tezę, że czujność społeczeństwa na zagrożenia w odniesieniu do działań zbrojnych została uśpiona poczuciem spokoju. Problem zagrożeń militarnych został rozmyty w obszarach konsumpcyjnego życia społecznego. Ta teza nie powinna budzić zdziwienia. Społeczeństwo polskie rozwija się, bogaci, zdobywa nowe doświadczenia, a rządzący państwem stwarzają warunki dla bezpiecznej egzystencji jej społeczeństwa. Obecnie wskaźnikiem większego zainteresowania społeczeństwa sprawami obronnymi są wydarzenia wojenne na wschodzie Europy (wojna rosyjsko-ukraińska) i konflikt w Strefie Gazy.

Doświadczenia wojenne dotyczące wpływu nowoczesnej technologii militarnej i niemilitarnej na zachowania i życie ludności, powinny zaowocować z jednej strony większą sprawnością korzystania z nowoczesnego sprzętu teleinformatycznego (mobilnych urządzeń komunikacji) przez społeczeństwo, a z drugiej większym poczuciem odpowiedzialności za ich używanie podczas działań zbrojnych. Nowe technologie, mimo swoich niewątpliwie wielu zalet, stanowią duże źródło zagrożeń. Szkodliwość odnosi się nie tylko do sposobu użytkowania, lecz także do czasu i miejsca użycia sprzętu teleinformatycznego, wieku użytkowników oraz rodzajów i sposobów przekazu informacji, przeciwnik bowiem dysponuje sprzętem pozwalającym na wykrycie, przechwycenie i lokalizację naszych urządzeń teleinformatycznych, a w konsekwencji ma możliwość oddziaływania środkami elektromagnetycznymi i ogniowymi w miejsce lokalizacji – tam będzie człowiek.

Przedstawiona sytuacja problemowa jest wynikiem obserwacji przebiegu konfliktów z pierwszych dekad XXI wieku, analizy treści informacji z doniesień z konfliktów umieszczanych na portalach informacyjnych, a także z przekazów treści serwisów informacyjnych w telewizji i z materiałów źródłowych. Jednocześnie wykorzystano doświadczenia autora jako specjalisty walki radioelektronicznej. Celem artykułu jest wskazanie konieczności opracowania zasad bezpieczeństwa i podniesienia świadomości proobronnej społeczeństwa polskiego, związanej z rozważanym używaniem mobilnych urządzeń telekomunikacyjnych w warunkach konfliktu zbrojnego w nowej rzeczywistości informatycznej. Problem ujęto

w pytaniu: Dlaczego powinno się uczyć społeczeństwo bezpiecznego korzystania z mobilnych urządzeń komunikacyjnych podczas konfliktu zbrojnego w warunkach nowoczesnego środowiska informatycznego? Przyjęte założenie badawcze wskazuje, iż można postawić następującą tezę: społeczeństwo polskie powinno być uświadamiane jak stosować zasady bezpiecznego korzystania z mobilnych urządzeń telekomunikacji nie tylko w czasie pokoju, ale również podczas stanu zagrożenia wojennego i wojny, zarówno w aspektach ochrony własnego życia, jak i na potrzeby systemu obronnego państwa.

Z obserwacji wynika, że wysoka świadomość korzystania z mobilnych urządzeń telekomunikacyjnych odnosi się tylko do warunków stabilnej sytuacji polityczno-militarnej. Natomiast, gdy występują zagrożenia związane z konfliktem zbrojnym, wiedza co do zagrożeń jest niska i nie występuje poczucie dyskomfortu bezpieczeństwa. Taka sytuacja sprawia, że osoby posługują się bezkrytycznie swoimi urządzeniami teleinformatycznymi monitorując i zapisując wszelkie zdarzenia związane działaniem wokół siebie. Zaobserwowane wydarzenia umieszczają w portalach społecznościowych chwaląc się osiągnięciami. Brak wiedzy, a często wyobraźni o skutkach swoich działań, np. związanych z ujawnieniem informacji o ataku rakietowym przeciwnika lub miejsc postoju sprzętu wojskowego, może narazić życie ich i wielu osób znajdujących się w pobliżu.

Obserwując charakter obecnie toczących się wojen, stwierdzić należy, że jest to wojna, która przyjęła naturę wojny barbarzyńskiej z permanentną inwigilacją i oddziaływaniem systemami rażenia rakietowego, walki informacyjnej, radioelektronicznej, dezinformacji oraz propagandy, w której cel ataku staje się aż nadto wyrazisty – ludność cywilna.

METODY PODSŁUCHU URZĄDZEŃ MOBILNYCH

O bezpieczeństwie użytkowania telefonów, smartfonów, tabletów wpływających na rozwój i zachowanie dzieci, młodzieży i dorosłych napisano już wiele opracowań (Burke, 2021; Pieleszek, 2018), odbyło się wiele szkoleń, prelekcji. Czy jednak zawsze pamiętamy o przestrzeganiu przekazanych nam zasadach bezpieczeństwa?

Społeczną ułomność braku przestrzegania zasad bezpieczeństwa używania telefonu komórkowego często wykorzystują służby wywiadowcze, hakerzy na usługach służb, pododdziały rozpoznania cybernetycznego, których zadaniem jest wykrycie i przechwycenie informacji o osobach zapewniających bezpieczeństwo innym obywatelom w czasie konfliktu zbrojnego. Dlatego problem podsłuchu

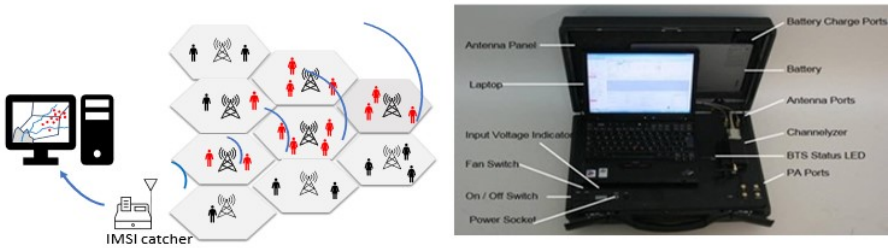
i lokalizacji telefonu komórkowego nabiera znacznie większego znaczenia. Telefon, smartfon lub inne urządzenie może stanowić źródło zagrożenia życia dla danej osoby i osób znajdujących się w jej otoczeniu. Przeciwnik, wykorzystując różne systemy oddziaływania (ogniowe, atak bezzałogowym statkiem powietrznym – BSP, atak EM, dezinformacja), będzie starał się destabilizować funkcjonowanie nie tylko pojedynczych osób, lecz także całego społeczeństwa.

Stałe monitorowanie systemów telekomunikacyjnych przez przeciwnika, szczególnie przez systemy radioelektroniczne i informatyczne, nie powinno zaskakiwać, ponieważ zasady rozpoznania strony przeciwnej były stosowane jak tylko ludzie zaczęli prowadzić wojny między sobą. Bieżące konflikty, a także przyszłe, nie będą pomijały tych zasad. Zmienią się tylko narzędzia i sposoby zdobywania informacji, rozszerzy się zasięg i krąg osób, którymi zainteresowany będzie przeciwnik. Większa uwaga skupiona będzie na osobach funkcyjnych, na których przeciwnikowi szczególnie zależy. Z uwagi na ich pozycję w strukturach administracji państwowej lub w wojsku będą nieustannie monitorowane i namierzane, a te procesy rozpoczną się na długo przed rozpoczęciem działań zbrojnych. Czas prowadzenia działań zbrojnych to potwierdzenie ich lokalizacji w danym terenie i dalsza kontrola działalności. Wybuch wojny może spowodować, że część osób funkcyjnych zmieni miejsca przebywania, wymieni środki telekomunikacji, zastosuje sposoby lub urządzenia maskujące łączność itd. Będą to standardowe procedury na wypadek wojny dla osób funkcyjnych. Nie wszystkie osoby i instytucje zostaną objęte ochroną systemów bezpieczeństwa. Część będzie pozbawiana tej ochrony, chociażby z powodu dużej liczby ludzi podlegających ochronie. To one będą w dużej mierze podlegać infiltracji przez systemy rozpoznawcze przeciwnika.

Wśród sposobów zdobywania informacji przez systemy rozpoznania (wywiadu) przeciwnika wyróżniamy: przechwytywanie komunikacji abonentów po wcześniejszym odpowiednim rozpoznaniu osób; namierzanie urządzenia mobilnego, czyli wskazanie jego lokalizacji. Na bazie oceny sytuacji operacyjnej decydenci strony przeciwnej zdecydują, które źródło informacyjne (telefon, smartfon) będzie monitorowane systemem rozpoznania radioelektronicznego, a które przez systemy informatyczne lub inne. Decydenci podejmą także decyzję, czy będą stosować zakłócanie elektromagnetyczne (EM), czy użyją w stosunku do tego źródła, a zarazem osoby nim się posługującej, inne działania, np.: dezinformacyjne, propagandowe lub oddziaływanie środkami niszczenia fizycznego (np. rakieta, BSP).

Komunikację za pomocą telefonu komórkowego można podsłuchać na (co najmniej) trzy różne sposoby (Konieczny, 2013):

1. Podsłuch telefonu na warstwie protokołów komunikacji GSM. Metoda wymaga obecności podsłuchującego z fałszywym urządzeniem BTS (ang. *Base Transceiver Statio* – fałszywa stacja bazowa) w obrębie właściwego BTS ofiary, czyli miejsca, gdzie telefon się loguje. Fałszywa stacja bazowa to tzw. Międzynarodowy moduł wykrywający tożsamość abonenta mobilnego (ang. *International Mobile Subscriber Identity-Catcher* – IMSI Catcher), popularnie zwany jaskółką. Moduł zastępuje właściwy nadajnik podszywając się pod jego parametry techniczne. Włączenie modułu IMSI Catcher powoduje, że telefony komórkowe będące w okolicy wieży właściwej zauważają, iż pojawił się mocniejszy sygnał sieci i przekierowują się na fałszywy nadajnik. Fałszywy nadajnik z kolei łączy się z oryginalną siecią, aby przechwycone komórki mogły wykonywać i odbierać połączenia (rysunek 1). Jest to klasyczny atak *Man in the Middle*, czyli będący w środku komunikacji. Fałszywy BTS nie musi łamać szyfrowania protokołów sieci GSM, bowiem wymusza brak szyfrowania połączeń, korzystając z tego, iż większość telefonów komórkowych w żaden sposób nie sygnalizuje swojemu właścicielowi, że podłączyło się do sieci GSM bez szyfrowania. Brak szyfrowania pozwala fałszywemu BTS-owi na podsłuchiwanie rozmów, SMS-ów, transmisji pakietowej (Internet). Transmisje osób można nagrywać i namierzać, nawet gdy zmieniły telefon (ale korzystają z tej samej karty), zmieniły kartę SIM (ale korzystają z tego samego telefonu) albo zmieniły kartę SIM i telefon jednocześnie (ale dalej wykonują połączenia na te same numery).



Rysunek 1. Przykład zastosowania IMSI Catcher
i jego faktyczny widok w postaci przenośnej firmy Verint GI2

Źródło: Dudek, 2018; Řezník, Horáková i Szturc, 2015.

2. Podsłuch telefonu na warstwie innej niż GSM protokołów komunikacyjnych, np. poprzez interfejs sieci bezprzewodowych Wi-Fi. W tym przypadku wykorzystuje się interfejsy Wi-Fi tych użytkowników telefonów, którzy nie wyłączają tej funkcji, kiedy przestają korzystać z sieci bezprzewodowej. Telefon,

mimo że jest wyłączony, co jakiś czas skanuje okolicę w poszukiwaniu nazwy najbliższej sieci Wi-Fi (ang. *Service Set Identifier – SSID*), z której już kiedyś korzystał. Jeżeli ją rozpozna (np. poprzez hotspot poczty, księgarni) to łączy się automatycznie. Po nawiązaniu połączenia uruchamiają się aplikacje, które synchronizują wiadomości np. z poczty i Messengera lub inne ostatnio używane. W tym ataku wykorzystywany jest zaimplementowany fałszywy *access point*. Aplikacja wykrywa znane jej sieci Wi-Fi, do których dana osoba się logowała i automatycznie uruchamia fałszywe *access pointy*. Telefon identyfikuje je jako znajomą sieć. Przejęty ruch internetowy jest dodatkowo uwierzytelniany szybszą obsługą lub nawet modyfikacją prób połączenia do stron z protokołem HTTPS, zmieniając ruch na strony z protokołem HTTP (warunek konieczny do takiego ataku to źle skonfigurowany telefon ofiary).

3. Podsłuch telefonu na warstwie (złośliwej) aplikacji. Metoda odbioru i nagrywania rozmów oraz SMS-ów odbywa się poprzez wcześniej nieświadomie lub świadomie (przez atakującego) zainstalowaną dedykowaną aplikację podszywającą się pod znany program, np. sklep. Pozostawienie telefonu bez opieki na jakiś czas, jest jedną z przyczyn celowego instalowania takich aplikacji. Innym sposobem ataku jest nieświadomy odbiór SMS-a, który jest złośliwą aplikacją przekierowującą telefon na spreparowaną stronę internetową z poziomu przeglądarki w telefonie. Służby wywiadowcze muszą tak zaprojektować aplikacje śledzące, żeby przechwyt informacji następował podczas korzystania z mikrofonu lub głośnika, a zapis informacji, które ofiara mówi, pisze, a nawet o tym, że wykonuje zdjęcia był odbierany poza szyfrowaniem transmisji. Co oznacza, że szyfrowanie nie ma wpływu na przechwycenie informacji, ponieważ odbywa się ono na końcówce kryptograficznej, czyli przed zaszyfrowaniem i po rozszyfrowaniu słów ofiary.

W praktyce występują jeszcze inne sposoby podsłuchu rozmów telefonicznych. Jedną z nich jest podsłuch na łączach operatorskich. W tym celu wykorzystuje się połączenia przewodowe stacji BTS z centralą GSM (niekiedy z wykorzystaniem infrastruktury internetowej). Warunkiem takiego podsłuchu jest obecność telefonu atakowanego w zasięgu danego BTS, gdzie zainstalowano sondy podsłuchowe. W tym wypadku znajomość nawyków osób, które podlegają inwigilacji jest jednym z warunków skutecznego przechwycenia. Poprzez obserwację wywiadowczą ustala się zachowania i nawyki danej osoby i instaluje sondy podsłuchowe w miejscach najczęściej odwiedzanych, gdzie może nastąpić skuteczne przechwycenie informacji. Należy w tym przypadku zaznaczyć, że w warunkach przygotowania przeciwnika do wojny realizuje on te zadania z dużym wyprzedzeniem.

Z oczywistych względów służby nie chwalą się swoją działalnością. Niemiej jedną z głośniejszych spraw związanych z wykorzystaniem złośliwych aplikacji śledzących jest tzw. inwigilacja za pomocą programu Pegasus lub podobnych. Rynek IT oferuje wiele różnych programów (oczywiście nie każdego na to stać) legalnych i nielegalnych. Inna sprawa, że takie nielegalne oferty często mają zupełnie legalne zastosowanie przez działające firmy – na przykład wywiadownie gospodarcze. Media często informują opinię publiczną o wykrytej inwigilacji, gdzie specjalistyczne firmy zajmujące się cyberprzestępczością wykrywają nielegalne śledzenie. Przykładem jest m.in. inwigilacja prezydenta Sopotu czy jego zastępcy (Madejski, 2023). Takich przykładów jest oczywiście znacznie więcej. Skuteczność nowoczesnego sprzętu rozpoznania radioelektronicznego, podsłuchowego lub monitorującego jest tak wysoka, że przekazy informacyjne dotyczące przechwytywania, rozpoznania i lokalizacji mogą odbywać się na bieżąco (McDermott, 2019, 2020; Creery, 2019).

NAJPOPULARNIEJSZE METODY LOKALIZACJI TELEFONÓW

Mobilne urządzenia telekomunikacyjne namierzamy z co najmniej dwóch powodów: pierwszy, gdy zgubiliśmy telefon, a drugi, gdy celowo poszukujemy urządzania (danej osoby). W obu przypadkach należy odpowiednio przygotować się do lokalizacji urządzenia. Oznacza to, że o bezpieczeństwo swojego telefonu należy zadbać jeszcze przed jego zgubieniem lub próbą namiaru przez systemy namierzania przeciwnika.

Do podstawowych metod lokalizujących telefony komórkowe, smartfony lub inne urządzenia mobilne wykorzystujące dostęp do Internetu można uznać te, które wykorzystują usługę GPS, czyli lokalizację przez konto Google lub iCloud. Telefony komórkowe (smartfony) z systemem operacyjnym Android najprościej zlokalizować używając konta Google. Użytkownik, w chwili dokonywanej operacji musi być powiązany z kontem Google i mieć włączoną lokalizację oraz czynne łącze z siecią. W przypadku intruza (wywiadowcy, hakera) lokalizacja w opisany sposób będzie nieco utrudniona, z uwagi na brak wielu danych logowania dostępnych tylko posiadaczowi telefonu, a poza tym atakujący musi uzyskać bezpośredni dostęp do jego konta. Jest to sytuacja, w której śledzona osoba już jest pod kontrolą służb wywiadowczych posiadających pełny dostęp do danych telefonu. Podobny sposób lokalizacji telefonu można dokonać w przypadku telefonów typu iPhone.

Nieco odmiennym sposobem lokalizacji urządzenia mobilnego jest wykorzystanie funkcji wirusów na telefon. Korzystamy wówczas z modułu antykradzieżowego lub funkcji *Anti-Theft* – nazwa zależy od antywirusa, jednak zasada działania jest taka sama. Zainstalowane aplikacje mają różne możliwości. Przykładowo *Bitdefender Mobile Security* umożliwia: zlokalizowanie telefonu na mapie, zdalne blokowanie urządzenia, zdalne czyszczenie (przywrócenie do ustawień fabrycznych), krzyk (głośny alarm). Aplikacje komercyjne można przeprogramować na potrzeby służb wywiadowczych. Wymaga to jednak czasu, wiedzy i środków niezbędnych do wykonania zdania. Dedykowany program antywirusowy musiałby wówczas być dostępny dla wielu osób nie budząc podejrzeń. Praktyczne jego użycie wydaje się dość kłopotliwe. Wymaga zastosowania socjotechnicznych czynności wobec ofiary, a rozpoczęcie akcji powinno wystąpić na długo przed działaniami zbrojnymi. Ten sposób lokalizacji opłacalny będzie w przypadku bardzo ważnych osób w monitorowanym państwie. Odmianą takiego rozwiązania może być sposób jaki wykorzystuje się do kontroli rodzicielskiej. Wówczas instalacja wirusa jest na telefonie ofiary i szpiega. Takie rozwiązanie pozwoli śledzić lokalizację ofiary w dowolnym momencie.

Jednym z prostszych sposobów lokalizacji telefonu jest wykorzystanie znanego położenia stacji bazowej BTS. Lokalizacja telefonu komórkowego polega na pomiarze siły sygnału pomiędzy BTS, a lokalizowanym telefonem. Warunkiem koniecznym jest przebywanie osoby z telefonem w zasięgu przynajmniej trzech stacji bazowych, co pozwoli na zastosowanie metody triangulacji do wyznaczenia położenia urządzenia (rysunek 2).

Rysunek 2. Określanie lokalizacji mobilnego urządzenia z wykorzystaniem stacji BTS

Źródło: Řezník, Horáková i Szturc, 2015.

Telefon komórkowy można zlokalizować także po numerze IMEI (ang. *International Mobile Equipment Identity*). Numer IMEI może posłużyć do zablokowania telefonu oraz do jego odnalezienia. Jest to 15-cyfrowy kod zapisany w różnych miejscach telefonu (np. na opakowaniu, koło baterii, z tyłu obudowy lub w ustawieniach urządzenia). Dokonując lokalizacji korzysta się ze specjalnej aplikacji, np. IMEI Number Checker 2021. Aplikację można kupić ze sklepu internetowego i zainstalować, ale dla celów wywiadowczych bardziej celowym jest odpowiednio przygotowaną aplikację zainstalować na telefonie ofiary. Jest to metoda niedoskonała i podobnie jak w opisanych wcześniej przypadkach wymagająca uprzedniego przygotowania i obserwacji czynności codziennych ofiary.

Do określenia położenia użytkownika telefonu komórkowego nie jest potrzebny dostęp do systemu GPS, wystarczy śledzić różnice w poborze mocy smartfona, czyli stan naładowania baterii (Curry, 2015). Nie są do tego potrzebne żadne uprawnienia, a więc każda aplikacja może „po cichu" lokalizować telefon i jego użytkownika w przestrzeni z 90-procentową skutecznością. Odczyt poboru mocy urządzenia bazuje na odległości telefonu od BTS-ów (im dalej, tym więcej mocy potrzebuje nadajnik telefonu). Według tej zasady można zmapować daną trasę pod kątem poboru mocy telefonu w danych obszarach, następnie badać (korzystając z aplikacji) poziom mocy, a w konsekwencji – sprawdzać, czy charakterystyka jego poboru odpowiada uprzednio zmapowanej trasie.

Wykorzystując tę metodę musimy liczyć się z dwoma ograniczeniami. Pierwsze dość zasadnicze – ktoś lub urządzenie rozpoznawcze, wcześniej musi „zmapować" pobór mocy wysyłany przez urządzenie na danej trasie, musi więc być obecny w obszarze danego BTS. Drugie to zakłócenia elektromagnetyczne (EM) spowodowane np. włączeniem w smartfonie odtwarzacza muzyki, który dodatkowo obciąża baterię i wprowadza anomalię lub włączeniem silniejszego urządzenia promieniującego EM w pobliżu danej osoby, co zakłóca pracę urządzenia i powoduje większe zużycie mocy baterii.

Ze względu na ograniczenia stacji ruchomych związanych z dostępnymi systemami zasilania (czas pracy urządzenia) oraz kosztów budowy systemów namierzania, do celów lokalizacji stacji ruchomych nie można stosować radionawigacji do namierzania. Dlatego telefonia komórkowa musi się ograniczyć do mniej dokładnych technik lokalizacyjnych, wykorzystujących dostępne zasoby funkcjonalne. Metod lokalizacji użytkowników w sieci jest wiele (zob. Simon, 2007; Kabaciński i Żal, 2013, s. 124-125; Simon i Walczyk, 2002).

Wskazując złożoność problemu nie sposób pominąć czynnika ludzkiego, który należy traktować jako najsłabsze ogniwo w systemie komunikacji. Przeciwnik nie zawsze musi włamywać się do telefonów komórkowych należących do

przedstawicieli rządu lub wyższych rangą dowódców wojskowych czy funkcjonariuszy. Nie musi także przełamywać zaawansowanych zabezpieczeń systemów telekomunikacyjnych używanych przez administrację lub wojsko. Dysponując odpowiednio dużą liczbą analityków oraz mając dostęp do masowej wymiany informacji, narzędziami białego wywiadu (OSINT) opierającego się na mediach społecznościowych, jest w stanie wykryć i namierzyć każdą osobę. Wyniki analiz często zaskakują samych analizujących. Potwierdzeniem tej tezy są artykuły po dokonanych śledztwach, przykładowo informacje o zestrzeleniu pasażerskiego odrzutowca MH17 przez separatystów rosyjskich (ujawniono nagrania obsługi broni) (*Katastrofa samolotu MH17*, 2023). Analiza zdjęć umieszczanych w Internecie pozwoliła na wskazanie osób odpowiedzialnych za tę katastrofę. Dokonana analiza śledcza wykazała skuteczność narzędzi białego wywiadu. Oczywiście czas lokalizacji danej osoby będzie znacznie dłuższy, ale należy oszacować skuteczność prowadzonego rozpoznania w stosunku do czasu i poniesionych nakładów oraz efektu jaki przeciwnik pragnie osiągnąć.

BEZPIECZEŃSTWO UŻYTKOWANIA URZĄDZEŃ MOBILNYCH – OGÓLNE ZASADY

Stan pokoju i zagrożenia kryzysowego cechuje się stabilnością przekazów informacyjnych zarówno w sieciach informatycznych, jak i telekomunikacyjnych. Z kolei stan wojny to duża niepewność poprawności działania tych sieci, spowodowana dużą niewiedzą na temat właściwego użytkowania mobilnych urządzeń telekomunikacyjnych, aby nie narazić na niebezpieczeństwo siebie i ludzi wokół. Bezmyślność w przekazie informacji (multimedialnych, tekstowych) w bezpośredniej bliskości prowadzonej walki to poważne zagrożenie nie tylko dla danej osoby, lecz także dla wszystkich osób przebywających w jej otoczeniu. Zakładając, że ciekawska osoba filmuje przebieg walki i na żywo transmituje działania, ujawnia w ten sposób pozycje obronne swoich żołnierzy i staje się źródłem informacji dla strony przeciwnej. Systemy rozpoznania radioelektronicznego przeciwnika mogą bowiem przechwytywać te transmisje, lokalizując jednocześnie telefon, co w konsekwencji może spowodować skierowanie ognia artylerii, rakiet lub BSP w zlokalizowane miejsce. Brak świadomości, wagi i konsekwencji wykonywanych filmików, rozmów, zdjęć w przekazie telekomunikacyjnym stanowi poważne zagrożenia nawet dla całych zgrupowań wojsk.

W Polsce edukacja dotycząca bezpieczeństwa telekomunikacyjnego ukierunkowana jest głównie na aspekty ochrony danych osobowych, danych bankowych,

wizerunkowych. Natomiast brakuje informowania społeczeństwa o zagrożeniach militarnych, szczególnie gdy rozpatrujemy współczesne środowisko teleinformatyczne. Programy edukacyjne prezentowane m.in. w telewizji Polsat[1] (krótkie spoty reklamowe) informują, a zarazem uczą społeczeństwo zasad bezpiecznego użytkowania telefonu komórkowego (nie odbieraj podejrzanych SMS-ów, nie otwieraj nieznanych linków w poczcie internetowej) tylko w odniesieniu do okresu „tu i teraz", brak edukacji jak zachowywać się w przyszłości, gdy zaistnieje zagrożenie wojną lub bardzo poważnym kryzysem. Emitowane programy edukacyjne dla dzieci zwracają uwagę na właściwe korzystanie z telefonu komórkowego, ale w odniesieniu do ich zdrowia i bezpieczeństwa osobistego. One również odnoszą się do sytuacji stabilnej i bezpiecznej. Nie należy jednak demonizować, że grozi nam konflikt zbrojny i musimy stosować inne zasady użytkowania telefonów komórkowych. Jednakże sytuacja za wschodnią granicą Polski oraz wydarzenia na granicy polsko-białoruskiej wskazują na próby destabilizacji sytuacji bezpieczeństwa, a to już jest przesłanką do wdrażania procedur propedeutycznych w społeczeństwie, do których nie jesteśmy aktualnie przygotowani.

Zagrożenia teleinformatyczne w czasie pokoju dotyczą głównie trzech obszarów: zdrowia, finansów i wizerunku. Każdy z tych obszarów szeroko opisany jest w literaturze i szeroko komentowany już od szkoły podstawowej. Zasady są wypracowane, ale jak już wspominano, nie przestrzegane. W książce *Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów* autorzy wykazują na trzy inne obszary zagrożeń: prywatność, informacje i technologie (Rywczyńska i Wójcik, 2018, s. 63-91). Wskazane obszary również podnoszą kwestie bezpieczeństwa użytkowania telefonów komórkowych w czasie stabilnej sytuacji polityczno-militarnej, nie wykazując zagrożeń związanych z niebezpieczeństwem działań zbrojnych.

Popularną formą oszustw internetowych jest *phishing* (połączenie angielskich słów *password harvesting* oraz *fishing* – łowienie haseł) (Grzelak i Liedel, 2012, s. 125-139). Skuteczność metod socjotechnicznych opiera się na zaufaniu, jakie internauci okazują znanym instytucjom lub osobom. Niejednokrotnie okazuje się, że użytkownicy sieci z pośpiechu lub lenistwa wolą jak najszybciej kliknąć w link/ikonę, zamiast zastanowić się, czy jest to działanie bezpieczne.

Urządzenia mobilne, głównie smartfony, to „przyjaciele młodzieży", bez których młodzi ludzie nie wyobrażają sobie funkcjonowania. Dla dorosłych to raczej urządzenia służące do komunikacji i pracy oraz załatwiania bieżących

[1] Spoty edukacyjne dotyczące bezpiecznego używania telefonów komórkowych i odbieranej poczty internetowej ukazują się od września 2023 r. głównie w telewizji Polsat.

spraw np. finansowych; dla starszych osób to nadal podstawowa forma komunikacji z elementami wizualizacji rozmówcy jako dodatkowy wymiar rozmowy. Użytkownicy korzystają z urządzeń mobilnych stosownie do swoich przyzwyczajeń, zwyczajów, upodobań nie zastanawiając się czy jest to im potrzebne czy zbędne. Telefon stał się rzeczą nierozłączną, a nawyk odbioru i przeglądania, nawet SMS-a z reklamą, to niezbędna czynność zaraz po usłyszeniu sygnału w telefonie. Można postawić tezę, że są to choroby społeczne które już zidentyfikowano jako: fonholizm, smombie, nomofobia.

Jednym z ciekawszych badań wskazujących na fonoholizm są badania Macieja Dębskiego zawarte w pracy *Nałogowe korzystanie z telefonu komórkowego. Szczegółowa charakterystyka zjawiska fonoholizmu w Polsce. Raport z badań* (Dębski, 2016), w którym autor identyfikuje zjawisko i jednoczenie wskazuje, jakie można przedsięwziąć kroki zaradcze.

Z zasady dzieci i młodzież szybciej przyswajają nowinki techniczne niż ich rodzice i nauczyciele. Niestety świadomość zagrożeń wśród nich nie jest powszechna. Z tego powodu ważne jest pokazanie dzieciom i młodzieży, jak korzystać z telefonów komórkowych i mediów w sposób odpowiedzialny. Nowoczesne metody edukacyjne mogą zachęcić uczniów do koncentracji i pobudzić w nich chęć do nauki (Buchegger, 2013, s. 64-74.). Zakaz używania telefonów komórkowych w szkole powinien być długofalowym rozwiązaniem, jednak nie jest realistycznym działaniem. Z kolei długotrwałe monologi o zasadach używania także nie wpłyną na poprawę świadomości bezpiecznego używania telefonu. Właściwie nie ma złotego środka, są natomiast ciekawe ćwiczenia edukacyjne mogące zainspirować i zaciekawić młodzież, a przez to zwiększyć ich wiedzę o zagrożeniach w czasie, gdy nastąpi konflikt zbrojny.

W przypadku konfliktu zbrojnego, gdy pełnimy odpowiedzialną funkcję w strukturach administracyjnych państwa, samorządu lub zajmujemy predysponowane stanowisko w strukturach siłowych, to tym bardziej narażamy się na niebezpieczeństwo oddziaływania zarówno działaniami dezinformacyjnymi, elektromagnetycznymi (zakłócenia telefonu), jak i w ostateczności oddziaływaniem środkami rażenia. Za przykład niefrasobliwości mogą posłużyć sytuacje z konfliktu na Ukrainie, m.in. eliminacja rosyjskiego szefa sztabu wojsk powietrzno-desantowych armii Rosji, gen. Andrieja Simonowa, który podczas ataku na Izum prowadził rozmowy przez telefon komórkowy korzystając z sieci telefonii komórkowej Ukrainy (Dereszyński, 2022). Podobną sytuację można przedstawić na przykładzie ataku rakietowego wojsk ukraińskich w Makiejewce. Miejsce przebywania rosyjskich żołnierzy zdradziły przesyłane życzenia noworoczne przez telefony komórkowe. Namierzył ich system Echelon stworzony

przez armię amerykańską jako globalną sieć wywiadu elektronicznego. W Makiejewce, w szkole, żołnierze rosyjscy zorganizowali skład amunicji i tymczasowe koszary dla około 600 żołnierzy. Lokalizacja żołnierzy rosyjskich nastąpiła w wyniku przechwytu bardzo licznych połączeń telefonicznych, jakie wykonywali w sylwestra. Wojska ukraińskie wykorzystały dane lokalizacyjne z systemu Echelon (strona amerykańska nie potwierdza tych informacji) i wykonały uderzenie artyleryjskie. Według źródeł ukraińskich w wyniku ataku zginęło około 400 żołnierzy, a według rosyjskich – około 63 (Potocka, 2023).

Beztroskie wykorzystywanie smartfonów przez rosyjskich żołnierzy już wcześniej pomagało wojskom Ukraińskim namierzyć wroga. Okupanci, słynący z masowych kradzieży wśród ludności ukraińskiej, m.in. ze sprzętów elektronicznych marki Apple, nie zorientowali się, że zagubione lub przywłaszczone urządzenia mają funkcję namierzania. W ten sposób wielokrotnie zostali zlokalizowani, a w konsekwencji także miejsca dyslokacji jednostek. Niefrasobliwość w korzystaniu z sieci teleinformatycznej rozlokowanej na terenie Ukrainy powodowała, że namierzono osoby komunikujące się ze skradzionych telefonów, a to pozwoliło na zlokalizowanie wielu zbrodniarzy wojennych, m.in. z Buczy. Lokalizacja odnosiła się także do innych urządzeń elektronicznych wskazując miejsca składowania zdobyczy.

ZASADY BEZPIECZNEGO UŻYTKOWANIA URZĄDZEŃ MOBILNYCH

Większość autorów publikacji związanych z bezpieczeństwem użytkowania mobilnych urządzeń telekomunikacyjnych przedstawia zasady bezpiecznego ich korzystania w aspektach zdrowotnych i behawioralnych. Aspekt bezpieczeństwa zdrowotnego dotyczy tylko możliwych chorób związanych z promieniowaniem EM wytwarzanym przez telefon (czasami przez BTS) lub uzależnieniem od użytkowania, a także złego samopoczucia, czyli odnosi się do objawów świadczących o niewielkim wpływie na zdrowie, a bardziej o uzależnieniu od telefonów komórkowych. W ogólności są to choroby związane z naszą psychiką i można je leczyć. Dużo miejsca w literaturze zajmują teksty behawioralne zawierające zasady bezpiecznego korzystania z telefonów z uwagi na utratę poufności, wizerunku danych osobowych czy zagubienie albo kradzież telefonu. Nieco mniej jest informacji o sposobach namierzania osób lub telefonu albo przechwytywania informacji w sieciach GSM jako celowego działania. Oczywiście można doszukać się szerszego potraktowania tematu, ale powszechność takiej literatury jest ograniczona. Ogólniki lub techniczne informacje nie zawsze są zrozumiałe dla szerokiego

grona odbiorców. Czynnik niedostatku publikacji związanych z lokalizacją osób lub telefonów jako element zagrożenia stanowi istotną lukę edukacyjną, bo jak już wspominano często podczas konfliktu zbrojnego ta wiedza może uratować życie człowieka. Najwięcej informacji można znaleźć na stronach internetowych, ale i tam autorzy często piszą językiem technicznym, nieprzystępnym dla wszystkich odbiorców.

Z analizy literatury przedmiotu wynika, że wielu przedstawicieli firm i organizacji, których charakter prowadzenia działalności związany jest bezpieczeństwem informacyjnym lub cybernetycznym publikuje, prowadzi prelekcje propagujące zasady bezpieczeństwa w znaczeniu behawioralnym (Nowak, 2022). Przekazywane społeczeństwu wskazówki i dobre rady dotyczą korzystania z telefonów, smartfonów w warunkach bezpiecznego i stabilnego państwa, natomiast nieco inne zasady powinny być przestrzegane podczas zagrożenia wojennego. Konflikt zbrojny to czas, w którym obie strony prowadzą walkę radioelektroniczną, informacyjną, cybernetyczną. Monitorują środowisko elektromagnetyczne i informatyczne starając się wykryć zarówno relacje łączności telefonicznej, jak i radiowej; stosują szereg przedsięwzięć dezinformacyjnych w cyberprzestrzeni i radiofonii. Zagrożone są pojedyncze osoby, grupy osób a nawet firmy przekazujące w strumieniach informacji dane wrażliwe. Działania wojenne na Ukrainie wyraźnie wskazują, że wojna informacyjna, radioelektroniczna trwa bez końca, a wygrywa ten, kto szybciej i precyzyjniej ustali źródła informacji oraz podejmie stosowne decyzje.

Zapewniając większe bezpieczeństwo użytkowania mobilnych urządzeń telekomunikacyjnych można określić przedsięwzięcia, do zrealizowania przez organy państwowe i wojskowe podczas konfliktu zbrojnego, takie jak:

– rozesłanie rodzinom żołnierzy dedykowanych (darmowych) aplikacji do kontaktu z nimi na froncie wraz z zasadami prowadzenia rozmów,

– rozpowszechnienie nowego numeru alarmowego (zmiana numeru 112 na inny – wojenny),

– rozesłanie darmowych programów antywirusowych dla wszystkich obywateli podczas konfliktu zbrojnego,

– monitorowanie aktywności hakerskiej w sieciach każdego z operatorów,

wdrożenie systemów antywłamaniowych w obrębie newralgicznych stacji BTS (szczególnie przy infrastrukturze krytycznej),

– dążenie poprzez akcje informacyjne, szkoleniowe do zwiększenia świadomości istniejących zagrożeń wśród społeczeństwa,

– nałożenie obowiązków na operatorów sieci teleinformatycznych zwiększenia zasad bezpieczeństwa w sieciach poprzez rozwiązania organizacyjno-techniczne i proceduralne.

Oprócz obowiązków nałożonych na przedstawicieli organów rządzących, powinny być również zasady obowiązujące obywateli. Wśród nich można wymienić:

– przestrzeganie opracowanych zasad użytkowania telefonów, smartfonów i innych urządzeń komunikacji mobilnej w czasie konfliktu zbrojnego przez organy państwa,

– przestrzeganie prawa (nakazów i zakazów) ogłaszanych na danym obszarze lub strefie dotyczące zasad bezpieczeństwa telekomunikacyjnego,

– ograniczenie liczby wysyłanych wiadomości SMS, MMS, Video, szczególnie z miejsc walki i dyslokacji sprzętu oraz jednostek wojska i infrastruktury krytycznej,

– przestrzeganie używania dedykowanych dla społeczeństwa aplikacji do komunikacji,

– włączenie automatyczne archiwizowania danych,

– wyłączanie urządzeń mobilnych w czasie nalotów samolotów, BSP, rakiet, a także innych ofensywnych działań przeciwnika np. podczas ogłoszenia, że stosuje atak radioelektroniczny,

– ograniczenie aktywności w social mediach, szczególnie przez młodzież i dzieci,

– bezwzględny zakaz odbierania informacji z nieznanego źródła (również podejrzanych numerów telefonów),

– nieużywanie pozostawionych (znalezionych, podarowanych) telefonów lub smartfonów (możliwa prowokacja z zainstalowanym programem śledzącym).

Wraz z nakazami i zakazami nakładanymi na organy rządowe i obywateli, także operatorzy sieci komórkowych powinni przestrzegać opracowane zasady bezpieczeństwa na wypadek działań wojennych. Można do nich zaliczyć (wybór):

– wspieranie najbliższych jednostek wojskowych w identyfikacji zagrożenia (informowanie o wykrytych źródła elektronicznych, fałszywych BTS-ach, innych źródłach promieniujących energię EM),

– w sytuacjach krytycznych umożliwienie kierowania działaniami jednostek wojskowych (np. kierowanie ogniem artylerii),

– automatyczne zapisywanie zobrazowania sytuacji radioelektronicznej po ataku przeciwnika i przesyłanie danych do wyznaczonych organów wojskowych i cywilnych celem przekierowania strumieni komunikacyjnych i ochrony infrastruktury telekomunikacyjnej,

– zabezpieczanie danych wrażliwych, w tym danych osobowych, finansowych przed atakami hakerskimi strony przeciwnej.

Z doświadczeń operatorów ukraińskiej sieci telefonii komórkowej można zaczerpnąć wielu praktycznych rozwiązań. Jednym z ciekawszych przykładów rozwiązań organizacyjnych było rozpowszechnienie aplikacji na telefon, za pomocą której wszyscy obywatele mogli przesyłać dane z pola walki i wskazywać

na działania wojsk rosyjskich, dokumentować zarodnie i prowadzić bezpośredni przekaz informacji do organu kierowania lub do chmury, po czym następowało automatyczne czyszczenie pamięci telefonu, aby w przypadku aresztowania przez przeciwnika nie być posądzonym o szpiegostwo. Wojsko ukraińskie po uzyskaniu takich informacji używało sztucznej inteligencji, by weryfikować i procedować zebrane dane oraz integrować je z procesem identyfikacji i namierzania celów, np. dla artylerii ukraińskiej (Bartosiak, 2022). Z doniesień wojennych wynika, że nawet niedoświadczona osoba cywilna może kierować artylerią.

Inne rozwiązania to uruchomienie specjalnych aplikacji dla rodzin do łączności z żołnierzami. Kolejne przykłady to wykorzystanie szybkich łączy służących jako środek zastępczy systemów łączności wojskowej (odpowiednio szyfrowane), namierzenia telefonów przeciwnika za pomocą fałszywych BTS-ów podkładanych przez wojska specjalne, BSP (drony) lub system podpięć do stacjonarnych BTS-ów z zaimplantowanymi aplikacjami. Doświadczenia uczą, że można takich systemów użyć jako systemów amorficznego rozproszonego systemu przekazu informacji na potrzeby dowództw wyższego szczebla. Zaprezentowane rozwiązania są tylko wybranymi, ale istotnymi i możliwymi do zastosowania w rozwiązaniach telefonii rodzimych operatorów.

WNIOSKI

Rozwój technologii cybernetycznych i radioelektronicznych postępuje w tempie geometrycznym. Należy przewidywać, że w najbliższej przyszłości będzie coraz więcej ataków na systemy i sieci teleinformatyczne, w tym telekomunikacyjne. Jest to efekt nieustannego rozwoju technologii i jej wykorzystywania w telefonach komórkowych do komunikacji za pośrednictwem najróżniejszych kanałów komunikacji, takich jak: Bluetooth, SMS, komunikatory, e-mail, Wi-Fi. Coraz częstsze będzie także zjawisko *SMiShingu*, czyli odmiany *phishingu* dokonywanej przy użyciu wiadomości SMS. Rozwój technologii jest stymulatorem poszukiwań nowych rozwiązań zabezpieczających telefony przed utratą danych i możliwością namierzenia abonenta.

W aktualnej sytuacji stabilnego państwa i dość stabilnej sytuacji polityczno-militarnej dla większości użytkowników telefonii komórkowej zagrożenie nie jest duże. Wykorzystywane technologie do przekazywania informacji poufnych są bezpieczne, a różne organizacje przestępcze (hakerskie) są skutecznie wykrywane. Nie oznacza to jednak osiągniecia pełnego stanu euforii. Należy na bieżąco analizować i wyciągać wnioski z konfliktów, a zdobytą wiedzę i doświadczenia przekazywać do praktycznych rozwiązań we własnym środowisku teleinformatycznym.

Głównym zadaniem organów państwowych odpowiedzialnych za edukację ludzkości jest uwrażliwienie społeczeństwa, w tym młodzieży, na poruszone w niniejszym opracowaniu zagadnienia i wprowadzenie w życie „komórkowego kodeksu bezpieczeństwa na wypadek działań zbrojnych". Pozwoli to na podniesienie świadomości istniejących zagrożeń wśród wielu ludzi i mam nadzieję, że uświadomi, w jaki sposób bezpiecznie używać mobilnych urządzeń telekomunikacyjnych w czasie konfliktu zbrojnego w nowoczesnym środowisku teleinformatycznym.

BIBLIOGRAFIA

Bartosik J. (2022), *Lekcje z wojny na Ukrainie dla Polski. Część. 3.* Strategy and Future, nr 11, https://strategyandfuture.org/lekcje-z-wojny-na-ukrainie-dla-polski-czesc-3/ [dostęp: 12.05.2023].

Buchegger B. (2013), *Korzystanie z telefonu komórkowego w szkole, Zarządzanie szansami i zagrożeniami*, Warszawa: Fundacja Rozwoju Systemu Edukacji.

Burke H. (2021), *Jak rozpoznać i pokonać uzależnienia od smartfona. Praktyczne wskazówki*, przekł. A. Trzcińska-Hildebrandt. Warszawa: Zwierciadło.

Creery M. (2019), *The Russian Edge in Electronic Warfare*, Georgetown University Center for Security Studies, https://georgetownsecuritystudiesreview.org/2019/06/26/the-russian-edge-in-electronic-warfare/ [dostęp: 21.02.2023].

Curry Vi. (2015), *Telefon komórkowy może cię zlokalizować przez ...analizę poboru mocy*, https://niebezpiecznik.pl/post/telefon-komorkowy-moze-cie-zlokalizowac-przez-analize-poboru-mocy/ [dostęp: 15.05.2023].

Dereszyński T. (2022), *Wojna na Ukrainie. Amerykanie pomagają namierzać rosyjskich generałów. Już 12 wysokich rangą dowódców zginęło z rąk Ukraińców*, https://i.pl/wojna-na-ukrainie-amerykanie-pomagaja-namierzac-rosyjskich-generalow-juz-12-wysokich-ranga-dowodcow-zginelo-z-rak-ukraincow/ar/c1-16323545 [dostęp: 14.06.2022].

Dębski M. (2016), *Nałogowe korzystanie z telefonu komórkowego. Szczegółowa charakterystyka zjawiska fonoholizmu w Polsce. Raport z badań*, Gdańsk: Uniwersytet Gdański.

Dudek M. (2018), *Wykrywanie fałszywych stacji bazowych za pomocą własnego telefonu*, https://zaufanatrzeciastrona.pl/post/wykrywanie-falszywych-stacji-bazowych-za-pomoca-wlasnego-telefonu [dostęp: 21.06.2023].

Grzelak M. i Liedel K. (2012), *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, Bezpieczeństwo Narodowe 2, nr 22, s. 125-139.

Kabaciński W. i Żal M. (2013), *Sieci telekomunikacyjne*, Warszawa: Wydawnictwa Komunikacji i Łączności.

Katastrofa samolotu MH17 w Ukrainie w 2014 r. Nowe ustalenia (2023), https://podroze.onet.pl/ciekawe/katastrofa-samolotu-w-ukrainie-w-2014-r-nowe-ustalenia-winny-putin/8k8ftnb [dostęp: 21.06.2023].

Konieczny P. (2013), *3 sposoby na podsłuch telefonów komórkowych ...i rady jak podsłuchu uniknąć*, https://niebezpiecznik.pl/post/3-sposoby-na-podsluch-telefonu-komorkowego/ [dostęp: 20.06.2023].

Madejski M. (2023), *Nie tylko Pegasus. Oni mogą grzebać ci w telefonie i wysłać wiadomość do żony*, https://businessinsider.com.pl/wiadomosci/nie-tylko-pegasus-oni-moga-grzebac-ci-w-telefonie-i-wysylac-wiadomosci/rqbmzyr [dostęp: 16.04.2023].

McDermott R. (2019), *Russia's Advances in Electronic Warfare Capability*, Publication: Eurasia Daily Monitor 16, nr 135, https://jamestown.org/program/russias-advances-in-electronic-warfare-capability/ [dostęp: 20.05.2023].

McDermott R. (2020) *Russia's Armed Forces Test and Refine Electronic Warfare Capability*, Publication: Eurasia Daily Monitor 17, nr 59, https://jamestown.org/program/russias-armed-forces-test-and-refine-electronic-warfare-capability/ [dostęp: 20.02.2023].

Nowak M. (2022), *Bezpieczne korzystanie ze smartfona – 7 zasad, o których trzeba pamiętać* https://android.com.pl/porady/485982-bezpieczne-korzystanie-ze-smartfona/ [dostęp: 30.06.2022].

Pieleszek M. (2018), *Bądź bezpieczny w cyfrowym świecie. Poradnik bezpieczeństwa IT dla każdego*, Warszawa: Helion.

Potocka J. (2023), *Zdradziły ich telefony. Tak Ukraińcy namierzyli rosyjskich żołnierzy w bazie w Makiejewce*, https://www.rmf24.pl/raporty/raport-wojna-z-rosja/news-zdradzily-ich-telefony-tak-ukraincy-namierzyli-rosyjskich-zo,nId,6511685#crp_state=1 [dostęp: 14.04.2023].

Řezník T., Horáková B. i Szturc R. (2015), *Advanced methods of cell phone localization for crisis and emergency management applications*, International Journal of Digital Earth 8, nr 4, 259-272. https://doi.org/10.1080/17538947.2013.860197

Rywczyńska A. i Wójcik S. (2018), *Bezpieczeństwo dzieci i młodzieży online. Kompendium dla rodziców i profesjonalistów*, Warszawa: NASK-PIB i Fundacja Dajemy Dzieciom Siłę.

Simon A. i Walczyk M. (2002), *Sieci komórkowe GSM/GPRS. Usługi i bezpieczeństwo*, Kraków: Wydawnictwo Xylab.

Simon A.M. (2007). *Bezpieczeństwo telefonii komórkowej (3) Bezpieczeństwo usług i użytkownika*, https://www.computerworld.pl/news/Bezpieczenstwo-telefonii-komorkowej-3-Bezpieczenstwo-uslug-urzedzen-i-uzytkownika,321537,4.html [dostep: 03.06.2023].

BEZPIECZEŃSTWO UŻYTKOWANIA URZĄDZEŃ MOBILNYCH PODCZAS KONFLIKTU ZBROJNEGO

Streszczenie

W opracowaniu przedstawiono problem braku zasad bezpieczeństwa używania mobilnych urządzeń telekomunikacji, tj. smartfonów, smartwatchy, telefonów komórkowych podczas działań zbrojnych. Telefon komórkowy mimo niewątpliwie wielu zalet w czasie działań zbrojnych stanowi również zagrożenie dla człowieka i jego otoczenia. Uwagę skupiono na braku opracowanych zasad bezpieczeństwa oraz na dostępnych metodach lokalizacji tegoż urządzenia. Jednocześnie zwrócono uwagę, jak łatwo namierzyć telefon i osobę podczas trwania konfliktu zbrojnego. Wskazano na celowość posiadania i użytkowania zabezpieczanych urządzeń mobilnych przez odpowiedzialne osoby za kierowanie administracją państwową i wojskową. Osobne miejsce poświęcono świadomości osób korzystających z urządzeń mobilnych, które mogą poprzez nieumyślną korespondencję przekazywać istotne informacje stronie przeciwnej. Wskazano także na praktyczne rozwiązania i wnioski jakie wynikają z podobnej sytuacji w Ukrainie podczas toczącego się konfliktu zbrojnego.

Słowa kluczowe: mobilne urządzenia telekomunikacyjne; lokalizacja GPS; konflikt zbrojny; bezpieczeństwo telefonii komórkowej.