Sławomir Pepłoński

TELEFONIA KOMÓRKOWA NA WOJNIE?

W drugiej połowie 2022 r. agenci izraelskiej agencji wywiadowczej Mossad uprowadzili przebywającego na wakacjach w Malezji Palestyńczyka Omara al-Balbaisi. Omar al-Balbaisi jest jednocześnie hakerem (wysokiej klasy ekspertem w zakresie wykorzystywanego w smartfonach systemu Android) oraz wykładowcą akademickim. Znajduje się na liście najbardziej poszukiwanych przez Mossad osób. Jest odpowiedzialny za infiltrację izraelskiego systemu obrony powietrznej „Żelazna Kopuła". W latach 2015 i 2016 włamywał się do systemów teleinformatycznych „Żelaznej Kopuły", co umożliwiło brygadom Al-Kassam skuteczne wystrzelenie rakiet w kierunku Izraela. W październiku 2023 r. Omar al-Balbaisi, podczas operacji Hamasu „Burza Al-Aksa" prawdopodobnie wyłączył częściowo system kierowania barierą między Strefą Gazy i Izraelem, co pozwoliło przedrzeć się ok. 3000 bojowników i zaatakować Izrael. Oba ww. systemy wykorzystywały infrastrukturę sieci komórkowej GSM.

Świadomy pościgu Mossadu, Omar al-Balbaisi od 2020 r. mieszkał w Stambule w Turcji i był pod stałym nadzorem służb specjalnych tego państwa. Co więcej, turecka agencja wywiadowcza, Narodowa Organizacja Wywiadowcza (MIT), trzykrotnie ostrzegła Omara o planach Mossadu dotyczących jego porwania i zainstalowała aplikację lokalizującą w jego telefonie. Pomimo tych środków, kilka dni po przybyciu do Malezji, Omar został porwany przez Mossad. Był torturowany i przesłuchiwany, w tym również przez VTC bezpośrednio z Iraela. W czasie przesłuchań Izraelczycy próbowali dowiedzieć w jaki sposób haker włamywał się do telefonów żołnierzy i funkcjonariuszy rządowych poprzez system Android, w jaki sposób uzyskał dostęp do Żelaznej Kopuły i bariery. Wywiady malezyjski i turecki wspólnie uwolniły porwanego, jednocześnie zatrzymując 11 agentów izraelskich. Haker (prawdopodobnie) znajduje się w bezpiecznym miejscu w Turcji.

Czy informacje uzyskane od hakera sieci komórkowych są warte poświęcenia 11 agentów Mossadu? Powyższy przykład wskazuje, że chyba tak.

Błędy w projektowaniu i zasadach wykorzystania wojskowego systemu łączności budowanego na bazie cyfrowej sieci komórkowej GSM kosztują życie żołnierzy. Widać to szczególnie dobrze analizując sytuację na froncie toczącej się wojny pomiędzy Ukrainą i Rosją.

Federacja Rosyjska zbudowała i uruchomiła w 2021 r. wojskowy system kryptofonowy (bezpieczny, szyfrowany telefon GSM) ERA (domniemana nazwa systemu) w oparciu o sieć

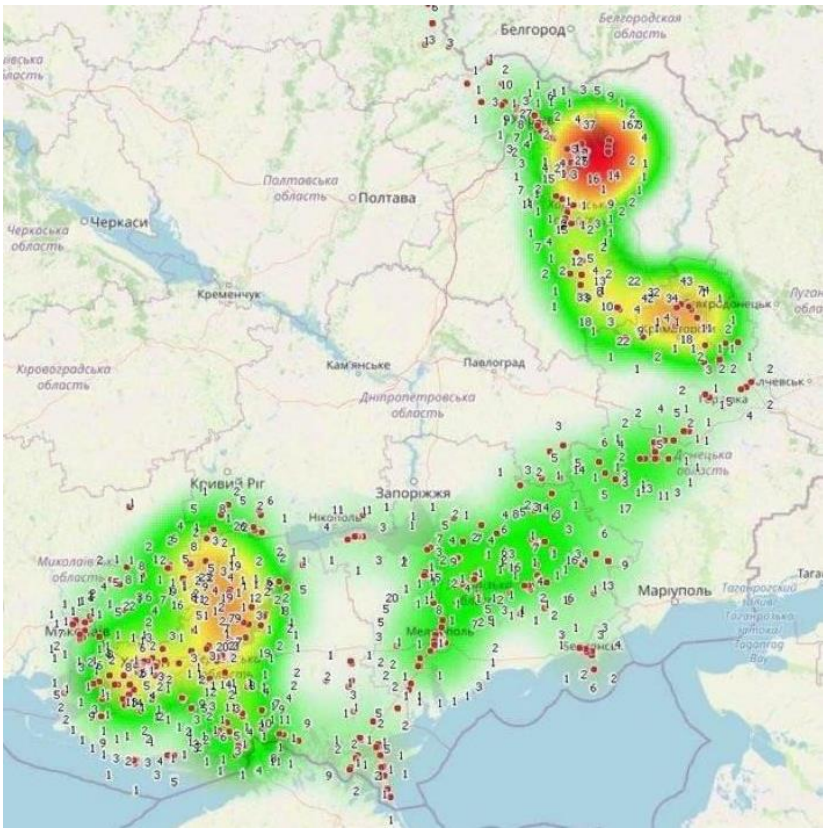
GSM 3G/4G. Cały projekt ERA obejmuje również projekty „Kwarc" i „Pasport", zapewniające żołnierzom spersonalizowany, zdalny, bezpieczny dostęp do danych z tzw. etykietowaniem. W swoim założeniu system łączności miał wykorzystywać wyłącznie transmisję szyfrowanych danych poprzez infrastrukturę rosyjskiego operatora MegaFon i być zarządzany z Moskwy. Jednak na ukraińskich terenach zajmowanych przez wojska rosyjskie nie było infrastruktury MegaFonu, a uszkodzenia lub zniszczenia stacji bazowych sieci komórkowych (Base Transceiver Station - BTS) i wyłączenie transmisji danych skutecznie unieszkodliwiło rosyjski system ERA. Dlatego też na początku konfliktu Internet zalały zdjęcia rosyjskich żołnierzy z chińskimi walkie-talkie Baofeng. Dodatkowo, smartfony ERA, używane w rejonach ze zdegradowaną infrastrukturą telekomunikacyjną automatycznie logowały się do sieci ukraińskich, co pozwoliło na identyfikację i geolokalizację dowódców. W efekcie wielu z rosyjskich generałów (około 12 generałów i 40 wyższych oficerów, np. generał Witalij Gierasimow, szef sztabu 41. Armii pod Charkowem) poniosło śmierć w wyniku precyzyjnych ataków.

Ataki na dowódców, korzystających z telefonów komórkowych lub satelitarnych stają się powszechne. Jeden z pierwszych takich przypadków miał miejsce w 1996 r., kiedy to rosyjski samolot rozpoznawczy namierzył używany telefon satelitarny Dżochara Dudajewa, pierwszego prezydenta Czeczeńskiej Republiki Iczkerii. Chwilę później przywódca separatystycznej republiki został trafiony rakietami naprowadzanymi laserowo. Podobny los spotkał dowódcę irackiej Al-Kaidy, Abu Musab al-Zarkawiego.

Geolokalizacja jest procesem, który zależy od charakterystyki telefonu komórkowego. Może odbywać się poprzez przesyłanie lokalizacji GPS lub rejestracji w sieci komórkowej karty SIM znajdującej się w telefonie. Lokalizowanie telefonu z użyciem GPS jest najprostsze, ale wymaga zainstalowania na telefonie dedykowanego oprogramowania, które wysyła współrzędne pozycji GPS do dedykowanego serwera (jak w przypadku Omara al-Balbaisi). Jest to forma dostępnej powszechnie kontroli rodzicielskiej. Lokalizowanie telefonu na podstawie jego adresu i logowania do sieci jest dostępne tylko dla operatora sieci i uprawnionych służb specjalnych. Konieczne jest monitorowanie logowania telefonu (unikalnego adresu karty SIM lub numeru IMEI modułu radiowego aparatu) do stacji bazowych BTS znajdujących się w zasięgu aparatu i precyzyjne wyliczenie położenia metodą triangulacji. Naturalnie, im więcej stacji bazowych odbiera sygnał z telefonu tym większa jest precyzja określenia jego położenia.

Strona ukraińska publikuje w Internecie mapy, pokazujące lokalizacje kryptofonów ERA (poniżej). Amerykańskie oraz brytyjskie służby wywiadowcze również zbierają informacje o

intensywności wykorzystania i skupiskach kryptofonów ERA w pobliżu linii frontu. Informacje te są udostępniane wojskom ukraińskim w czasie prawie rzeczywistym.



Rosyjski kryptofon to tak naprawdę wzmocniony telefon komórkowy oparty na rosyjskich smartfonach MIG C55V lub M-663C „Atlas", które zostały opracowane dla rosyjskich agencji wywiadowczych przez „Centrum Naukowo-Techniczne Atlas". Co ciekawe, M-663C jest modyfikacją chińskiego telefonu RugGear P860 (który z kolei jest mocno wzorowany na telefonach wojskowych Sonim XP3 Enduro). Koszt aparatu wynosił ponad 115 tysięcy rubli, co było sumą pokaźną, ale biorąc pod uwagę zaawansowaną technologię i małoseryjną, ręczną produkcję – uzasadnioną.

Prawdopodobnie telefon wykorzystuje wymianę danych do komunikacji głosowej – podobnie jak aplikacje, takie jak WhatsApp, Signal itp. i zapewnia pełne programowe szyfrowanie pomiędzy nadawcą i centrum zarządzania. Możliwe jest również prowadzenie klasycznych rozmów jawnych. W celu zapewnienia bezpieczeństwa systemu ERA wojsko rosyjskie wykorzystuje dedykowane stacje bazowe (własnej produkcji lub chińskie klony urządzenia StingRay firmy L3Harris). StingRay pełni funkcję „fałszywej" stacji bazowej i staje się pośrednikiem między telefonem a antenami dostawcy usług telefonii komórkowej. W teorii system ERA jest bezpieczny. Jednak zawsze jest jakieś, ale ... Posiadając wzorce transmisji danych typowych dla kryptofonów ERA oraz sygnatury sygnału, operator sieci komórkowej może jednoznacznie je zidentyfikować i zlokalizować. W Internecie można znaleźć algorytmy wykrycia i geolokalizacji rosyjskich urządzeń. Procedury tzw. EraRecognizer są dostępne na witrynie Github.

Rosyjskie BTSy typu „StingRay" wykorzystywane są również do przechwytywania łączności komórkowej wojsk ukraińskich. Ponadto, są elementem składowym wprowadzonego na wyposażenie wojsk FR w 2019 roku systemu walki radioelektronicznej i psychologicznej RB-341V Leer-3. Oprócz BTS system Leer-3 posiada również na wyposażeniu m.in. 3 samoloty bezpilotowe (UAV) Orłan-10 o zasięgu ok. 10 km., które wyposażone są w przenośne BTS. Rosyjscy żołnierze używający Leera-3 są w stanie zakłócać pracę szyfrowanej telefonii komórkowej armii ukraińskiej (do 2000 abonentów sieci) w promieniu 30 km przez ok. 10 godzin.

System pozwala na monitorowanie ruchu komórkowego, na przechwytywanie transmisji danych komórkowych i przejmowanie połączeń, blokowanie połączeń z i do konkretnych numerów itd. Może również rozsyłać wiadomości i wykonywać połączenia do zalogowanych telefonów.

Wartość systemu RB-341V Leer-3 dla sił bezpieczeństwa została również potwierdzona podczas zamieszek w Kazachstanie. Źródła podają, że „Nie ma wątpliwości, że uruchomienie systemu Leer-3 nie tylko przerwało łączność pomiędzy grupami bojowymi a ich zagranicznymi kontrolerami, ale także zapewniło kazachskim siłom bezpieczeństwa ich dane geolokalizacyjne. Utrata dowodzenia i kontroli przez konkretnych dowódców oraz niezdolność do działań, doprowadziły do eliminacji grup bojowych". System był również testowany i wykorzystywany w Syryjskiej Republice Arabskiej.

Rosyjski system Leer-3 jest zawsze wartościowym celem dla wojsk ukraińskich. Filmy, obrazujące zniszczenie systemu, dumnie udostępniane są w mediach społecznościowych (np.

film z rejonu Zaporoża pokazujący zniszczenie systemu przez drony 129. Brygady Obrony Terytorialnej Ukrainy).

Urządzeń typu StingRay używa oczywiście również armia ukraińska.

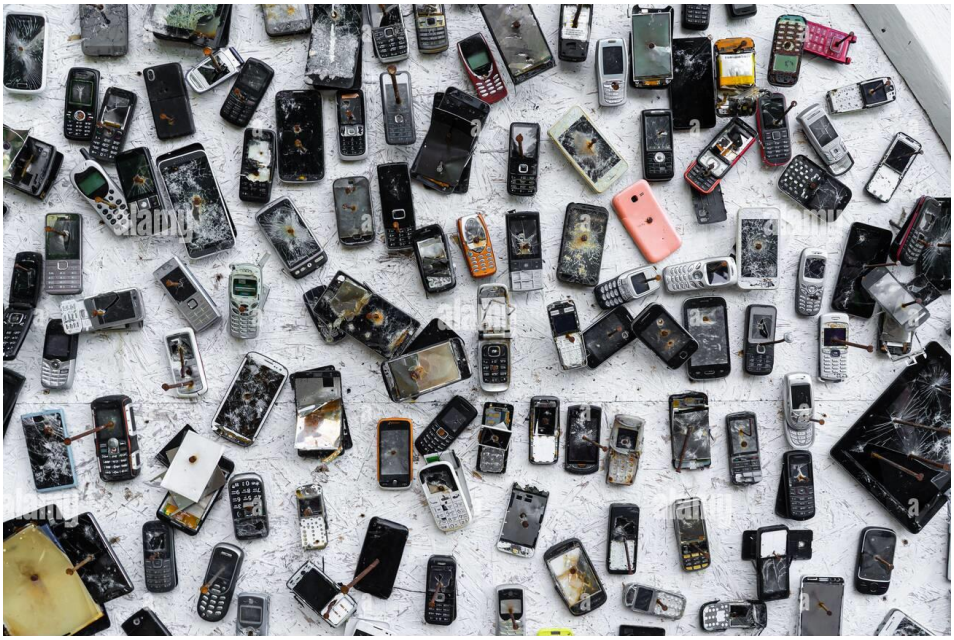
Z uwagi na ww. zdolności wojsk rosyjskich w zakresie łączności komórkowej dowództwo ukraińskie nakazało przestrzeganie żołnierzom nw. zasad:

1. Zostaw swoją kartę SIM w domu.
2. Najlepszym miejscem zakupu kart SIM jest sama strefa konfliktu.
3. Jeśli dzwonisz, to rób z odległości odległość co najmniej 400–500 metrów od stanowiska pododdziału.
4. Nie oddalaj się od pododdziału, zawsze zabieraj ze sobą uzbrojonego kolegę jako osłonę.

5. Telefonu używaj w miejscach z dużą liczbą ludności cywilnej, najlepiej w niedawno wyzwolonych miastach.
6. Zawsze wyłączaj telefon. Od tego zależy Twoje życie. Pociski Grad trafiają w całą drużynę.
7. Nie akceptuj kodów doładowujących ani kart SIM od mieszkańców. Młoda kobieta z sąsiedniej wioski, która Ci to oferuje za darmo, może działać dla wroga. W tej chwili FSB i SBU muszą przeanalizować ogromnej ilości danych, aby zidentyfikować telefony komórkowe naszych własnych obywateli i wroga. Nie ułatwiaj wrogowi pracy.
8. Czuwaj nad swoimi towarzyszami – znajomy dzwoni do swojej dziewczyny i godzinę później wasze pozycje są ostrzelane lub zaatakowane.
9. Pamiętaj, że wróg może podsłuchiwać Twoje połączenia, bez względu na to z jakiego operatora i z jakiej karty korzystasz.

Ww. zasady obowiązują obie strony konfliktu. Internet pełen jest zdjęć telefonów GSM należących do żołnierzy nieprzestrzegających reguł postępowania, przybitych do „ścian hańby" lub drzew. Niestety, rutyna i nuda są śmiertelnymi wrogami. Jeden z ukraińskich żołnierzy walczących w 2017 r. w Donbasie powiedział - „Siedząc całymi dniami, a nawet tygodniami w ziemiankach, okopach i bunkrach, nie ma nic do roboty, ludzie zaczynają wariować. wyszukasz czegoś, co oderwie ich od codziennych spraw".

Oficjalnie SZ FR odpowiednie zakazy wprowadziły w lutym 2018 r. Nastąpiło to po ataku dronów w rosyjskich bazach w Hmeimim i Tartus w Syrii. Drony miały mieć możliwość śledzenia telefonów o konkretnych numerach.



Zamiast zakończenia

Niewątpliwie wykorzystanie telefonii komórkowej, komercyjnej i w rozwiązaniach dedykowanych wojsku, niesie za sobą wiele korzyści. Szczególnie w czasie pokoju, z dala od rejonów narażonych na rozpoznanie i celowe przeciwdziałanie.

Szerokie, ale nieprzemyślane wykorzystanie telefonii komórkowej w rejonach działań militarnych jest z kolei niebezpieczne i destrukcyjne.

Należy analizować wszystkie pozytywne i negatywne aspekty oraz potencjalne konsekwencje podejmowanych decyzji. I wybierać mądrze.

Materiał powstał na podstawie informacji z otwartych, jawnych źródeł, dostępnych w Internecie.