Studia Bezpieczeństwa Narodowego
Zeszyt 31 (2024)
ISSN 2028-2677, s. 107-122
DOI: 10.37055/sbn/183538

Instytut Bezpieczeństwa i Obronności
Wydział Bezpieczeństwa, Logistyki i Zarządzania
Wojskowa Akademia Techniczna
w Warszawie

National Security Studies
Volume 31 (2024)
ISSN 2028-2677, pp. 107-122
DOI: 10.37055/sbn/183538

Institute of Security and Defense
Faculty of Security, Logistics and Management
Military University of Technology
in Warsaw

APLIKACJE MOBILNE NA FRONCIE WOJNY ROSYJSKO-UKRAIŃSKIEJ

MOBILE APPLICATION ON THE FRONT LINE OF THE RUSSIA-UKRAINE WAR

Jacek Meissner
ORCID: 0000-0001-7481-6115
Wojskowa Akademia Techniczna im. Jarosława Dąbrowskiego w Warszawie

Abstrakt. Współczesne wojny, tak jak inne obszary życia społecznego, ulegają coraz większej cyfryzacji. Oprogramowanie i urządzenia mobilne są powszechnie wykorzystywane także na potrzeby wojskowe. Konflikt rosyjsko-ukraiński od samego początku w 2014 r. spowodował wprowadzenie innowacyjnych rozwiązań wykorzystujących nowe technologie. Problemem badawczym jest rola aplikacji mobilnych we współczesnym konflikcie zbrojnym, a celem badań było dokonanie przeglądu aplikacji mobilnych w ramach wojny rosyjsko-ukraińskiej oraz przedstawienie wpływu wykorzystania tego typu narzędzi na zdolności wojskowe i szerzej na bezpieczeństwo narodowe. Przeprowadzona analiza potwierdza hipotezę, że wykorzystanie aplikacji mobilnych w nowoczesnym konflikcie zbrojnym nie jest krytyczne dla osiągnięcia sukcesu militarnego, ale stanowi ważny czynnik, multiplikator „twardych" zdolności, w szczególności w zakresie świadomości sytuacyjnej i łączności, oraz bezpieczeństwa obywateli i ich wsparcia na rzecz sił zbrojnych. Przedmiotem badań są zarówno typowo wojskowe aplikacje (z zakresu C4ISR, np. systemy BMS), półamatorskie oprogramowanie wykorzystywane przez wojsko oraz narzędzia dla cywili. Po stronie ukraińskiej często są dziełem wolontariuszy, start-upów, samego wojska, powstają także w ramach specjalnie powołanego w tym celu klastra technologii obronnych Brave1. Aplikacje mobilne rozumiane są jako oprogramowanie na urządzenia mobilne (przede wszystkim smartfony i tablety). Ponadto same urządzenia mogą być wojskowe lub ogólnodostępne. Autor formułuje wnioski z wykorzystania aplikacji mobilnych w warunkach wojennych, jak również pochyla się nad kwestią tego rodzaju aplikacji na gruncie polskim. Autor opiera się o analizę ogólnodostępnych źródeł (głównie ukraińskich i rosyjskich), których większość pojawiła się po 2022 r. Liczba publikacji naukowych dotycząca tej tematyki jest ograniczona. W ocenie autora problematyka ta zasługuje na dalsze badania, gdyż w przyszłych konfliktach wykorzystanie aplikacji mobilnych będzie powszechne i o co raz większym wpływie na prowadzenie działań zbrojnych oraz ochronę ludności cywilnej.
Słowa kluczowe: analityka pola walki, aplikacje mobilne, cyberbezpieczeństwo, cyfryzacja, wojna rosyjsko-ukraińska

Abstract. Modern warfare, like other areas of social life, is becoming increasingly digitalised. Software and mobile devices are also widely used for military purposes. From its very beginning in 2014, the Russian-Ukrainian conflict was linked with the introduction of innovative solutions based on new technologies The research problem is the role of mobile applications in modern armed conflict, and the objective of the research was to overview mobile applications in the Russian-Ukrainian War and outlines the impact of the use of this type of tools on military capabilities, and in general on national security. The analysis confirms the hypothesis that the usage of mobile applications in modern armed conflict is not critical to military success, but is an important factor, a multiplier of "hard" capabilities, particularly in terms of situational awareness and communications, and the security of citizens and their support for the armed forces. The subjects of research are both typically military applications (in particular in the C4ISR field, e.g. BMS systems), semi-amateur software used by the military and tools for civilians. On the Ukrainian side, they are often effect of work of volunteers, start-ups, the military itself, and are also developed under the Brave1 defence technology cluster specially established for this purpose. Mobile applications are understood as a software for mobile devices (mainly smartphones and tablets). In addition, the devices themselves can be military or publicly accessible. The author draws conclusions from the use of mobile applications in wartime conditions, as well as leans into the issue of such applications on Polish soil. The author relies on the analysis of publicly available sources (mainly Ukrainian and Russian), most of which appeared after 2022. The number of scientific publications on this topic is limited. In the author's opinion, this issue deserves further research, as in future conflicts the use of mobile applications will be widespread and with an ever-increasing impact on military operations and the protection of civilians.
Keywords: battlefield analytics, mobile applications, cybersecurity, digitization, Russia-Ukraine War

Wprowadzenie

Współczesne pole walki, tak jak inne obszary życia społecznego, ulęgają coraz większej cyfryzacji. Oprogramowanie i urządzenia mobilne są powszechnie wykorzystywane nie tylko w gospodarce i codziennym życiu człowieka, ale też przez siły zbrojne i cały system obronny państwa. Konflikt rosyjsko-ukraiński od samego początku w 2014 r. spowodował wprowadzenie innowacyjnych rozwiązań wykorzystujących nowe technologie, w tym aplikacji mobilnych. Po pełnoskalowej inwazji na Ukrainę w lutym 2022 r. nasycenie pola walki innowacjami tylko wzrosło. Nowe technologie pozwalają na uzyskanie przewagi nad przeciwnikiem lub niwelowanie jego potencjału. W szczególności po stronie Ukrainy widać było wiele nowatorskich narzędzi, co wynikało z mobilizacji społecznej w obliczu zagrożenia kraju (Jones, Egan, Rosenbach, 2023).

Problemem badawczym jest rola aplikacji mobilnych we współczesnym konflikcie zbrojnym, a celem badań było dokonanie przeglądu aplikacji mobilnych w ramach wojny rosyjsko-ukraińskiej oraz przedstawienie wpływu wykorzystania tego typu narzędzi na zdolności wojskowe i szerzej na bezpieczeństwo narodowe. Autor stawia hipotezę, że wykorzystanie aplikacji mobilnych w nowoczesnym konflikcie zbrojnym nie jest krytyczne dla osiągnięcia sukcesu militarnego, ale stanowi ważny czynnik, multiplikator „twardych" zdolności, w szczególności w zakresie świadomości sytuacyjnej i łączności, oraz bezpieczeństwa obywateli i ich wsparcia na rzecz sił zbrojnych.

Metodyka badań i weryfikacja literatury

Zastosowane zostały metody teoretyczne takie jak analiza, w tym analiz źródeł, synteza, porównanie, uogólnienie. Autor opiera się o analizę ogólnodostępnych źródeł (głównie ukraińskich i rosyjskich), których większość pojawiła się po 2022 r. Liczba publikacji naukowych dotycząca tej tematyki jest ograniczona. W ocenie autora problematyka ta zasługuje na dalsze badania, gdyż w przyszłych konfliktach wykorzystanie aplikacji mobilnych będzie powszechne i o co raz większym wpływie na prowadzenie działań zbrojnych oraz ochronę ludności cywilnej.

Przedmiotem badań są zarówno typowo wojskowe aplikacje (z szeroko rozumianego obszaru C4ISR - dowodzenie, kontrola, łączność, komputery, wywiad, obserwacja i rozpoznanie, np. systemy BMS - System Zarządzania Polem Walki), półamatorskie oprogramowanie wykorzystywane przez wojsko oraz narzędzia dla cywili. Po stronie ukraińskiej często są dziełem wolontariuszy, start-upów, samego wojska, powstają także w ramach specjalnie powstałego w tym celu klastra Brave1, za którego inicjatywą stoi Ministerstwo Transformacji Cyfrowej (Kistol, 2022; Мельник, 2022b). Aplikacje mobilne rozumiane są jako oprogramowanie na urządzenia mobilne (smartfony, tablety, czasem też laptopy). Instalowane są na:

a) urządzeniach wojskowych, które mogą podlegać akredytacji/certyfikacji;
b) na ogólnodostępnych urządzeniach, ale konieczne jest uwierzytelnienie, np. przez innego użytkownika lub poprzez rządową aplikację Diia;
c) na zwykłych ogólnodostępnych urządzeniach, a aplikacji może używać dowolna osoba.

Artykuł nie wyczerpuje problematyki, omawia jedynie najważniejsze aplikacje, informacja o części może nie być upubliczniona, poza tym cały czas powstają nowe narzędzia.

Dyskusja

Rola aplikacji mobilnych w wojnie rosyjsko-ukraińskiej

Wojna rosyjsko-ukraińska częściowo ma charakter typu „XX-wiecznego", z wykorzystaniem klasycznego uzbrojenia, np. broni pancernej i zmechanizowanej, czy artylerii. Jednocześnie istotną rolę odgrywają nowe technologie, takie jak:

a) bezzałogowe statki powietrzne (BSP, drony), wykorzystywane w tysiącach sztuk, w tym komercyjne po militaryzacji;
b) technologie satelitarne obejmujące rozpoznanie obrazowe, łączność, nawigację (w przypadku Ukrainy zapewniane przez państwa zachodnie i komercyjne firmy, np. terminale Starlink);

c) precyzyjna artyleria (wykorzystująca oprogramowanie oparte o zaawansowane algorytmy; środki rozpoznania, w tym drony; inteligentną amunicję);
d) przedmiot artykułu, czyli aplikacje mobilne.

W konflikcie rosyjsko-ukraińskim, szczególnie od lutego 2022 r., aplikacje mobilne pozwalają Ukrainie niwelować przewagę rosyjską. Agresja rosyjska w 2014 i 2022 r. spowodowała mobilizację społeczną, która zaowocowała m.in. rozwojem oprogramowania i rozwiązań sprzętowych na potrzeby obronne kraju. W określonych warunkach organizacyjno-technicznych aplikacje mobilne mogą multiplikować zdolności wojskowe dając przewagę informacyjną, zwiększając świadomość sytuacyjną wojsk, wspierając rozpoznanie, łączność, dowodzenie, usprawniając cykl decyzyjny; choć niewłaściwe używanie urządzeń cywilnych może rodzić też zagrożenia dla żołnierzy, np. poprzez namierzenie ich pozycji. Dają też zupełnie nowe możliwości w zakresie ochrony ludności cywilnej oraz wsparcia ze strony społeczeństwa na rzecz sił zbrojnych (Bohrn, 2023; The Economist, 2023; Schmidt, 2023).

Wykorzystanie innowacyjnych narzędzi wpisuje się w trend rozwijania i adaptowania na potrzeby wojskowe nowych i przełomowych technologii (*Emerging and Disruptive Technologies*, EDT), co dostrzeżono także m.in. w NATO, w ramach którego stworzono strategię EDT oraz mechanizmy ich rozwoju, takie jak akcelerator innowacji obronnych DIANA. W przypadku Ukrainy to wojna był impulsem, który zaowocował wysiłkiem wielu programistów i inżynierów, często *pro bono*, oraz zwinne podejście do realizacji projektów i adaptowania cywilnych rozwiązań.

Przy czym w Ukrainie od lat istniał silny sektor IT. Jak wskazuje Raport „Do IT like Ukraine", jeszcze przed wojną ta gałąź gospodarki notowała wzrost 25-30% r/r i odpowiadała za 4% ukraińskiego PKB. W 2022 r. eksport w sektorze IT wzrósł o 6%. I to pomimo zaangażowania pracowników na rzecz wysiłku obronnego. W 70% firm specjaliści IT służą w Siłach Zbrojnych Ukrainy (SZU), z czego w 43% firm 5% informatyków służy w wojsku, w 25% jest to 5-15%. Ponadto ok. 200 tys. ukraińskich informatyków w inny sposób wspiera armię swojego kraju (Malich, 2022).

Aplikacje wykorzystywane przez Ukrainę

Bodaj najsłynniejszą aplikacją wykorzystywaną przez stronę ukraińską jest Palantir Edge AI amerykańskiej firmy Palantir Technologies Inc. Jest to narzędzie analityki pola walki wykorzystujące sztuczną inteligencję, system świadomości sytuacyjnej. Palantir Edge AI pozwala na integrację danych z wielu różnych źródeł takich jak zobrazowanie satelitarne, z BSP, czy udostępnione zdjęcia (producent nie ujawnia wszystkich źródeł danych) (Jones, Egan, Rosenbach, 2023; Мельник, 2023).

Aplikacja jest też zintegrowana z innym narzędziem tej firmy, jakim jest Meta-Constellation. Zbiera ono dane zobrazowania satelitarnego od dostawców komercyjnych (np. Maxar, Airbus, Capella, ICEYE). Przykładowo w ramach ofensywy

chersońskiej ok. 40 satelitów komercyjnych przeleciało nad miastem w ciągu 24 godzin, zapewniając zobrazowanie o rozdzielczości 3,3 metra (Сабадишина, 2022; Focus, 2022).

Istnieje też możliwość korelacji między rozpoznaniem radioelektronicznym a satelitarnym poprzez rozpoznanie obiektu i jego lokalizację. Informacje o danym obszarze są automatycznie przetwarzane i wyświetlane na cyfrowej mapie. Narzędzie wspiera podejmowanie decyzji w oparciu o zautomatyzowaną analizę możliwych opcji działania i rekomendację najlepszego wariantu. Algorytmy uczenia maszynowego umożliwiają analizę wielu zmiennych, pozwalają też dostrzec to co trudno widoczne dla człowieka (np. identyfikacja stanowisk dowodzenia). Jednym z zastosowań aplikacji jest też ocena strat przeciwnika (Maçães, 2023).

Palantir Edge AI jest instalowany na tabletach, a żołnierze mogą zadaniować oprogramowanie na konkretny obszar. Łączność oparta jest głównie o internet satelitarny Starlink. Narządzie firmy Palantir wykorzystywane są w Ukrainie nie tylko do celów wojskowych, ale też np. do wsparcia przy przesiedlaniu uchodźców (Український мілітарний центр, 2023).

Typowo wojskową ukraińską aplikacją o największych możliwościach jest Delta (*Дельта*). Jest to system BMS umożliwiający gromadzenie, przetwarzanie i prezentowanie informacji o siłach przeciwnika, zapewnia kompleksowy obraz aktualnej sytuacji na polu walki, wyświetlany i podsumowywany na przyjaznej dla użytkownika cyfrowej interaktywnej mapie. Jego funkcjonalności obejmują planowanie operacji, koordynowanie wojsk własnych, zapewnianie świadomości sytuacyjnej. Delta opracowana została przez powstałe w 2021 r. Centrum Innowacji i Rozwoju Technologii Obronnych Ministerstwa Obrony (na bazie jednostki A2724, dawniej organizacja pozarządowa „Aerorozwidka") (Ukrainian Military Center, 2022; Jones, Egan, Rosenbach, 2023; Rosengren, 2023).

Działanie Delty oparte jest o chmurę obliczeniową (obecnie przeniesioną za granicę), a łączność zapewnia Starlink. Jest to system przyjazny dla użytkownika, nie wymaga bowiem specjalnych ustawień i jest gotowy do użycia na laptopach, tabletach czy smartfonach. Umożliwia agregowanie danych z różnych źródeł, takich jak zdjęcia satelitarne, zobrazowanie zapewniane przez BSP, radary, przechwycona komunikacja radiowa, *trackery* GPS, inne typy sensorów, media społecznościowe, wywiad osobowy. Za odpowiednie wprowadzanie danych do systemu oraz ręczne przypinanie obiektów na mapie odpowiadają autoryzowani serwisanci (Danylov, 2022b; Kistol, 2022; The Kyiv Independent, 2023; Rosenbach, 2023;).

Tylko w 2022 r. aplikacja zyskała ponad 30 nowych funkcji. System cechuje się wysoką decentralizacją, co ma służyć ograniczaniu rosyjskich prób oddziaływania środkami cyberwalki i walki radioelektronicznej (WRE). Choć jednocześnie Rosjanie nie ustępują w próbach zhakowania Delty, np. poprzez maile phisingowe do użytkowników systemu. Według informacji medialnych rosyjscy hakerzy uzyskali

ograniczony dostęp do systemu, ale nie udało im się uzyskać istotnych informacji (Danylov, 2022b; Kovacs, 2022).

Delta posiada integrację z chatbotami opracowanym przez Ministerstwo Transformacji Cyfrowej (MTC) – eVorog oraz Służbę Bezpieczeństwa Ukrainy (SBU) –@ stop_russian_war_bot. Aplikacje pozwalają ludności cywilnej informować o jednostkach przeciwnika. Sam chatbot SBU otrzymał tysiące powiadomień w pierwszych dniach inwazji (Ukrainian Military Center, 2022).

Typowo wojskową aplikacją jest też Kropyva (*Кропива*), nazywana „Uberem dla artylerii". Oprogramowanie to zostało opracowane przez organizację „ArmiaSOS" jeszcze w 2014 r., po tym jak artylerzystom wydano mapy wydrukowane w latach 80. XX wieku. Aplikacja jest wykorzystywana na poziomie taktycznym poprzez automatyzację zadań na szczeblu batalionu, kompanii i plutonu. Obejmuje takie funkcjonalności jak lokalizacja pozycji wojsk własnych i przeciwnika, dane rozpoznawcze, nawigacja, mapa topograficzna, obliczenia balistyczne. Przykładowo Kropyva umożliwia operatorowi drona oznaczanie lokalizacji rosyjskiego sprzętu wojskowego (SpW) i udostępnienie danych dowolnej baterii artylerii w okolicy. Umożliwia to skrócenie czasu reakcji do minut, w przypadku rozmieszczenia baterii 5-krotnie, a przy ogniu kontrbateryjnym 10-krotnie.

Według dostępnych danych w 2022 r. 90-95% ukraińskich artylerzystów używało Kropyvy, gdyż po 24 lutego masowo wprowadzano tablety z aplikacją. Przy czym system używany jest nie tylko w artylerii, ale też w wojskach pancernych, piechoty, rozpoznania i obrony przeciwlotniczej (uzupełnia obraz radarowy), a różne rodzaje wojsk wykorzystują różne funkcjonalności. Możliwa jest także wymiana danych z innymi użytkownikami oraz transmisja danych ze środków rozpoznania, jak np. BSP, czy radarów.

Aplikacja działa na tabletach z systemem operacyjnym Android, a dane nie są przechowywane centralnie na serwerach, tylko w zasobach chmurowych. Na każdym tablecie znajdują się jedynie informacje o potrzebnych pozycjach i SpW. Początkowo aplikacja bazowała na Google Maps, ale cywilne rozwiązanie okazało się niewystarczające (Axe, 2022; Бойченко, 2022; The Economist, 2023; Мельник, Т., 2022a; Мельник, Т., 2022b; War.Ukraine.UA, 2023). Inną aplikacją o podobnym zastosowaniu jest GisArt, która rozwinęła się z mapy offline w system świadomości sytuacyjnej szczebla batalionów i brygad.

Aplikacją stworzoną dla artylerzystów jest też MilChat. Rozwiązanie to opracował w 2018 r. J. Szerstiuk, zawodowy artylerzysta i programista-samouk. Obecnie wykorzystuje ją ok. 60 tys. ukraińskich wojskowych. Aplikacja umożliwia m.in. wymianę danych taktycznych, wyznaczanie współrzędnych i azymutu oraz przesyłanie danych geolokalizacyjnych.

Ten sam żołnierz opracował także aplikację UKROP (УКРОП) (taką nazwę nosi na urządzeniach z systemem operacyjny Android, w przypadku iOS nosi nazwę

MyGun). Jest to prosty kalkulator balistyczny zaprojektowany w celu usprawnienia obliczeń artyleryjskich (Kistol, 2022; Мельник, 2022b).

Wspomniana aplikacja eVorog (єВорог) to komunikator/chatbot pozwalający cywilom dostarczać wojsku informacje o ruchach rosyjskich wojsk. Umożliwia przesłanie geolokalizacji, zdjęć, filmów i opisu sytuacji. Aby z niej korzystać należy potwierdzić tożsamość przez aplikację Diia. Po stronie wojskowej aplikacja jest zintegrowana z systemem Delta. Specjalny zespół przetwarza dane w trybie 24/7 przy wykorzystaniu oprogramowania MS Teams i Google Hangouts. eVorog posiada też dodatkową funkcjonalność pozwalającą zgłaszać informacje o zaminowanych obiektach. Przez pierwsze trzy miesiące wojny z chatbota skorzystało 257 tys. Ukraińców (Міністерство цифрової трансформації України, 2022; War.Ukraine.UA, 2023).

Kolejną „obywatelską" aplikacją jest ePPo. Pozwala przesyłać informacje o zaobserwowanych celach powietrznych i podać ich pozycję. Informacje przesyłane przez ePPo pozwalają uzupełniać dane z rozpoznania radiolokacyjnego. Ułatwia to i przyspiesza namierzenie i zestrzelenie celów przez obronę przeciwlotniczą (OPL). Użytkownik po zobaczeniu celu powietrznego może klikając na ekranie telefonu odpowiednią ikonkę wybrać jego typ (BSP, rakieta, śmigłowiec, samolot), a następnie należy przytrzymać smartfon w kierunku ruchu celu i nacisnąć czerwony przycisk. W ten sposób wojska OPL zobaczą na mapie symbol, który uzupełni informacje radarowe. Przy czym aplikacja wykorzystuje GPS i kompas, dzięki temu użytkownik musi jedynie skierować urządzenie w stronę lecącego obiektu. Od wysłania informacji do jej dostarczenia mija od 2 do 7 sekund. Z kolei do ostrzegania ludności o atakach powietrznych służy aplikacja Powitriana trywoha (Повітряна тривога) (Ajax Systems, 2022).

Sami wojskowi mają być zadziwieni skutecznością ePPo, rzekomo miała pomóc przechwycić wiele celów, w szczególności pocisków manewrujących lecących na niskiej wysokości (gdyż te są trudne do wykrycia za pomocą radarów) oraz w sytuacji przeciążenia OPL zmasowanymi uderzeniami. Przykładowo, w październiku 2022 r. dzięki temu, że kilku obywateli przekazało informację za pomocą ePPo udało się zestrzelić pocisk Kalibr, choć leciał na niskiej wysokości i wykorzystywał ukształtowanie terenu do skrywania swojej obecności.

Autoryzacja użytkownika odbywa się poprzez aplikację Diia. ePPo jest dostępne na urządzenia z systemami operacyjnymi Android i iOS. Według stanu na koniec marca 2023 r. aplikację pobrało 330 tys. użytkowników (Danylov, 2022a; Sabbagh, 2022).

Nie sposób nie wspomnieć o kilkukrotnie już przywoływanej aplikacji Diia (Дія), która daje dostęp do cyfrowych usług publicznych, odpowiednik polskiego mObywatela. Jeszcze przed rosyjską inwazją w lutym 2022 r. Ukraina realizowała ambitne reformy cyfryzacji. Był to jeden z elementów, który w warunkach wojny umożliwiał zapewnienie ciągłości funkcjonowania państwa. Z aplikacji korzysta obecnie ok. 20 mln Ukraińców (mObywatel ma ok. 15 mln użytkowników).

Aplikacja oferuje dostęp do ponad 130 usług, z czego ponad 70 pojawiło się już po wybuchu wojny, w tym dotyczące obsługi osób wewnętrznie przesiedlonych, czy programu eOdbudowa. Nową funkcjonalnością ma być interaktywna mapa schronów. W aplikacji dostępne będą adres i zdjęcia schronu, dane o jego pojemności i rodzaju. Ponadto będzie można ocenić stan schronu, złożyć skargę lub sugestię. Władze państwowe i samorządowe będą zobowiązane do stałego aktualizowania informacji, a także monitorowania stanu i dostępności schronów (Міністерство цифрової трансформації України, 2023a; 2023b; 2023c).

Poprzez aplikację można też kupować wojskowe obligacje, czy grać w grę, w której można wcielić się w operatora drona i przekazywać darowizny na rzecz tzw. „Armii Dronów". Poza tym w 2023 r. wprowadzono możliwość rejestracji wojskowej, w tym możliwość spełnienia obowiązku podania swojego miejsca przebywania na potrzeby ewentualnego powołania i mobilizacji. W styczniu 2024 r. Werchowna Rada przyjęła ustawę, która wprowadza digitalizację rejestru poborowych i rezerwistów. Jest to istotne w kontekście uchylania się od służby wojskowej i obaw społecznych o rozsyłanie wezwań do wojska poprzez Diia, choć wcześniej wicepremier Fedorow zapewniał, że wezwania nie będą w ten sposób wysyłane (BBC News Україна, 2023; TehnoFan, 2023; АрміяInform, 2024).

W wojnie rosyjsko-ukraińskiej powszechnie wykorzystywane są też komunikatory znane wielu użytkownikom telefonów na całym świecie. Korzystają z nich obie strony konfliktu, choć w większym stopniu Ukraińcy, co wynika z ograniczeń po stronie rosyjskiej, o których będzie mowa w dalszej części. Wykorzystywany jest Signal uznawany za bezpieczny komunikator do komunikacji prywatnej (o charakterze otwarto źródłowym), jak też WhatsApp. Żołnierze tworzą grupy, na których wymieniają się informacjami, np. o zlokalizowanych wysokowartościowych celach, co umożliwia szybką reakcję najbliższej jednostki (The Economist, 2023).

Aplikacje te nie spełniają wojskowych standardów bezpieczeństwa, są raczej substytutem brakujących wojskowych środków łączności, jak radiostacje taktyczne. Niemniej warto zauważyć, że łączność radiowa może być zagłuszana przy pomocy środków WRE, a komunikatory wykorzystują połączenie internetowe, a te Ukraińcy zapewniają sobie na terenach walk za pomocą terminali Starlink, które bywają trudne do zakłócenia i namierzenia. Częściowym rozwiązaniem problemu wykorzystania niewojskowej łączności ma być projekt HIMERA opracowany w ramach klastra Brave1. Jest to radio, które ma być wykonane z tanich komponentów, a jednocześnie odporne ma zakłócenia przez środki WRE (Defense Express, 2023).

Aplikacją, która może pomóc rozliczyć zbrodnie wojenne jest Dattalion. Jest to baza danych ze zdjęciami i filmami, zawiera relacje naocznych świadków. Narzędzie dostarcza dowody na rosyjskie zbrodnie na trzech poziomach: a) źródła oficjalne, np. od urzędników, b) źródła zaufane (dziennikarze i uwiarygodnione osoby), c) naoczni świadkowie i niezweryfikowane źródła (istnieje możliwość anonimowego

przesłania materiałów). Według stanu na kwiecień 2023 r. w bazie dostępnych jest ponad 4400 materiałów wideo, 19500 zdjęć, 120 relacji świadków. Baza danych, połączona ze stroną Dattalion, to Dysk Google. Aplikacja prowadzona jest przez 100 wolontariuszy ukraińskich i międzynarodowych, z czego 98% to kobiety, a 48% przebywa w Ukrainie (Heugas, 2022; Duszczyk 2023). Podobny cel ma też aplikacja #RussianWarCrimes (Офіс Генерального прокурора).

Aplikacje wykorzystywane przez Rosję

Rosja również posiada silny sektor IT, wielu utalentowanych informatyków, którzy opracowali liczne innowacje, które nie są tylko kopią zachodnich odpowiedników (np. Telegram, VK, Yandex). Jednak agresja na Ukrainę nie spowodowała mobilizacji społecznej i wsparcia wojska, wręcz odwrotnie, zwiększoną migrację, a po ogłoszeniu mobilizacji we wrześniu 2022 r. wręcz exodus. Oficjalne dane rosyjskiego rządu wskazują, że na koniec 2022 r. z Rosji wyjechało na stałe co najmniej 100 tysięcy specjalistów IT, czyli około 10% wszystkich pracowników branży. Prawdopodobnie dane te są istotnie zaniżone. Organizacja pozarządowa „OK Russians", na podstawie ankiet wśród opuszczających kraj z powodu wojny zidentyfikowała, że ok. 30% emigrantów to fachowcy sektora IT (Bryc, 2022; Позычанюк, Дадашова, 2023).

Rosja w swojej wojnie przeciwko Ukrainie wykorzystuje przede wszystkim rozwiązania typowo wojskowe, jak systemy BMS, opracowane przez rosyjski kompleks wojskowo-przemysłowy przy udziale Sił Zbrojnych Federacji Rosyjskiej (SZ FR). Jak wskazuje M. Korowaj pojawiają się informacje o propozycjach wdrożenia cyfrowych rozwiązań w SZ FR, ale są też informacje o nieprawidłowościach i zaniedbaniach, np. w zakresie nowoczesnych środków łączności, które są piętą achillesową rosyjskiej armii (pomimo wysp nowoczesności) (Korowaj, 2023). Rosja do rozwijania nowych technologii wojskowych wykorzystuje Fundusz Perspektywicznych Badań (mający być odpowiednikiem amerykańskiej DARPA) oraz wojskowe innowacyjne technopolis ERA, jednak niewiele jest informacji o rzeczywistych wdrożeniach.

Jeśli chodzi o systemy BMS, w SZ FR funkcjonuje szereg tego typu rozwiązań, a do najbardziej zaawansowanych zalicza się Andromeda-D wykorzystywany przez Wojska Powietrzno-Desantowe (WDW). System ten obejmuje m.in. wszystkie szczeble dowodzenia, elektroniczne mapy, prezentowanie na ekranie danych z rozpoznania, obliczanie współrzędnych dla celu (uwzględniając np. pogodę) i przekazywanie gotowych koordynatów, możliwość wideokonferencji. Andromeda-D wykorzystuje łączność satelitarną (zapewnianą przez własne satelity) oraz rosyjski system nawigacji. Jak zapewniają Rosjanie ma się cechować odpornością na działania WRE. Jako system wojskowy jest on postawiony wyłącznie na urządzeniach wojskowych, takich jak tablety, które mogą być na wyposażeniu żołnierza lub zainstalowane w pojazdach, np. wozach bojowych piechoty (Ераносян, В., 2023).

Przykładem powszechnie dostępnej aplikacji jest Wojskowy bank polowy. Jest to aplikacja mobilna dla personelu wojskowego umożliwiająca przeprowadzanie transakcji. Ma zapewniać działanie także w warunkach zakłóceń w sektorze bankowym oraz wysoki poziom bezpieczeństwa i ochrony danych. Transakcje finansowe mają być szyfrowane i przechowywane na bezpiecznych serwerach. Aplikacja pozwala także na dokonywanie analiz i statystyk na temat wykorzystania zasobów finansowych żołnierzy (Play-Side.ru).

Niewielkie wykorzystanie aplikacji mobilnych wynika m.in. z zakazu używania prywatnych smartfonów i innych „inteligentnych" urządzeń w SZ FR wprowadzonego w 2019 r. (Решетникова, 2022). W praktyce jednak rosyjscy żołnierze korzystają z własnych telefonów, co dobrze było widoczne na chwilę przed rosyjską inwazją. Aplikacja Google Maps pokazywała rosyjskie wojska ustawiające się na pozycje do inwazji na Ukrainę jako korki uliczne, gdyż żołnierze mieli przy sobie telefony z tą aplikacją.

Po stronie rosyjskiej należy wspomnieć o chatbotach rosyjskiego komunikatora Telegram, które pozwalają donosić na osoby krytykujące reżim oraz zgłaszać antyrządowe treści. Tego typu rozwiązania uruchomiono już w Kraju Nadmorskim i obwodzie biełgorodzkim (Antoniuk, 2023).

Wobec masowego korzystania przez Ukrainę z Palantir Edge AI czy własnych aplikacji takich jak Delta czy Kropyva pojawiają się pytania czy Rosja dysponuje „rosyjskim Palantirem"? SZ FR dostrzegają znaczenie świadomości sytuacyjnej i szybkości przepływu informacji na współczesnym polu walki, co wiadomo z dokumentów strategicznych i doktrynalnych oraz wypowiedzi rosyjskich wojskowych. Jednak jak wynika z rozmów portalu *Moskowskij Komsomolec* z rzekomym przedstawicielem rosyjskiego resortu obrony, choć w SZ FR również istnieją systemy gromadzenia i analizy danych, to jednak pozostają daleko w tyle za możliwościami Palantira. Wynikać to ma nie z braku kadr programistycznych, ale raczej z niechęci po stronie wojska, bo choć zwierzchnicy wiele mówią o digitalizacji pola walki, to wojsko wciąż jest od tego dalekie, pozostaje sceptyczne m.in. z uwagi na brak odpowiednich kadr, które potrafiłyby efektywnie wykorzystywać tego typu zaawansowane narzędzia. Innymi problemami są łączność oraz brak interoperacyjności między różnymi rodzajami wojsk, a są to kluczowe elementy, aby skutecznie wykorzystać tego typu narzędzia wspierające świadomość sytuacyjną. Rosyjska armia jest aparatem wysoce scentralizowanym, któremu brakuje synchronizacji, elastyczności i zdolności do prowadzenia połączonych operacji na dużą skalę. Sytuacja ma lepiej wyglądać w rosyjskich instytucjach bezpieczeństwa takich jak Federalna Służba Bezpieczeństwa, Federalna Służba Podatkowa i Ministerstwo ds. Sytuacji Nadzwyczajnych, które szerzej wykorzystują systemy analityczno-informacyjne (Петрушова, 2022).

Aplikacje mobilne w obszarze obronności w Polsce

Również w Siłach Zbrojnych RP wprowadzono do użytku różnego typu aplikacje (m.in. Żołnierz RP, TAK, #OTrening i #OTakcja), które pozwalają wspomóc wymianę informacji, szkolenie, świadomość sytuacyjną (MON, 2016; DKWOC, 2022; DKWOC, 2023, Szopa, 2023). Planowany jest rozwój krajowego systemu BMS (Dmitruk, 2023). Większe wykorzystanie aplikacji mobilnych może wspomóc zwiększenie zdolności C4ISR. Stan pokoju nie wymaga doraźnych szybkich rozwiązań, ale też nie wywiera presji na elastyczność i większą skłonność do ryzykownych innowacyjnych rozwiązań. Jednocześnie szersze wdrożenie tego typu rozwiązań może wiązać się z wyzwaniami w zakresie testowania, badań kwalifikacyjnych, certyfikacji, akredytacji urządzeń i oprogramowania.

W obliczu doświadczeń płynących z Ukrainy, konieczne jest zwiększenie digitalizacji Sił Zbrojnych RP, w tym przy wykorzystaniu aplikacji mobilnych. W tym celu należałoby alokować na ten cel odpowiednie środki finansowe i osobowe oraz efektywnie zarządzać mechanizmami rozwoju technologii takimi jak:

a) badania naukowe i prace rozwojowe w dziedzinie obronności;
b) opracowanie przez Siły Zbrojne RP własnymi zasobami, także we współpracy z uczelniami wojskowymi i wojskowymi instytutami badawczymi (np. jako zadanie zlecone);
c) nowe mechanizmy innowacji obronnych takie jak Pilna Potrzeba Innowacyjna, program rozwoju technologii podwójnego zastosowania IDA;
d) a w zakresie przetestowania i porównania ukraińskich i polskich narzędzi także w ramach projektu Batalion przyszłości i ćwiczenia *Field Experimentation Exercise* (Palowski, 2023).

Wnioski z wykorzystania aplikacji mobilnych w konflikcie zbrojnym

Przeprowadzona analiza potwierdziła postawioną hipotezę. Aplikacje mobilne jako element digitalizacji zmieniają pole walki, są jedną z obserwowanych innowacji militarnych. Aplikacje te zwiększają świadomość sytuacyjną i wspierają inne zdolności operacyjne, umożliwiają lepszą ochronę ludności, materializują koncepcje obrony powszechnej oraz odporności państwa i społeczeństwa. W dalszej części autor formułuje wnioski z wykorzystania aplikacji mobilnych w warunkach wojennych, jak również pochyla się nad kwestią tego rodzaju aplikacji na gruncie polskim.

Na podstawie powyższego przeglądu aplikacji autor formułuje następujące wnioski własne oraz oparte o inne źródła:

- narzędzia zwiększające świadomość sytuacyjną wspierają zdolności wojskowe, pozwalają niwelować przewagę przeciwnika, wspierają ochronę

ludności, urzeczywistniają koncepcje powszechnej obrony oraz odporności państwa i społeczeństwa;
- w Ukrainie, tak jak w rozwiniętym świecie, motorem innowacji jest sektor cywilny oraz następuje adaptacja rozwiązań cywilnych do zastosowań wojskowych;
- Ukraina opracowując swoje aplikacje mobilne i inne innowacje (np. drony) częściowo odeszła od klasycznego B+R, gdyż konieczne były natychmiastowe rozwiązania;
- do pewnego stopnia bezpieczeństwo wykorzystania aplikacji (poufność, integralność) zapewnia uwierzytelnianie wieloskładnikowe oraz przypisanie urządzeń do konkretnych żołnierzy i jednostek wojskowych;
- bezpieczeństwo danych zwiększa przechowywanie, przetwarzanie i zarządzanie nimi w chmurze obliczeniowej;
- dostrzegana jest potrzeba standaryzacji, np. protokołów szyfrowania danych, ich wymiany i przechowywania; po stronie ukraińskiej pojawiają się też obawy, że Palantir zdominuje krajowe systemy (Мельник, 2022b);
- w SZU funkcjonuje wiele systemów szczebla taktycznego, ale dostrzega się deficyt na poziomie operacyjnym (Мельник, 2022a);
- potrzebne jest dostostosowane do nowej rzeczywistości przepisów dotyczących ochrony informacji oraz konieczne jest uproszczenie przepisów wojskowych i ochrony informacji, aby nie zniechęcić start-upów, które obecnie są głównym źródłem innowacji (Мельник, 2022b).

BIBLIOGRAFIA

[1] Ajax Systems, 2022. The Air Alert app is now available for Android and Ios [online]. Dostępne pod adresem: https://ajax.systems/blog/zastosunok-povitryana-trivoga/ [dostęp: 25 stycznia 2024].

[2] Antoniuk, D., 2023. Russian region launches chatbot to report 'extremist' neighbours, Recorded Future [online]. Dostępne pod adresem: https://therecord.media/russian-region-primorsky--krai-snitching-chatbot [dostęp: 12 stycznia 2024].

[3] Axe, D., 2022. There's A Good Reason the Russian Air Force Is Faltering. Ukrainian Air-Defense Crews Have Better Apps, Forbes [online]. Dostępne pod adresem: https://www.forbes.com/sites/davidaxe/2022/10/18/theres-a-good-reason-the-russian-air-force-is-faltering-ukrainian-air-defense-crews-have-better-apps [dostęp: 15 stycznia 2024].

[4] BBC News Україна, 2023. Чи справді через "Дію" видаватимуть військовий квиток та повістку в армію [online]. Dostępne pod adresem: https://www.bbc.com/ukrainian/features-64455513 [dostęp: 15 stycznia 2024].

[5] Bohrn, B., 2023. Four Tech Lessons Learned from the Ongoing War in Ukraine, Bertelsmann Stiftung [online]. Dostępne pod adresem: https://globaleurope.eu/europes-future/four-tech-lessons-learned-from-the-ongoing-war-in-ukraine/ [dostęp: 15 stycznia 2024].

[6] Bryc A., 2022. Rosjanie w pośpiechu wyjeżdżają z ojczyzny. A może uciekają? Polityka.pl. [online]. Dostępne pod adresem: https://www.polityka.pl/tygodnikpolityka/swiat/2165655,1,rosjanie-w-pospiechu-wyjezdzaja-z-ojczyzny-a-moze-uciekaja.read [dostęp: 15 stycznia 2024].

[7] Danylov, O., 2022a, ePPO – a mobile application for informing about cruise missiles and kamikaze drones, Mezha [online]. Dostępne pod adresem: https://mezha.media/en/2022/10/14/eppo-a-mobile-application-for-informing-about-cruise-missiles-and-kamikaze-drones/ [dostęp: 15 stycznia 2024].

[8] Danylov, O., 2022b. The unique Ukrainian situational awareness system Delta was presented at the annual NATO event, Mezha [online]. Dostępne pod adresem: https://mezha.media/en/2022/10/28/the-unique-ukrainian-situational-awareness-system-delta-was-presented-at-the-annual-nato-event/ [dostęp: 15 stycznia 2024].

[9] Decyzja Nr 94/MON Ministra Obrony Narodowej z dnia 19 września 2023 r. w sprawie testowania rozwiązań technicznych w ramach Pilnej Potrzeby Innowacyjnej (Dz.Urz.MON poz. 109).

[10] Decyzja Nr 94/MON Ministra Obrony Narodowej z dnia 19 września 2023 r. w sprawie testowania rozwiązań technicznych w ramach Pilnej Potrzeby Innowacyjnej (Dz.Urz. MON poz. 109).

[11] Defense Express, 2023. HIMERA Created a Radio to Keep Ukrainian Drone Operators „Invisible" to russian SIGINT [online]. Dostępne pod adresem: https://en.defence-ua.com/weapon_and_tech/himera_created_a_radio_to_keep_ukrainian_drone_operators_invisible_to_russian_sigint-8214.html [dostęp: 17 stycznia 2024].

[12] Dmitruk, T., 2023. Decyzje dotyczące wyboru system BMS dla czołgów Abrams i KTO Rosomak, Dziennik Zbrojny [online]. Dostępne pod adresem: https://dziennikzbrojny.pl/aktualnosci/news,1,11944,aktualnosci-z-polski,decyzje-dotyczace-wyboru-system-bms-dla-czolgow-abrams-i-kto-rosomak [dostęp: 14 stycznia 2024].

[13] Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, 2022. DKWOC prezentuje TAK [online]. Dostępne pod adresem: https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/dkwoc-prezentuje-tak/ [dostęp: 15 stycznia 2024].

[14] Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni, 2023. DKWOC stworzyło aplikację Żołnierz RP [online]. Dostępne pod adresem: https://www.wojsko-polskie.pl/woc/articles/aktualnosci-w/dkwoc-stworzylo-aplikacje-zolnierz-rp/ [dostęp: 15 stycznia 2024].

[15] Duszczyk, M., 2023. Rekordy dezinformacji w sieci. Te firmy tworzą bat na manipulacje, Rzeczpospolita [online]. Dostępne pod adresem: https://cyfrowa.rp.pl/biznes-ludzie-startupy/art39125841-rekordy-dezinformacji-w-sieci-te-firmy-tworza-bat-na-manipulacje [dostęp: 15 stycznia 2024].

[16] Focus, 2022. Давид розриває Голіафа: чому технологію Palantir у ЗСУ можна порівняти з наявністю ядерної зброї [online]. Dostępne pod adresem: https://focus.ua/uk/voennye-novosti/542162-david-razryvaet-goliafa-pochemu-tehnologiya-palantir-v-vsu-sravnima-s-nalichiem-yaderno-oruzhiya [dostęp: 14 stycznia 2024].

[17] Heugas, A., 2022. DATTALION: Information Sharing in Times of War, Salzburg Global [online]. Dostępne pod adresem: https://www.salzburgglobal.org/news/latest-news/article/dattalion-information-sharing-in-times-of-war [dostęp: 15 stycznia 2024].

[18] Jones, G., Egan, J., Rosenbach, E., 2023. Advancing in Adversity: Ukraine's Battlefield Technologies and Lessons for the U.S., Harvard Kennedy School Belfer Center, 31.07.2023 [online]. Dostępne pod adresem: https://www.belfercenter.org/publication/advancing-adversity-ukraines-battlefield-technologies-and-lessons-us [dostęp: 14 stycznia 2024].

[19] Kistol, K., 2022. Digital weapons of war: applications and software that help Ukraine to win, War.Ukraine.UA [online]. Dostępne pod adresem: https://war.ukraine.ua/articles/digital-weapons-of-war-applications-and-software-that-help-ukraine-to-win/ [dostęp: 14 stycznia 2024].

[20] Korowaj M., 2023. Rosyjska armia przyszłości. Moskwa wdraża lekcje z wojny na Ukrainie [ANALIZA], Defence24 [online]. Dostępne pod adresem: https://defence24.pl/sily-zbrojne/

rosyjska-armia-przyszlosci-moskwa-wdraza-lekcje-z-wojny-na-ukrainie-analiza [dostęp: 15 stycznia 2024].

[21] Kovacs, E., 2022. Ukraine's Delta Military Intelligence Program Targeted by Hackers, Security Week [online]. Dostępne pod adresem: https://www.securityweek.com/ukraines-delta-military-intelligence-program-targeted-hackers/ [dostęp: 15 stycznia 2024].

[22] Maçães, B., 2023, How Palantir Is Shaping the Future of Warfare, The Time [online]. Dostępne pod adresem: https://time.com/6293398/palantir-future-of-warfare-ukraine/ [dostęp: 14 stycznia 2024].

[23] Malich, Y., 2022. Do IT like Ukraine, IT Ukraine Association [online]. Dostępne pod adresem: https://itukraine.org.ua/files/reports/2022/DoITLikeUkraine2022_EN.pdf [dostęp: 13 stycznia 2024].

[24] Ministerstwo Obrony Narodowej, 2016. Nowatorskie aplikacje dla OT [online]. Dostępne pod adresem: https://www.gov.pl/web/obrona-narodowa/nowatorskie-aplikacje-dla-ot-2 [dostęp: 15 stycznia 2024].

[25] Palowski J., 2023. „Grupa Bojowa Przyszłości" w Żelaznej Dywizji, Defence24 [online]. Dostępne pod adresem: https://defence24.pl/sily-zbrojne/ida-zmiany-w-wojsku-polskim-eksperymentalne-cwiczenia [dostęp: 14 stycznia 2024 r.].

[26] Play-Side.ru. Военно-полевой банк: мобильное приложение для военнослужащих [online]. Dostępne pod adresem: https://play-side.ru/обзоры/военно-полевой-банк-мобильное-прилож [dostęp: 15 stycznia 2024].

[27] Rosengren, O., 2023. Network-centric Warfare in Ukraine: The Delta System, Grey Dynamics [online]. Dostępne pod adresem: https://greydynamics.com/network-centric-warfare-in-ukraine-the-delta-system/ [dostęp: 15 stycznia 2024].

[28] Sabbagh, D., 2022, Ukrainians use phone app to spot deadly Russian drone attacks, The Guardian [online]. Dostępne pod adresem: https://www.theguardian.com/world/2022/oct/29/ukraine-phone-app-russia-drone-attacks-eppo [dostęp: 15 stycznia 2024].

[29] Schmidt, E., 2023. "Innovation Power", Foreign Affairs, 28.02.2023 [online]. Dostępne pod adresem: https://www.foreignaffairs.com/united-states/eric-schmidt-innovation-power-technology-geopolitics [dostęp: 14 stycznia 2024].

[30] Szopa, M., 2023, TAK – system mapowy jak szwajcarski scyzoryk [ANALIZA], Defence24 [online]. Dostępne pod adresem: https://defence24.pl/technologie/tak-system-mapowy-jak-szwajcarski-scyzoryk-analiza [dostęp: 15 stycznia 2024].

[31] TehnoFan, 2023. У "Дія" все ж таки запустили нову функцію: багато українців тепер зможуть стати військовими [online]. https://tehnofan.com.ua/2023/04/09/u-diya-vse-zh-taky-zapustyly-novu-funktsiyu-bahato-ukrayintsiv-teper-zmozhut' -staty-viys' kovymy/ [dostęp: 15 stycznia 2024].

[32] The Economist, 2023. The war in Ukraine shows how technology is changing the battlefield, 03.07.2023 [online]. Dostępne pod adresem: https://www.economist.com/special-report/2023/07/03/the-war-in-ukraine-shows-how-technology-is-changing-the-battlefield [dostęp: 14 stycznia 2024].

[33] The Kyiv Independent, 2023. Ukraine to introduce Delta situational awareness system for military [online]. Dostępne pod adresem: https://kyivindependent.com/government-introduces-nato-standard-delta-management-defense-system/ [dostęp: 15 stycznia 2024].

[34] Ukrainian Military Center, 2022. Ukraine unveiled its own Delta situational awareness system [online]. Dostępne pod adresem: https://mil.in.ua/en/news/ukraine-unveiled-its-own-delta-situational-awareness-system/ [dostęp: 15 stycznia 2024].

[35] War.Ukraine.UA, 2023. Ukrainian military innovations proved effective – and they're changing modern warfare. Here is how [online]. Dostępne pod adresem: https://war.ukraine.ua/articles/ukrainian-innovations-are-changing-approaches-to-modern-warfare/ [dostęp: 15 stycznia 2024].

[36] АрміяInform, 2024. Військовий облік та отримання УБД: Рада ухвалила законопроєкт про цифровізацію армії [online]. Dostępne pod adresem: https://armyinform.com.ua/2024/01/16/vijskovyj-oblik-ta-otrymannya-ubd-rada-uhvalyla-zakonoproyekt-pro-czyfrovizacziyu-armiyi/ [dostęp: 17 stycznia 2024].

[37] Бойченко, А., 2022. Софт для богів війни та «вбивця» російських позицій «Валькірія». Як «Армія SOS» наближає нашу перемогу, #ШоТам [online] . Dostępne pod adresem: https://shotam.info/soft-dlia-bohiv-viyny-ta-vbyvtsia-rosiyskykh-pozytsiy-valkiriia-yak-armiia-sos-nablyzhaie-nashu-peremohu/ [dostęp: 15 stycznia 2024].

[38] Ераносян, В., 2023. Туманна «Андромеда» только для глаз противника, ЗВЕЗДА [online]. Dostępne pod adresem: https://zvezdaweekly.ru/news/20208261143-q1xUL.html [dostęp: 15 stycznia 2024].

[39] Мельник, Т., 2022a. Жалюча «Кропива». Як українське програмне забезпечення для артилеристів впливає на перебіг війни, Forbes [online]. Dostępne pod adresem: https://forbes.ua/innovations/zhalyucha-kropiva-yak-ukrainske-programne-zabezpechennya-dlya-artileristiv-vplivae-na-khid-viyni-22072022-7054 [dostęp: 15 stycznia 2024].

[40] Мельник, Т., 2022b, IT-хаос на службі ЗСУ. Сотні тисяч військових користуються різним софтом, який розробили волонтери. Чи небезпечна така децентралізація, Forbes [online]. Dostępne pod adresem: https://forbes.ua/innovations/it-khaos-na-sluzhbi-zsu-sotni-tisyach-viyskovikh-koristuyutsya-riznim-softom-yakiy-rozrobili-volonteri-chi-nebezpechna-taka-detsentralizatsiya-14112022-9700 [dostęp: 14 stycznia 2024].

[41] Мельник, Т., 2023. Компанія Palantir забезпечить підтримку української армії в сфері IT, Forbes [online]. Dostępne pod adresem: https://forbes.ua/news/amerikanska-kompaniya-palantir-domovlyaetsya-pro-spilni-proekti-z-ukrainskimi-viyskovimi-rozrobkami-16032023-12411 [dostęp: 14 stycznia 2024].

[42] Міністерство цифрової трансформації України, 2022. Допоможи ЗСУ знищити окупанта: Мінцифра запускає чатбот єВорог [online]. Dostępne pod adresem: https://thedigital.gov.ua/news/dopomozhi-zsu-znishchiti-okupanta-mintsifra-zapuskae-chatbot-evorog [dostęp: 15 stycznia 2024].

[43] Міністерство цифрової трансформації України, 2023a. Перереєстрація авто, е-Підприємець та новий дизайн Дії: які послуги презентували на Diia Summit [online]. Dostępne pod adresem: https://thedigital.gov.ua/news/perereestratsiya-avto-e-pidpriemets-ta-noviy-dizayn-dii-yaki-poslugi-prezentuvali-na-diia-summit [dostęp: 15 stycznia 2024].

[44] Міністерство цифрової трансформації України, 2023b. У Дії з'явиться інтерактивна мапа укриттів: Уряд ухвалив постанову [online]. Dostępne pod adresem: https://thedigital.gov.ua/news/u-dii-zyavitsya-interaktivna-mapa-ukrittiv-uryad-ukhvaliv-postanovu [dostęp: 15 stycznia 2024].

[45] Міністерство цифрової трансформації України, 2023c. Понад 30 послуг у Дії та розвиток Defence Tech: головні досягнення Мінцифри за 2023 рік [online]. Dostępne pod adresem: https://thedigital.gov.ua/news/ponad-30-poslug-u-dii-ta-rozvitok-defence-tech-golovni-dosyagnennya-mintsifri-za-2023-rik [dostęp: 15 stycznia 2024].

[46] Офіс Генерального прокурора. Якщо ви стали потерпілим або свідком воєнних злочинів Росії – фіксуйте та надсилайте докази! [online]. Dostępne pod adresem: https://warcrimes.gov.ua [dostęp: 30 stycznia 2024].

[47] Петрушова, С., Главный секрет Пентагона: разведчик описал американскую программу слежения MetaConstellation, Московский Комсомолец [online]. Dostępne pod adresem: https://www.mk.ru/politics/2022/11/21/razvedchik-opisal-amerikanskuyu-programmu-meta constellation-pozvolyayushhuyu-vsu-nakhodit-rossiyskie-celi.html [dostęp: 14 stycznia 2024].

[48] Позычанюк В., Дадашова К., 2023. „Куда уезжают айтишники, доля фиктивных сделок на крипторынке и как вести расследования в интернете", The Bell [online]. Dostępne pod adresem: https://thebell.io/kuda-uezzhayut-aytishniki-dolya-fiktivnykh-sdelok-na-kriptorynke-i-kak-vesti-rassledovaniya-v-internete [dostęp: 14 stycznia 2024 r.].

[49] Решетникова, М., 2022, Signal и клон WhatsApp: какими мессенджерами пользуются армии мира, РБК [online]. Dostępne pod adresem: https://trends.rbc.ru/trends/industry/62039ccf9a7947eb529ade24 [dostęp: 15 stycznia 2024].

[50] Сабадишина, Ю., 2022. Компанія Palantir вже має офіс в Україні, а її ПЗ використовують на фронті. 10 тез із репортажу Washington Post, DOU.ua [online]. Dostępne pod adresem: https://dou.ua/lenta/news/palantir-and-war-in-ukraine/ [dostęp: 14 stycznia 2024].

[51] Український мілітарний центр, 2023. Компанія Palantir забезпечить підтримку української армії в сфері IT [online]. Dostępne pod adresem: https://mil.in.ua/uk/news/kompaniya-palantir-zabezpechyt-pidtrymku-ukrayinskoyi-armiyi-v-sferi-it/ [dostęp: 14 stycznia 2024].