UNIWERSYTET JANA DŁUGOSZA W CZĘSTOCHOWIE
Res Politicae 2023, t. 15, s. 73–86

http://dx.doi.org/10.16926/rp.2023.15.04

Tomasz PĄCZKOWSKI
https://orcid.org/0000-0002-6124-6157
Uniwersytet Jana Długosza w Częstochowie

Wojna cybernetyczna – wskazówki z Ukrainy*

Streszczenie

Agresja Rosji na Ukrainę oznaczała jednocześnie wybuch wojny cybernetycznej, która toczy się za pośrednictwem Internetu praktycznie na całym świecie. Objęła ona wiele aspektów współczesnego życia – od trollingu po wykorzystanie technologii cybernetycznej bezpośrednio na polu bitwy. Współczesna broń konwencjonalna bez zastosowania zaawansowanej technologii cyfrowej staje się bardzo mało użyteczna, pozbawiona informacji o polu bitwy jest dramatycznie niecelna. Widać to wyraźnie na przykładzie Rosjan, którzy po wykorzystaniu zapasów inteligentnej amunicji bombardują i ostrzeliwują Ukrainę praktycznie na oślep, powodując duże straty wśród ludności cywilnej. Mamy również do czynienia z licznymi formami ataków cybernetycznych na kraje Unii Europejskiej. Rosyjscy hakerzy podejmują liczne próby ataków na strony i portale zarówno rządowe, jak i organizacji społecznych.

Słowa kluczowe: Internet, bezpieczeństwo, wojna cybernetyczna, zagrożenia, cyberprzemoc, cyberprzestępczość, inteligentna broń i amunicja.

Rozwój zagrożeń w cyberprzestrzeni

Lata 2020–2021 były okresem specyficznym, gdyż wraz z nastaniem epidemii koronawirusa proces przenoszenia się działalności zawodowej oraz kontaktów społecznych do Internetu uległ drastycznemu przyśpieszeniu. Oprócz zalet takiego rozwiązania powstało zagrożenie polegające na tym, że pozostając w domach i przenosząc swoje życiowe potrzeby na forum sieci, ludzie stali się bardziej podatni na wszelkiego typu cyberzagrożenia.

Tymczasem zbyt duża konsumpcja nowych technologii niesie ze sobą wiele zagrożeń. Najpopularniejszymi kanałami cyberataków, czyli ofensywnych dzia-

* Artykuł koresponduje z anglojęzycznym tekstem: R. Kochańczyk, T. Pączkowski, *Cybernetic warfare an element of modern military operations*, „Zeszyty Naukowe SGSP" 2023, t. 86, ss. 127–140.

łań w Internecie, których celem mogą być systemy informatyczne, sieci komputerowe lub urządzenia osobiste były:

— e-mail i komunikatory.
— dziury w systemie.
— USB (np. pendrive).
— portale społecznościowe.

Współczesne cyberataki coraz częściej wykorzystują nieświadomość internautów. Socjotechniki najczęściej praktykowane są przez osoby wykradające poufne dane i wiążą się z konsekwencjami dla użytkownika. Zagrożenie ciężko rozpoznać, a atak może być prowadzony przez długi czas. Ofiara często jest zmanipulowana, a atakujący może podawać się za kogoś innego lub wykorzystywać skradzioną tożsamość.

Według Rzecznika Ministra Koordynatora Służb Specjalnych Zespół CSiRT GOV[1] w ABW notuje zwiększoną ilość zgłoszeń incydentów komputerowych. Spośród najczęściej zgłaszanych incydentów można wskazać kampanie phishingowe, podszywanie się (spoofing), malware, skanowania czy ataki DDoS. Wymienione rodzaje cyberataków stanowią obecnie najpoważniejsze zagrożenia dla sieci i systemów teleinformatycznych[2].

Reakcją na wspomniane zagrożenia było wprowadzenie w Polsce stopnia alarmowego Charlie. Stopień alarmowy Charlie-CRP, aktywny na terenie całej Polski, jest trzecim z czterech stopni. Jak wyjaśnia Rządowe Centrum Bezpieczeństwa: „Stopień ten jest wprowadzany w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym w cyberprzestrzeni albo uzyskania wiarygodnych informacji o planowanym zdarzeniu”[3].

Współczesne siły zbrojne to nie tylko armie i konwencjonalne środki walki wykorzystywane na wielką skalę. Istotną częścią składową – jeśli nie pod względem liczby ludzi i sprzętu, to pod względem powagi realizowanych zadań oraz efektywności działania – są siły specjalne. Jest to wynik starań o zapewnienie zdolności szybkiej adaptacji sił zbrojnych państwa do tych nowych wyzwań i zagrożeń. W dobie konfliktów, w których stroną może stać się aktor pozbawiony podmiotowości prawno-międzynarodowej, nieposiadający stałego terytorium ani nawet jasno określonej bazy działania, siły zbrojne muszą przybierać postać pozwalającą na elastyczne reagowanie, z dużą precyzją, na pojawiające się nagle zagrożenia ze strony niewielkich, zdeterminowanych grup[4].

---

[1] CSIRT NASK to Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego, działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy z siedzibą w Warszawie.

[2] Portal GOV.pl Uwaga na zagrożenia w cyberprzestrzeni https://www.gov.pl/web/sluzby-specjalne/uwaga-na-zagrozenia-w-cyberprzestrzeni [dostęp: 10.08.2022].

[3] T. Siewko, Stopień alarmowy CHARLIE-CRP znów przedłużony w całej Polsce TVN24 [dostęp: 6.04.2022].

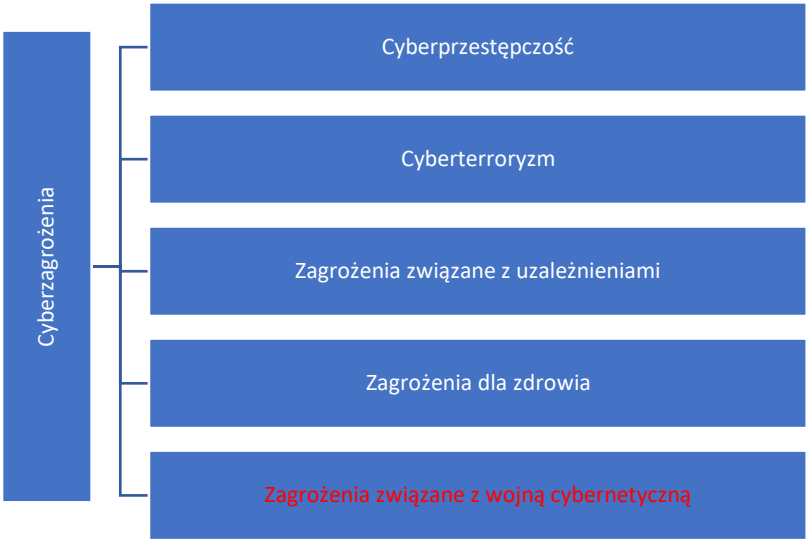
[4] Zob. R. de Wijk, *The Limits of Military Power*, [w:] *Terrorism and Counterterrorism. Understanding the New Security Enrolment*, eds. R.D. Howard, R.L. Sawyer, Guilford 2005, s. 452.

Elementy mające wpływ na bezpieczeństwo w cyberprzestrzeni

Problemy związane z cyberprzestępczością w dalszym ciągu są mało rozpowszechnione w naszym kraju. Aktualnie w przestrzeni nie funkcjonuje konkretna i jedyna definicja cyberprzestępczości. Na co dzień można spotkać zróżnicowane określenia, które używane są zamiennie np. przestępczość komputerowa, przestępczość związana z komputerami, przestępczość przy użyciu zaawansowanych technologii, przestępstwa związane z technologią cyfrową[5], przestępstwa związane z technologią przetwarzania informacji, przestępstwa internetowe[6].

Dotychczasowo można było scharakteryzować trzy generacje cyberprzestępstw, tj.:

— pierwsza generacja cyberprzestępstw obejmowała zamachy skierowane na komputer, sieci komputerowe i dane;
— druga generacja była związana z rozwojem sieci teleinformatycznych i atakami na ich integralność i dostępność przez tzw. hakerów;
— trzecia – występująca w chwili obecnej – jest związana z zauważalnym procesem automatyzacji cyberprzestępczości będącej między innymi efektem wykorzystania specjalnego oprogramowania[7].



Rys. 1. Klasyfikacja współczesnych cyberzagrożeń

Źródło: opracowanie własne.

[5] Komunikat Komisji do Parlamentu europejskiego, Rady oraz Komitetu Regionów – *W kierunku ogólnej strategii zwalczania cyberprzestępczości*, {SEK(2007) 641}{SEK(2007) 642}, http://eur-lex.europa.eu [dostęp: 30.05.2017].

[6] Więcej np. A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 33 i nast.

[7] Por. M. Siwicki, *Cyberprzestępczość*, Warszawa 2013, s. 2.

Według Macieja Siwickiego w niektórych opracowaniach wyróżnia się również czwartą generację cyberprzestępczości, charakteryzującą się coraz powszechniejszym wykorzystywaniem przez sprawcę narzędzi hakerskich oraz dalszym rozwojem podziemia komputerowego. Powoduje to poszerzanie się kręgu osób, dla których dokonanie cyberprzestępstwa wymaga już nie szczególnych zdolności i umiejętności, ale tylko dostępu do przestępczych cybernarzędzi.

Atak Rosjan na Ukrainę uwidocznił pojawienie się kolejnej generacji cyberzagrożeń – związanych z wojną cybernetyczną.

Nowe zagrożenia płynące z korzystania z Internetu w wojnie konwencjonalnej

Zagrożenia, jakie niesie ze sobą korzystanie z Internetu dotychczas można było sklasyfikować, wyróżniając cztery podstawowe zagrożenia, a mianowicie:

1. Uzależnienie od Internetu;
2. Zagrożenia sprzętowe;
3. Niepożądany dostęp do danych;
4. Szkodliwe treści.

Trolle na wojnie

Wraz z rozpoczęciem wojny na Ukrainie walka na informacje w sieci osiągnęła niespotykaną dotąd skalę. Pojawiają się tysiące komentarzy popierających działania reżimu Władimira Putina lub oczerniających Ukrainę jako państwo, ale to nie wszystko. Obok wielkiej polityki nie brakuje zagrywek socjotechnicznych wymierzonych w społeczeństwo, które mają na celu wytworzenie w Polsce, dotychczas pomocnej i przyjaznej wobec naszego wschodniego sąsiada, nastrojów antagonistycznych[8].

Według ekspertów z Sentione, firmy zawodowo trudniącej się monitoringiem treści w Internecie, różne metody są wykorzystywane w kremlowskiej dezinformacji. Co gorsza – nie tylko kremlowskiej, ale też tej, która pochodzi z innych źródeł – na przykład nierzetelnych mediów. I przestrzega, by szczególnie uważać na:

— clickbaitowy[9] tytuł – niektóre portale chcą zarobić na wojnie i zwiększyć ruch na swojej stronie, więc będą przyciągać uwagę chwytliwymi tytułami na pograniczu kłamstwa,
— informacje, które wzbudzają skrajne emocje – szok, strach, gniew, ale też śmiech i radość, mają wysoki potencjał viralowy[10]. Dlatego informacja o za-

[8] P. Urbaniak, *Rosyjskie trolle atakują nową taktyką. Nie daj się podejść*, https://www.telepolis.pl/wiadomosci/wydarzenia/rosyjskie-trolle-polska-dezinformacja-hejt [dostęp: 25.07.2022].

[9] Clickbaitowy tytuł tekstu w postaci linku w mediach elektronicznych to taki, który jest zarazem intrygujący i niejasny, a więc skłaniający do kliknięcia.

[10] Virale to treści występujące w formie video, grafiki lub tekstu, których misja jest prosta: bardzo szybko się rozprzestrzenić i dotrzeć do jak największej liczby odbiorców.

blokowaniu dostępu do serwisu Pornhub w Rosji, która ostatecznie okazała się być fałszywa, tak szybko się rozprzestrzeniła. A w przypadku wojny spreparowanie treści szokujących i strasznych nie jest problemem,

— filmy, rolki i relacje w mediach społecznościowych również mają duży potencjał viralowy, nie tylko dlatego, że algorytmy tych platform są nastawione na promowanie treści video. Również my jako ludzie dużo intensywniej odbieramy treści video niż sam tekst,
— zdjęcia pochodzące z innych miejsc lub czasów – łatwo jest dokonywać manipulacji z pomocą archiwalnych materiałów, np. zdjęć z wojny w Jemenie prezentowanych jako zdjęcia z Kijowa. Media społecznościowe pozwalają szybko podawać informacje, ale niestety często brakuje czasu na weryfikację danych,
— deepfake[11] czyli sfabrykowany materiał video – bardzo łatwo teraz spreparować lub zmontować film tak, by ukazywał dowolne treści czy osoby w nieprawdziwych sytuacjach[12].

Przy korzystaniu z mediów społecznościowych, w tym z Twittera, podstawową zasadą jest sprawdzenie profilu użytkownika/rozmówcy, którego post wzbudził nasz niepokój: bardzo często rosyjskie trolle zakładają nowe konta, ponadto aktywne pozostają te, które w ciągu ostatnich dwóch lat negowały pandemię i akcję szczepień – teraz ich przekaz wymierzony jest np. w uchodźców. Czujność powinna wzbudzić liczba obserwujących dany profil – trollkonta często obserwuje góra kilku użytkowników (lub żaden) bądź też inne, powiązane z nim fejkowe profile[13].

Specjaliści od komunikacji internetowej ostrzegają przed działalnością prorosyjskich trolli, którzy masowo publikują i rozpowszechniają pomiędzy sobą na wszelkiej maści serwisach społecznościowych fałszywe informacje na temat ukraińskich uchodźców w Polsce.

Najbardziej popularnym tematem jest teraz nacisk na wywołanie negatywnych emocji i reakcji względem Ukraińców np. odnośnie wzrostu cen paliw czy produktów spożywczych w sklepach. Do tego dochodzi również podsycanie nienawiści na tle historii z ludobójstwem na Wołyniu i popularnością Bandery[14].

---

[11] Deepfake jest obróbką dźwięku i obrazu, która ma na celu utworzenie fałszywych obrazów i dźwięków przy użyciu technik z zakresu sztucznej inteligencji.

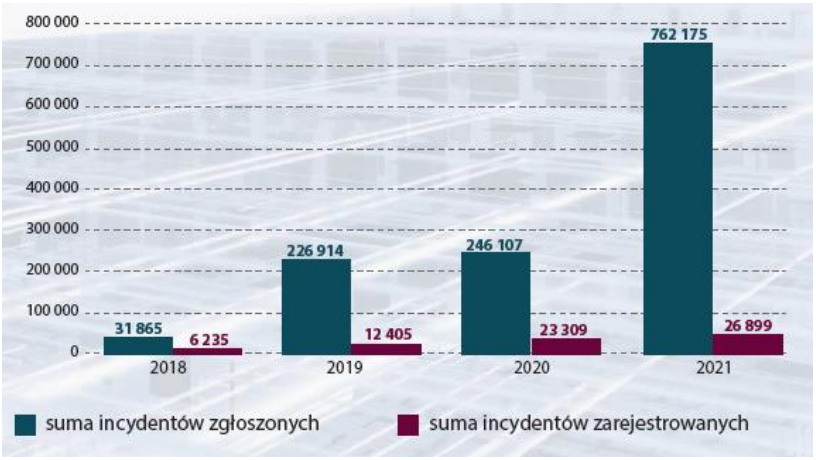
[12] J. Kralka, *Jak rozpoznać kremlowskiego trolla w polskim Internecie?*, https://bezprawnik.pl/jak-rozpoznac-kremlowskiego-trolla-w-polskim-internecie/ [dostęp: 10.07.2022].

[13] N. Bochyńska, *Wojna, trolle i fake newsy. Czyli na co zwracać uwagę w mediach społecznościowych*, https://publicystyka.ngo.pl/zanim-podamy-dalej-post [dostęp: 10.05.2022].

[14] Portal Geekweek, *Uważajcie na prorosyjskie trolle. Próbują nas skłócić z Ukraińcami*, https://geekweek.interia.pl/internet/news-uwazajcie-na-prorosyjskie-trolle-probuja-nas-sklocic-z-ukrai,nId,5907897 [dostęp: 23.06.2022].

Wojna informacyjna

W 2021 roku Zespół CSIRT GOV zarejestrował w sumie 762 175 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego, spośród których 26 899 zostało uznanych za incydenty. W 2021 roku zarejestrowano ponad trzykrotnie więcej zgłoszeń w stosunku do roku poprzedniego, gdzie w sumie zarejestrowano 246 107 zgłoszeń. Wzrost zarejestrowanych zgłoszeń wynika przede wszystkim z liczby alarmów generowanych przez system ARAKIS GOV. System ARAKIS GOV umożliwia identyfikowanie zagrożeń m in na podstawie dedykowanych sygnatur bezpieczeństwa.



Rys. 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych latach

Źródło: Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2021 roku. Zespół CSIRT GOV.

Z kolei RAND Corporation (Research ANd Development) – amerykański think tank i organizacja badawcza non-profit, pierwotnie sformowana dla potrzeb Sił Zbrojnych Stanów Zjednoczonych, przedstawiła wyniki raportu poświęconego analizie wpływu działań manipulacyjnych i ich skuteczności na rzecz kształtowania wyników wyborów w różnych częściach globu. Pierwszym wnioskiem płynącym z raportu jest stwierdzenie, że niezależnie od skuteczności tego wpływu faktem jest, że Kreml rozwinął bardzo mocno pakiet narzędzi, które dają potencjalną możliwość oddziaływania i mają zdolność, aby decydować o wynikach wyborów.

Badacze stwierdzili również, że państwa uznawane za autokratyczne – Rosja oraz Chiny – zaczęły wykorzystywać kanały informacyjne do uzyskania przewagi a także, że w ich przekonaniu są one uwikłane w wojną informacyjną z Zachodem, która – w ich opinii – została rozpętana przez Stany Zjednoczone wraz z ich sojusznikami[15].

[15] Raport Hostile Social Manipulation Present Realities and Emerging Trends, za: *Czy rosyjskiej dezinformacji należy się obawiać?* CyberDefence+ 24 https://cyberdefence24.pl/polityka-i-

Ataki na sieci komunikacyjne

Połączone sieci mogą być atakowane i zakłócane nie tylko przez państwa, ale także przez podmioty niepaństwowe, w tym rozproszone grupy, a nawet jednostki. Potencjalni przeciwnicy mogą również posiadać szeroki wachlarz możliwości. W ten sposób zagrożenie dla interesów USA może ulec znacznemu zwielokrotnieniu i będzie się zmieniać w miarę rozwoju coraz bardziej złożonych systemów i coraz szerszego rozpowszechniania wymaganej wiedzy fachowej.

Zatarte tradycyjne granice oddziaływania

Biorąc pod uwagę szeroki wachlarz możliwych przeciwników, broni i strategii, coraz trudniej jest odróżnić zagraniczne i krajowe źródła zagrożeń i działań IW (*information warfare*). Możesz nie wiedzieć, kto jest przez kogo atakowany lub kto nim kieruje. To znacznie komplikuje tradycyjne rozróżnienie ról między krajowymi organami ścigania z jednej strony, a krajowymi organami bezpieczeństwa i wywiadu z drugiej. Inną konsekwencją tego zacierania się zjawiska jest zanikanie wyraźnych rozróżnień między różnymi poziomami aktywności antypaństwowej, od przestępczości po działania wojenne.

Rozszerzona rola zarządzania percepcją

Możliwości agentów IW do manipulowania informacjami, które są kluczowe dla publicznego postrzegania, mogą wzrosnąć. Ponadto pojawia się możliwość, że same „fakty", zdarzenia mogą być manipulowane za pomocą technik multimedialnych i szeroko rozpowszechniane. I wprost przeciwnie, może wystąpić zmniejszona zdolność do budowania i utrzymywania krajowego poparcia dla kontrowersyjnych działań politycznych. Jedną z konsekwencji jest to, że przyszłe administracje USA mogą włączyć solidny komponent internetowy w ramach każdej publicznej kampanii informacyjnej.

Brak strategicznej inteligencji

Z różnych powodów tradycyjne metody zbierania i analizy danych wywiadowczych mogą mieć ograniczone zastosowanie w sprostaniu wyzwaniu strategicznego wywiadu (IW). Cele zbierania są trudne do zidentyfikowania, alokacja zasobów wywiadowczych jest trudna ze względu na szybko zmieniający się charakter zagrożenia, a luki w zabezpieczeniach i zestawy docelowe nie są jeszcze dobrze poznane. Podsumowując, Stany Zjednoczone mogą mieć trudności ze zidentyfikowaniem potencjalnych przeciwników, ich intencji i możliwości. Jedną z implikacji jest to, że potrzebne są nowe relacje organizacyjne w obrębie społeczności wywiadowczej oraz między tą społecznością a innymi podmiotami. Może być również wymagana restrukturyzacja ról i misji.

---

prawo/czy-rosyjskiej-dezinformacji-nalezy-sie-obwiac-okiem-amerykanskich-naukowcow-nie [dostęp: 17.05.2022].

TRUDNOŚĆ TAKTYCZNEJ OCENY ZAGROŻENIA I ATAKU

Ta cecha działań wojennych stwarza zupełnie nowe problemy w środowisku cyberprzestrzeni. Podstawowym problemem jest rozróżnienie między „atakami" a innymi zdarzeniami, takimi jak wypadki, awarie systemu lub hakowanie przez „poszukiwaczy mocnych wrażeń". Główną konsekwencją tej funkcji jest to, że Stany Zjednoczone mogą nie wiedzieć, kiedy trwa atak, kto go atakuje lub jak atak jest przeprowadzany.

Tak więc RAND Corporation zebrała i przedstawiła zasadnicze problemy wynikające z wojny informacyjnej.

Trudność budowania i utrzymywania koalicji

Wielu sojuszników USA i partnerów koalicyjnych będzie narażonych na ataki IW na ich podstawową infrastrukturę informacyjną. Na przykład uzależnienie od telefonów komórkowych w krajach rozwijających się może sprawić, że komunikacja telefoniczna w tych krajach będzie bardzo podatna na zakłócenia. Inne sektory na wczesnych etapach wykorzystywania rewolucji informacyjnej (np. energetyka i finanse) mogą również mieć słabe punkty, które przeciwnik może zaatakować, aby podważyć udział w koalicji. Takie ataki mogą również służyć zerwaniu „słabych ogniw" w realizacji planów koalicyjnych. Z drugiej strony, niepewni partnerzy koalicyjni, którzy pilnie potrzebują pomocy wojskowej, mogą chcieć zapewnienia, że amerykański plan rozmieszczenia w ich regionie własnych systemów uzbrojenia nie jest podatny na zakłócenia IW.

PODATNOŚĆ TERYTORIUM USA NA ATAKI

Wojna informacyjna nie ma linii frontu. Potencjalne pola bitwy znajdują się wszędzie tam, gdzie systemy sieciowe umożliwiają dostęp. Obecne trendy sugerują, że gospodarka Stanów Zjednoczonych będzie w coraz większym stopniu polegać na złożonych, połączonych ze sobą systemach kontroli sieci, takich jak rurociągi naftowe i gazowe, sieci elektryczne itp. Podatność tych systemów na ataki IW jest obecnie słabo poznana. Ponadto środki odstraszania i odwetu są niepewne i mogą opierać się na tradycyjnych instrumentach wojskowych oprócz zagrożeń IW[16].

W ostatnim okresie, kiedy dyrektor CIA Bill Burns pojawił się przed senacką komisją ds. wywiadu, aby mówić o sytuacji na Ukrainie, zapytano go o wykorzystywanie przez Rosję dezinformacji i przedstawianie własnego stanowiska jako instrumentów legitymizacji inwazji.

„To jest jedyna wojna informacyjna, którą, jak sądzę, Putin przegrywa" – odpowiedział Burns[17].

[16] Na podstawie: R.C. Molander, A. Riddile, P.A. Wilson, *Strategic Information Warfare A New Face of War* https://www.rand.org/pubs/monograph_reports/MR661.html.

[17] A. Demus, Ch. Paul, *Don't Sleep on Russian Information-War Capabilities* https://www.defenseone.com/ideas/2022/04/dont-sleep-russian-information-war-capabilities/364050/ [dostęp: 5.04.2022].

Blokada informacyjna – co to takiego

Agresja zbrojna przeciwko Ukrainie nie wywołała istotnych protestów w Rosji. Od 24 lutego dochodzi do nielicznych demonstracji antywojennych, mających w dużej mierze charakter spontaniczny, w tym do jednoosobowych pikiet. Każdorazowo są one rozbijane przez służby bezpieczeństwa. Liczba ich uczestników sięgnęła 24 lutego maksymalnie kilku tysięcy w Moskwie i Petersburgu. W kolejnych dniach, według dostępnych informacji, zbierają one przeciętnie od kilku do kilkuset osób.

Uczestnicy demonstracji są masowo zatrzymywani. Niezależny projekt medialny OVD-Info, zajmujący się monitorowaniem przypadków łamania praw człowieka, informuje, że w dniach 24–28 lutego zatrzymano ogółem prawie 7 tys. osób (najwięcej w związku z udziałem w akcjach 24 lutego – prawie 1980 osób w 67 miastach). 28 lutego, według wstępnych danych, zatrzymano 492 osoby w 14 miastach. Pojawiają się doniesienia o przepełnionych aresztach w Moskwie, wszczęto już setki spraw administracyjnych (demonstrantom grożą kary aresztu i grzywny) i pierwsze sprawy karne[18].

Inteligentna broń

Rosyjska agresja na Ukrainę i działania ukraińskich wojsk próbujących odeprzeć inwazję Władimira Putina pokazują, jak niebezpieczną bronią stały się w ostatnich latach bojowe drony. Ukraińska armia korzysta z nich przecież wyjątkowo skutecznie i już otrzymała kolejne wyposażenie tego typu. Mówiąc dokładniej, chodzi tu o drony typu Switchblade, które najprościej można opisać jako „inteligentne" bomby, które mogą przebywać w powietrzu przez określony czas przed uderzeniem w wybrany cel[19].

Kluczowe są dostawy inteligentnej broni przeciwpancernej (przeciwpancernych pocisków kierowanych) i przeciwlotniczej (zestawy MANPAD). Ta broń jest lekka i łatwa w transporcie, a zarazem błyskawicznie zwiększa możliwości obronne piechoty. To narzędzia wystarczające do zwalczania – w sprzyjających warunkach – najpotężniejszych czołgów i najnowocześniejszych samolotów i śmigłowców.

Najcenniejsze są dla Ukraińców PPK[20] trzeciej generacji – działające w systemie „wystrzel i zapomnij" – i to właśnie one są najważniejszym elementem dostaw broni przeciwpancernej. Ukraina otrzymuje głównie pociski FGM-148 Javelin oraz NLAW.

---

[18] M. Domańska, Reakcje społeczne w Rosji na inwazję na Ukrainę, Ośrodek Studiów Wschodnich, https://www.osw.waw.pl/pl/publikacje/analizy/2022-03-02/reakcje-spoleczne-w-rosji-na-inwazje-na-ukraine ANALIZY [dostęp: 13.05.2022].

[19] T. Mileszko, *USA wysyłają na Ukrainę nowoczesne drony kamikaze*, https://www.komputerswiat.pl/aktualnosci/militaria/usa-wysylaja-na-ukraine-nowoczesne-drony-kamikaze-wyjasniamy-co-potrafia-switchblade/kdmc448 [dostęp: 19.05.2022].

[20] Przeciwpancerne pociski kierowane.

Mianem MANPAD-ów (od ang. *Man-portable air-defence system*) określa się przeciwlotnicze pociski kierowane możliwe do przenoszenia i odpalenia przez jednego człowieka – niemal wszystkie współczesne odpalane są z ramienia. Dziś najcenniejsze są te z nich, które podobnie – jak w wypadku broni przeciwpancernej – nie wymagają długotrwałego specjalistycznego szkolenia.

Już w pierwszym tygodniu wojny Turcja dostarczyła w ekspresowym tempie pierwsze z kilkudziesięciu zamówionych przez Ukrainę kolejnych dronów Bayraktar TB-2. Te stricte bojowe maszyny są spore i zdolne do przenoszenia łącznie czterech bomb kierowanych.

Stany Zjednoczone przekazały natomiast Ukrainie 100 dronów Switchblade. To lekkie drony „kamikaze" wystrzeliwane z tuby niczym pocisk PPK i zdolne do lotu przez 30 minut.

Podczas wojny w Ukrainie po raz pierwszy na szerszą skalę zestawy MANPAD były stosowane również do obrony antyrakietowej. Zdolne są do zestrzeliwania przede wszystkim pocisków manewrujących Kalibr ze względu na podobną charakterystykę lotu jak w wypadku niektórych samolotów. Ukraińcy chwalili się zestrzeleniem w ten sposób już łącznie co najmniej kilkudziesięciu Kalibrów[21].

Pentagon twierdzi, że Rosjanom skończyła się już dobra, inteligentna amunicja. Teraz zmuszeni są wykorzystywać tak zwane „głupie bomby", czyli pociski, którymi nie można w żaden sposób sterować. Po ich zrzuceniu z samolotu lub wystrzeleniu nie da się już w żaden sposób kontrolować lotu. To oznacza, że broń jest mniej skuteczna, dokonuje bardziej przypadkowych zniszczeń, a na jej celność wpływają nawet warunki atmosferyczne[22].

Niestety w ramach współpracy między reżimami Iran dostarczył Rosji dużą ilość tzw. dronów kamikaze. Są one stosunkowo proste w budowie, ale niestety wysyłane w większych ilościach powodują duże straty zwłaszcza dla infrastruktury energetycznej Ukrainy.

Internet a pomoc ofiarom wojny

W Polsce wprowadzony został darmowy Internet od UPC w związku z wojną w Ukrainie. Miało to być kolejnym krokiem pomocowym skierowanym w stronę Ukraińców, którzy przebywają w Polsce. Co ciekawe, pomocą objęte są nie tylko osoby z Ukrainy, ale i niektórzy Polacy. UPC udostępni darmowy dostęp do Internetu światłowodowego oraz telewizję na okres pół roku. Skorzystać z usług

[21] W. Głowacki, *Jaką broń dokładnie otrzymuje Ukraina z Zachodu i jaką jeszcze mogłaby dostać?*, https://oko.press/jaka-bron-dokladnie-otrzymuje-ukraina-z-zachodu-i-jaka-jeszcze-moglaby-dostac/ [dostęp: 4.05.2022].

[22] E. Waszczuk, *Rosji skończyła się skuteczna broń! Już przegrali?*, https://www.planeta.pl/Wiadomosci/Swiat/ROSJI-SKONCZYLA-SIE-SKUTECZNA-BRON!-Maja-wadliwe-pociski-25-03-2022 [dostęp: 15.05.2022].

mogli obywatele Ukrainy, którzy przybyli do Polski po dniu 24 lutego, a także Polacy, którzy są właścicielami lokali, w których obecnie przebywają uciekający przed wojną. Co istotne, zgodnie z informacjami pochodzącymi od UPC, chodzi o tych, którzy w całości udostępniają mieszkanie lub dom[23].

Pod numerem +48 800 088 544 osoby pokrzywdzone wojną na Ukrainie mogą szukać bezpłatnej pomocy prawnej. Samorząd radców prawnych i inne zawody prawnicze uruchomili bezpłatną infolinię w kilku językach m.in. polskim, ukraińskim i angielskim[24].

Od wybuchu wojny w Internecie pojawiło się wiele stron, które zbierają informacje o osobach mogących udzielić schronienia uchodźcom i proszą o podanie ich danych oraz numeru telefonu. Kolejne grupy na Facebooku ochoczo podają linki do arkuszy Google, w których zbierane są informacje o możliwościach lokalowych, adresach i numerach telefonów – tych samych, z których korzysta się do weryfikacji konta w banku. Powstaje więc dokładna baza danych na temat osób niosących pomoc i samych uchodźców dostępna dosłownie dla każdego. Być może te informacje posłużą do organizacji pomocy dla rodzin ukraińskich, ale mogą też zostać sprzedane albo wykorzystane w inny sposób[25].

Oczywiście cały czas trwają zbiórki internetowe środków pieniężnych oraz rzeczowych dla uchodźców, a jako ciekawostkę warto przytoczyć zbiórki internetowe na zakup tureckich dronów dla armii ukraińskiej.

Nowe zagrożenia dla komputera i urządzeń mobilnych

W celu usystematyzowania przedstawionych możliwości i sposobów zapobiegania cyberzagrożeniom można podzielić cały problem na trzy poziomy.

— Poziom pierwszy obejmuje zagrożenia w skali całego państwa**.** Działania zapobiegawcze na tym poziomie powinny dotyczyć budowy i stałej modernizacji zabezpieczeń technicznych sieci informatycznych, implementacji i egzekwowania procedur bezpieczeństwa dostępu do sieci, zwalczania prób penetrowania systemów telekomunikacyjnych, międzynarodowej współpracy w zwalczaniu cyberprzestępczości, wspierania produkcji oprogramowania do celów zabezpieczeń, opracowywania procedur i planów na wypadek cyberzagrożenia.
— Kolejny szczebel dotyczy zagrożeń w skali organizacji i przedsiębiorstw. Podejmowane na tym poziomie działania powinny dotyczyć budowy i egzekwo-

[23] P. Mering, *UPC w związku z wojną w Ukrainie rozdaje darmowy Internet światłowodowy i telewizję na pół roku*, https://bezprawnik.pl/darmowy-internet-od-upc-w-zwiazku-z-wojna-w-ukrainie/ [dostęp: 19.06.2022].

[24] PAP, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8391991,uchodzcy-z-ukrainy-bezplatna-infolinia-z-pomoca-prawna.html (dostęp: 3.06.2022].

[25] J. Kralka, *Jak rozpoznać kremlowskiego trolla w polskim Internecie?*, https://bezprawnik.pl/jak-rozpoznac-kremlowskiego-trolla-w-polskim-internecie/ [dostęp: 4.06.2022].

wania systemów zabezpieczeń, przestrzegania dyscypliny dostępu do danych, regularnego używania oprogramowania antywirusowego, szkolenia pracowników w zakresie bezpieczeństwa korzystania z Internetu.

— Najniższy poziom dotyczy zagrożeń dla indywidualnych obywateli. Powinni oni stosować się do następujących zaleceń: regularnie używać oprogramowania antywirusowego, odwiedzać tylko zaufane strony i portale internetowe, krytycznie podchodzić do odbioru przychodzącej korespondencji, natychmiast sygnalizować policji wszelkie zjawiska związane z cyberprzemocą, przestrzegać zasad prowadzenia korespondencji przyjętych w sieci, brać udział w szkoleniach z zakresu bezpieczeństwa w Internecie, przeglądać publikacje dotyczące tego typu wiedzy.

Tak naprawdę kluczowym elementem w zarządzaniu bezpieczeństwem w cyberprzestrzeni pozostaje człowiek. Z jednej strony to zwykle jego bezrefleksyjne i nieodpowiedzialne zachowania sprowadzają zagrożenia na sieć komputerową w pracy lub w domu. Z drugiej zaś to przestępcze skłonności połączone niewątpliwie z wybitnymi umiejętnościami hakerów powodują stały „wyścig zbrojeń" w sieci. Warto odnotować analogię dotyczącą rozwoju broni konwencjonalnej – zawsze nowa broń motywowała do budowy kolejnej nowej, mocniejszej generacji. Tak więc nie możemy oczekiwać, że wyścig ten kiedyś zakończy się sukcesem, trzeba tylko stale dotrzymywać kroku nowej technologii.

Zarówno zasięg, jak i rozmaitość podejmowanych zagadnień oznaczają, że pełne opanowanie tematu jest niemożliwe. Ma na to wpływ wysoka dynamika działań, zarówno w wojnie klasycznej, jak i wojnie informacyjnej. W najbliższym czasie chciałbym w kolejnych publikacjach szerzej zaprezentować poszczególne elementy zagadnienia.

Bibliografia

Adamski A., *Prawo karne komputerowe*, C.H. Beck, Warszawa 2000.

Bochyńska N., *Wojna, trolle i fake newsy, czyli na co zwracać uwagę w mediach społecznościowych*, https://publicystyka.ngo.pl/zanim-podamy-dalej-post [dostęp: 10.05.2022].

Demus A., Paul Ch., *Don't Sleep on Russian Information-War Capabilities*, https://www.defenseone.com/ideas/2022/04/dont-sleep-russian-information-war-capabilities/364050/ [dostęp: 5.04.2022].

De Wijk R., *The Limits of Military Power*, [w:] *Terrorism and Counterterrorism. Understanding the New Security Enrolment*, red. R.D. Howard, R.L. Sawyer, Mc-Graw Hill, Guilford 2005.

Domańska M., *Reakcje społeczne w Rosji na inwazję na Ukrainę*, Ośrodek Studiów Wschodnich, https://www.osw.waw.pl/pl/publikacje/analizy/2022-03-02/reakcje-spoleczne-w-rosji-na-inwazje-na-ukraine ANALIZY [dostęp: 13.05.2022].

Głowacki W., *Jaką broń dokładnie otrzymuje Ukraina z Zachodu i jaką jeszcze mogłaby dostać?*, https://oko.press/jaka-bron-dokladnie-otrzymuje-ukraina-z-zachodu-i-jaka-jeszcze-moglaby-dostac/ [dostęp: 4.05.2022].

Kralka J., *Jak rozpoznać kremlowskiego trolla w polskim Internecie?*, https://bezprawnik.pl/jak-rozpoznac-kremlowskiego-trolla-w-polskim-internecie/ [dostęp: 10.07.2022].

Mering P., *UPC w związku z wojną w Ukrainie rozdaje darmowy Internet światłowodowy i telewizję na pół roku*, https://bezprawnik.pl/darmowy-internet-od-upc-w-zwiazku-z-wojna-w-ukrainie/ [dostęp: 19.06.2022].

Mileszko T., *USA wysyłają na Ukrainę nowoczesne drony kamikaze*, https://www.komputerswiat.pl/aktualnosci/militaria/usa-wysylaja-na-ukraine-nowoczesne-drony-kamikaze-wyjasniamy-co-potrafia-switchblade/kdmc448 [dostęp: 19.05.2022].

Molander R.C., Riddile A., Wilson P.A., *Strategic Information Warfare A New Face of War,* https://www.rand.org/pubs/monograph_reports/MR661.html.

Siewko T., *Stopień alarmowy CHARLIE-CRP znów przedłużony w całej Polsce*, TVN24 [dostęp: 6.04.2022].

Siwicki M., *Cyberprzestępczość*, C.H. Beck, Warszawa 2013.

Urbaniak P., *Rosyjskie trolle atakują nową taktyką. Nie daj się podejść*, https://www.telepolis.pl/wiadomosci/wydarzenia/rosyjskie-trolle-polska-dezinformacja-hejt [dostęp: 25.07.2022].

Waszczuk E., *Rosji skończyła się skuteczna broń! Już przegrali?*, https://www.planeta.pl/Wiadomosci/Swiat/ROSJI-SKONCZYLA-SIE-SKUTECZNA-BRON!-Maja-wadliwe-pociski-25-03-2022 [dostęp: 15.05.2022].

Komunikat Komisji do Parlamentu europejskiego, Rady oraz Komitetu Regionów – W kierunku ogólnej strategii zwalczania cyberprzestępczości, {SEK(2007) 641}{SEK(2007) 642}, http://eur-lex.europa.eu [dostęp: 30.05.2017].

Portal Geekweek, *Uważajcie na prorosyjskie trolle. Próbują nas skłócić z Ukraińcami*, https://geekweek.interia.pl/internet/news-uwazajcie-na-prorosyjskie-trolle-probuja-nas-sklocic-z-ukrai,nId,5907897 [dostęp: 23.06.2022].

Portal GOV.pl, *Uwaga na zagrożenia w cyberprzestrzeni*, https://www.gov.pl/web/sluzby-specjalne/uwaga-na-zagrozenia-w-cyberprzestrzeni [dostęp: 10.08.2022].

PAP, https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/8391991,uchodzcy-z-ukrainy-bezplatna-infolinia-z-pomoca-prawna.html [dostęp: 3.06.2022].

Raport Hostile Social Manipulation Present Realities and Emerging Trends, za: *Czy rosyjskiej dezinformacji należy się obawiać? CyberDefence*, https://cyberdefence24.pl/polityka-i-prawo/czy-rosyjskiej-dezinformacji-nalezy-sie-obwiac-okiem-amerykanskich-naukowcow-nie [dostęp: 17.05.2022].

Cybernetic warfare – tips from Ukraine

Summary

Russia's aggression against Ukraine also marked the outbreak of a cyberwar that is fought via the Internet practically all over the world. It has covered many aspects of modern life, from trolling to using cyber technology directly on the battlefield. Modern conventional weapons without the use of advanced digital technology become very useless, without information about the battlefield, it is dramatically inaccurate. This is clearly seen in the case of the Russians who, after using up their stocks of intelligent ammunition, bomb and shell Ukraine practically blindly, causing large losses among the civilian population. We are also dealing with numerous forms of cyberattacks against European Union countries. Russian hackers make numerous attempts to attack websites and portals, both governmental and social organizations.

Keywords: Internet, security, cyber warfare, threats, cyberbullying, cybercrime, smart weapons and ammunition.