Article No. 329
DOI: https://doi.org/10.26881/srg.2024.11.12
Artykuł badawczy / Research article
Dziedzina nauk społecznych / Social sciences
Dyscyplina naukowa: nauki o komunikacji społecznej i mediach / Discipline of science: communication and media studies

Citation:
Myślak, D.A., Plewik, K. (2024). Antyrosyjskie działania grupy Anonymous jako element kultury hakerskiej w kontekście agresji Rosji na Ukrainę. *Studia Rossica Gedanensia*, 11: 247–272.
DOI: https://doi.org/10.26881/srg.2024.11.12

ANTYROSYJSKIE DZIAŁANIA GRUPY ANONYMOUS JAKO ELEMENT KULTURY HAKERSKIEJ W KONTEKŚCIE AGRESJI ROSJI NA UKRAINĘ[2]

*DOMINIKA AGATA MYŚLAK
**KINGA PLEWIK

Uniwersytet Warmińsko-Mazurski w Olsztynie / / University of Warmia and Mazury in Olsztyn
Wydział Humanistyczny / Faculty of Humanities
Instytut Dziennikarstwa i Komunikacji Społecznej / Institute of Journalism and Social Communication
ul. Kurta Obitza 1, 10-725 Olsztyn, Polska / Kurta Obitza St. 1, 10-725 Olsztyn, Poland
*Corresponding Author e-mail: dominika.myslak@uwm.edu.pl
*ORCID: https://orcid.org/0000-0002-5421-6224
**Corresponding Author e-mail: lyoko3103@gmail.com
**ORCID: https://orcid.org/0009-0000-4469-3548
(nadesłano / received 19.07.2024; zaakceptowano / accepted 31.07.2024)

[2] W artykule odwołujemy się do badań i wniosków zawartych w pracy licencjackiej Kingi Plewik *Działalność grupy Anonymous w związku z agresją Rosji na Ukrainę w 2022 roku. Analiza serwisu „Komputer Świat"* obronionej 17.06.2024 roku na Uniwersytecie Warmińsko-Mazurskim w Olsztynie. Wkład procentowy autorów w powstanie publikacji przedstawia się następująco: D.A. Myślak – 50%, K. Plewik – 50%.

Abstract
Anti-Russian actions of the Anonymous group as an element of hacker culture in the context of Russia's aggression against Ukraine

The aim of the article is to look at the anti-war and anti-Putin actions of the Anonymous group as an element of hacker culture. These actions emerged after Russia's invasion of Ukraine on February 24, 2022. They quickly gained intensity, as if parallel to the escalation of the war barbarism, whose source was and still remains in the Kremlin. The authors try to show that the unfavorable image of cybercriminals, to which Anonymous is usually attributed, collapses when considering the fact that their online activity also had a positive ethical dimension. In the initial period of the Ukrainian-Russian armed conflict, members of this international community set out to conduct awareness-raising actions for Russian citizens about the real motives of Vladimir Putin's war in Ukraine and its horrifying consequences. The source material and analytical information were provided on the "Komputer Świat [Computer World]" specialized web portal.

Keywords: Anonymous, Russia, Ukraine, cyber-attacks, hackers, Władimir Putin, war, hactivism.

Abstrakt

Celem artykułu jest przybliżenie kultury hakerskiej i zobrazowanie antywojennych, a także antyputinowskich działań grupy Anonymous. Działania te pojawiły się po napaści Rosji na Ukrainę 24 lutego 2022 roku. Szybko przybrały na intensywności, równolegle do eskalacji wojennego barbarzyństwa, którego źródło było i wciąż pozostaje na Kremlu. Autorki starają się pokazać, że niekorzystny wizerunek cyberprzestępców, do jakich zalicza się zazwyczaj także grupę Anonymous, załamuje się, gdy bierze się pod uwagę fakt, iż ich aktywność w Sieci miała również pozytywny wymiar etyczny. W początkowym okresie ukraińsko-rosyjskiego konfliktu zbrojnego członkowie tej międzynarodowej społeczności postawili sobie za zadanie przeprowadzenie akcji uświadamiających obywateli Federacji Rosyjskiej o rzeczywistych pobudkach wywołania wojny przez Władimira Putina w Ukrainie i o jej przerażających skutkach. Materiał źródłowy i zarazem analityczny stanowiły informacje zamieszczone na specjalistycznym portalu „Komputer Świat".

Słowa kluczowe: Anonymous, Rosja, Ukraina, cyberataki, hakerstwo, haker, Władimir Putin, wojna, haktywizm.

Wprowadzenie

Współczesne hakerstwo jest zjawiskiem aktywnym w cyberprzestrzeni. Charakteryzuje je swoista kultura, w której ważne miejsce zajmują struktura, cele i zadania stawiane programowo lub doraźnie przez członków niejawnej społeczności między-

narodowej. Od początkowo niewinnego usuwania błędów w programach komputerowych wyraźnie ewoluowało ono, zwłaszcza w XXI wieku, ku wyspecjalizowanym rozwiązaniom informatycznym, z których hakerzy robią różnorodny użytek, a posiadane przez nich umiejętności nie zawsze służą realizacji szlachetnych celów. Z tego powodu mówi się dzisiaj o specyficznej etyce hakerskiej, usiłując wyjaśniać, a niekiedy usprawiedliwiać działania hakerów i łagodzić mimo wszystko negatywne nastawienie użytkowników Sieci do ich nielegalnych działań (Jordan 2011: 151).

Rozwój hakerstwa w czasie skutkował m.in. pojawieniem się terminologii, która stanowi dziś stały komponent jawnego języka zarówno samych hakerów, jak i badaczy zajmujących się nielegalnymi włamaniami cyberprzestępców do cudzych systemów informatycznych, a zwłaszcza rządowych, bankowych i sektora prywatnego. Ze względu na anonimowość tych działań i skrzętne ukrywanie swej tożsamości świat hakerstwa pozostaje rozproszony i niestabilny. Potwierdzają to spostrzeżenia badaczy, którzy ostrzegają internautów przed uzależnieniem od technologii sieciowych – ich zabezpieczanie postępuje wolniej niż ich rozwój (por. Chantizis, Stais 2022: 19).

Zasadniczym przedmiotem naszego badania stała się działalność grupy hakerskiej Anonymous[3]. Przyglądamy się jej internetowym akcjom związanym z przeciwdziałaniem agresji Rosji na Ukrainę. Celem artykułu jest zobrazowanie na podstawie tekstów zamieszczonych w portalu „Komputer Świat" antyrosyjskich działań tej grupy hakerskiej jako elementu kultury hakerskiej, które pojawiły się po napaści Rosji na Ukrainę. Serwis ten poddałyśmy analizie zawartości jakościowo-ilościowej w okresie od ataku Rosji na Ukrainę, tj. od 24 lutego do 10 maja 2022 roku, ponieważ wtedy właśnie doszło do większości ataków hakerskich Anonimowych wywołanych agresją Kremla na Ukrainę. Portal „Komputer Świat" profesjonalnie zajmuje się problematyką hakerstwa, w tym działaniami grupy Anonymous oraz akcjami organizowanymi przez kolektywy hakerskie. W serwisie znajduje się także wiele artykułów dotyczących wydarzeń w Ukrainie, dzięki czemu możliwe stało się sięgnięcie do materiałów archiwalnych i ich eksploracja pod określonym kątem.

Materiały źródłowe w serwisie „Komputer Świat" przeanalizowałyśmy z wykorzystaniem zakresowo szerszych i węższych słów lub wyrażeń kluczowych: Anonymous, agresja Rosji na Ukrainę, ataki Anonymous, hakerzy, ataki hakerskie, Rosja, propaganda rosyjska, Anonymous + agresja Rosji. Zebrany materiał z obranej cezury został podany analizie zawartości jakościowo-ilościowej. Przebadałyśmy zatem 41 artykułów oraz 2 filmy, stanowiące załączniki do artykułów zamieszczonych przez serwis. Zgromadzone teksty podzieliłyśmy według następującego klucza kategoryzacyjnego:

1. wiadomości hakerów do Władimira Putina – artykuły zawierające wiadomości od Anonymous bezpośrednio skierowane do prezydenta Rosji (w sumie 10 artykułów i 2 filmy);
2. ataki hakerskie na rząd rosyjski – publikacje opisujące działania haktywistów wymierzone w Kreml (14 artykułów);
3. ataki hakerskie na wybrane firmy w Rosji – materiały dotyczące akcji Anonymous wymierzone w konkretne firmy, które pozostały w Rosji (10 artykułów);

[3] W dalszej części tekstu zamiennie stosowana będzie także nazwa Anonimowi.

4. walka hakerów z dezinformacją i propagandą rosyjską – artykuły opisujące działania hakerów mające na celu pokazanie mieszkańcom Rosji prawdy o wydarzeniach wojennych (5 artykułów).

Z kultury hakerskiej

W XIX wieku Edward Taylor utożsamiał kulturę z cywilizacją: „Kultura, czyli cywilizacja jest to złożona całość, która obejmuje wiedzę, wierzenia, sztukę, moralność, prawa, obyczaje oraz inne zdolności i nawyki nabyte przez człowieka jako członka społeczeństwa" (Gajda 2003: 25). Z kolei Alfred Kroeber i Clyde Kluckhohn widzieli w kulturze złożoną obszarowość, tworzącą spójną jedność: historyczną, psychologiczną, genetyczną, opisową, normatywną oraz strukturalną (Kroeber, Kluckhohn 1952: 40). Dla Antoniny Kłoskowskiej kultura była względnie zintegrowaną całością, która obejmowała „zachowania ludzi przebiegające według wspólnych dla zbiorowości społecznej wzorów wykształconych i przyswajanych w toku interakcji oraz zawierające wytwory takich zachowań" (Kłoskowska 1980: 40). Marek Krajewski natomiast podkreślał, że definicja kultury jest płynna, zmienna ze względu na potrzeby i oczekiwania społeczeństw (Krajewski 2005: 7–9).

Kultura jest formacją nadrzędną wobec subkultury. Milton M. Gordon postrzega subkulturę jako obszar w obrębie kultury narodowej, który można wyodrębnić dzięki czynnikom o charakterze społecznym (np. grupa społeczna, etniczna, religia, zawód, miejsce zamieszkania) oraz sposobom, w jakich zestawy cech z poszczególnych kategorii łączą się ze sobą w grupach (Gordon 1947: 40). Subkultura to „wyodrębniony według jakiegoś kryterium (etnicznego, zawodowego, religijnego, demograficznego) segment życia społecznego i jego kultura" (Filipiak 1999: 13). Przykładem subkultury jest domena hakerska. Edwin Bendyk już w 2011 roku stawiał pytania, czym jest kultura hakerska, sugerując, że nie należy jej postrzegać jako jednej z barwnych, hałaśliwych i bez większego wpływu na rzeczywistość subkultur epoki ponowoczesności (Bendyk 2011: 10).

Słowo *hakerstwo* wywodzi się od angielskiego wyrazu *hack*, czyli 'włamywać się do komputera', w spolszczeniu: 'hakować go'. Stąd Tim Jordan twierdzi, że *hack* jest aktem hakerstwa (Jordan 2011: 17–32). Subkulturę hakerską zrodziła „rewolucja komputerowa", ściślej: pierwsi programiści. Początki „świadomych włamów do systemów informatycznych" łączy się zwykle z wynalazkiem Guglielmo Marconiego z 1903 roku, który miał umożliwiać bezpieczne i bezprzewodowe przesyłanie wiadomości na długie dystanse. Urządzenie skompromitował wówczas John Nevil Maskelyne (Murek 2015), a jego działania stały się inspiracją dla białych kapeluszy[4]. Historia hakerstwa odno-

[4] Wśród hakerów można wyróżnić „czarne kapelusze", czyli hakerów podejmujących nielegalne zarobkowe działania mające na celu zniszczenie danej firmy/instytucji czy też po prostu zrobienie komuś na złość. Skutki ich działań często są nieodwracalne. Najbardziej niebezpieczne są wycieki danych, które hakerzy mogą upublicznić. Drugą grupę stanowią „białe kapelusze", czyli hakerzy łamiący zabezpieczenia „sposobem czarnego kapelusza", lecz zamiast wykorzystać możliwość kradzieży danych, szantażu, niszczenia cyfrowego mienia, haker informuje o tym, w jaki sposób uzyskał dostęp do informacji, aby firma mogła usprawnić zabezpieczenia (tzw. testy penetracyjne). „Szare kapelu-

towała także nazwisko Josefa Carla Engressia, który nieświadomie stał się pierwszym na świecie phreakerem[5]. Listę osób „zasłużonych dla hakerstwa" tworzą takie znane nazwiska, jak William D. Mathews z Massachusetts Institute of Technology, który znalazł pierwszą lukę w oprogramowaniu Multics CTSS, czy Bob Thomas Creeper, twórca wirusa internetowego (Brzeziński 2022). Miano superzłoczyńcy przylgnęło do Kevina „Condor" Mitnicka, „który nałogowo włamywał się do systemów komputerowych i telekomunikacyjnych, siejąc w nich spustoszenie" (Bendyk 2011: 8).

W dziejach hakerstwa odnotowano pozytywny wątek rodzimy, albowiem w 1932 roku trzej Polacy – Marian Rejewski, Henryk Zygalski i Jerzy Różycki – złamali kod niemieckiej maszyny szyfrującej Enigma (Murek 2015). W czasach PRL-u za hakerstwo uznano budowę nadajnika, który umożliwiał zhakowanie publicznej telewizji przy użyciu komputera ZX Spectrum. Operacją tą zarządzali Zygmunt Turło oraz Eugeniusz Pazderski[6]. Słusznie zatem zauważa Bendyk, że „trudno o bardziej mistyfikowane pojęcie współczesnego języka" (Bendyk 2011: 8) niż haker.

Atak hakerski może być przeprowadzony z dowolnego miejsca na świecie, co oznacza, że w Sieci nie istnieją cybergranice. Ataki wirusowe są czynami nie tylko szkodliwymi, lecz także niebezpiecznymi dla człowieka. Negatywny przykład odnotowany w kulturze hakerskiej stanowi wyłączenie systemu komputerowego wieży kontroli lotów na lotnisku w Worcester w 1997 roku. Z kolei w 2011 roku od dziesiątek milionów użytkowników Playstation Network oraz Sony Online Entertainment cyberprzestępcy wykradli informacje osobowe, dane kart kredytowych i debetowych. Straty poszkodowanych oszacowano na około 1–2 mld dolarów (Jankowski 2022). Tego typu zachowania cyberprzestępców zmuszają ekspertów ds. bezpieczeństwa do tworzenia nowych cyberbroni i prowadzenia zaawansowanych kampanii nastawionych na walkę z cyberprzestępczością (Murek 2015).

W ujęciu stereotypowym haker jest kojarzony z kimś, kto podejmuje działania w Sieci szkodzące innym, polegające na przykład na kradzieży danych osobowych, pozyskaniu korzyści finansowych czy uprzykrzaniu komuś życia, a hakerstwo rozumiane jest jako bezprawne wtargnięcie do obcego komputera (Jordan 2011: 33–34). Zdaniem czołowego przedstawiciela i badacza kultury hakerów, Erica Stevena Raymonda, „hakerzy coś tworzą, a krakerzy to niszczą" (Raymond 2007). Uważa on, że hakerzy mają nie tylko swoją kulturę, ale też filozofię aktywną w niejednej dziedzinie nauki i sztuki. Utrzymuje, że hakerstwo wiąże się ze stylem życia, ze specyficznym sposobem myślenia o świecie i ludziach. Koncepcja Raymonda koresponduje w pewnym sensie z poglądem Manuela Castellsa, który kulturę hakerską łączy z kulturą technomerytokratyczną (Castells 2003: 54).

---

sze" zaś to hakerzy, którzy podejmują jednocześnie działania legalne i nielegalne, jednak w większości na rzecz dobra społeczeństwa. O tym: *Haker: Czarny…* (2022).

[5] Phreaker to osoba zajmująca się łamaniem zabezpieczeń telefonicznych w celu przeprowadzania tańszych lub darmowych rozmów.

[6] 14 września 1985 roku mieszkańcy Torunia na swoich odbiornikach telewizyjnych mogli ujrzeć przeźrocze, na którym widniał napis nawołujący do bojkotu wyborów, w tle zaś był nadawany Dziennik Telewizyjny. Zob. Górski 2022.

Jeśli istotą hakerstwa jest tworzenie nowych rzeczy, hakowanie musi pociągać za sobą określone zmiany:

> Hakować to tyle, co różnić się… Hakerzy umożliwiają przyjście na świat nowych rzeczy. Nie zawsze wielkich czy wspaniałych, czy nawet dobrych, ale – nowych. W sztuce, nauce, filozofii, kulturze, w jakimkolwiek tworzeniu wiedzy – wszędzie tam, gdzie można gromadzić dane, wydobywać z nich informacje, które stwarzają światu nowe możliwości, istnieją hakerzy hakujący nowe ze starego (McKenzie 2004: 3–4).

To z kolei przypomina pewne zjawiska obecne w medioznawstwie, jak hybrydyzacja i konwergencja. Castells twierdzi, że środowisko hakerów za najwyższą wartość uznaje wolność. Jest ona rozumiana jako: 1. swoboda w zakresie kreacji, 2. wolność w dostępie do wiedzy, 3. samodzielność w decydowaniu o dzieleniu się nową wiedzą (Wiedzo Znawca 2022).

Kulturę hakerską charakteryzują także wewnętrzne reguły postępowania, jak na przykład zasada współpracy przy usprawnianiu najnowszych technologii, co ma służyć wolnemu poszerzaniu ogólnoświatowej wiedzy informatycznej w myśl *copyleftu* (Bendyk 2011: 10). Z tego powodu kultura hakerska jest nazywana niekiedy kulturą darów. Dokonania hakerów, traktowane jako produkt podlegający prawom autorskiemu i rynkowym, oceniane są przez ich własne środowisko (Pietrowicz 2004: 210–211). Rezultaty działań hakerów nazywane są *labor of love.* Jak pisze Vickie Li, „Właśnie to kocham w hakowaniu aplikacji internetowych: chodzi o kreatywne myślenie, stawianie sobie wyzwań i robienie więcej, niż wydaje się to możliwe" (Li 2023: 17). Li uważa, że hakerzy przypominają superbohaterów, ale z tą różnicą, że można ich spotkać w świecie rzeczywistym. Pokonują oni ograniczenia informatyczne dzięki wyjątkowym umiejętnościom, intelektowi, kreatywności.

Hakerzy mają także własne konwencje i wydarzenia[7]. Do najsłynniejszych należy maraton hakerski (Hackathon), w którym uczestnicy wspólnie poszukują rozwiązań problemów nakreślonych przez organizatora (AI 2023, Cioch 2023). „Maratończycy" posługują się pseudonimami, a kontakt jest wyłącznie wirtualny. Ta właśnie cecha wyróżnia kulturę hakerów na tle innych odmian kultury merytokratycznej (Wiedzo Znawca 2022). Niektóre grupy hakerskie podczas spotkań we własnym gronie kładą nacisk na doskonalenie zasad programowania, zgłębianie tajników techniki komputerowej; inne, należące do ruchu makerów, zajmują się obróbką materiałów fizycznych (wycinarki, obrabiarki) oraz drukiem 3D (Zaród 2017: 233–235).

Hakerów cechuje specyficzna motywacja. „Haktywiści dążą do zmiany politycznej" (Jordan 2011: 118), cyberwojownicy dbają o interesy własnego państwa i angażują się w konflikty, cyberterroryści „szukają skutków politycznych przez stosowanie psychologicznie nośnej przemocy" (Jordan 2011: 118), a cyberprzestępcy działają dla własnego zysku. Nierzadko siłą napędową hakerów staje chęć wywołania szerokiego zamieszania w cyberprzestrzeni, zrobienia komuś ważnemu złośliwego żartu, uzyskania określonych korzyści czy zaszkodzenie atakowanej instytucji. W tym celu hakerzy

[7] Ich tworzenie zapoczątkowała grupa z Holandii. Mowa tu o eventach, jak np. Galactic Hacker Party (1989), Hacking at the End of the Universe (1993), Hacking In Progress (1997), Hackers At Large (2001) oraz What The Hack (2005). Zob. https://pl.frwiki.wiki/wiki/Hacker_(sous-culture) (dostęp 07.05.2022).

mogą działać bezpośrednio przez przełamanie zabezpieczeń i podszywanie się pod uprawnionego użytkownika lub pośrednio przez sięgnięcie po wirusy komputerowe. Tym, co łączy grupy hakerskie, są cyberataki. Można je przeprowadzić z wielu urządzeń, posługując się na przykład smartfonem, tabletem, laptopem, jednostką stacjonarną. Hakerzy telefonii komórkowej korzystają chętnie z *phishingu*, który polega na tworzeniu fałszywych, ale budzących zaufanie stron internetowych, a więc podszywaniu się pod rzeczywiste witryny, lub *bluehackingu*, umożliwiającym włamanie się do telefonu, gdy ten zaloguje się w niezabezpieczonej sieci Bluetooth.

Paradoksalnie hakerzy jako specjaliści wysokiej klasy bywają legalnie zatrudniani, najczęściej w instytucjach państwowych, do stworzenia zabezpieczeń chroniących dane i systemy sieciowe. W takich wypadkach „biały kapelusz", posługując się technikami „czarnego kapelusza", wykorzystuje kompetencje hakerskie przy łamaniu zabezpieczeń. Gdy komputerowy włamywacz uzyskuje dostęp do systemu i jego danych, informuje zleceniodawcę o lukach w zabezpieczeniu. Takie postępowanie nazywa się testowaniem penetracyjnym (zob. przyp. 4). Pisała o tym m.in. Li, która zwróciła uwagę na to, że jeszcze 10–20 lat temu zostałaby za tego rodzaju działania aresztowana, obecnie zaś takie jak ona osoby są zatrudniane przez najpotężniejsze światowe organizacje (Li 2023: 16).

Kultura hakerska jest pojęciem szerokim, dynamicznym. Najbardziej newralgicznym jej punktem nie jest jednak strona techniczna, lecz aspekt etyczny postępowania cyberprzestępców. Wydawać by się mogło, że ataki hakerskie zawsze powinny być oceniane jednoznacznie negatywnie, lecz wydarzenia, zorganizowane i przeprowadzone przez hakerów po wybuchu rosyjsko-ukraińskiego konfliktu zbrojnego w lutym 2022 roku, tę jednoznaczność raczej osłabiają. Aktywność grupy Anonymous na tym antywojennym i antyputinowskim polu jest dobrym tego przykładem.

Powstanie kolektywu Anonymous

Narodziny kolektywu hakerskiego Anonymous wiążą się bezpośrednio z powstaniem gier sieciowych i internetową akcją dla żartu (z ang. *for the lulz*), po której dostrzeżono wielki potencjał w tego typu aktach (Warzecha 2023). W latach 2004–2006 najpopularniejszym forum w Internecie był 4chan, stylizowany na współczesnego Reddita. Strona służyła przede wszystkim do komunikacji za pomocą obrazów. Na 4chan pojawiły się pomysły zakłócania działania innych stron internetowych na zasadzie trollingu. Wśród użytkowników tej strony znalazła się grupa aktywistów, która obrała sobie za cel zastraszenie innych społeczności internetowych (Svitlyk 2023). W tej właśnie społeczności powstał kolektyw hakerski pod nazwą Anonymous. Dokładna data powstania tej grupy nie jest możliwa do ustalenia, ale pierwsze skutki aktywności członków Anonymous dały się zauważyć w 2006 roku. Wtedy Anonimowi na swoich kontach w serwisie Habbo ustawili taki sam avatar – czarnoskórego mężczyznę z afro – po czym zablokowali dostęp do pływalni innym użytkownikom przez rozesłanie nieprawdziwej wiadomości, że została ona zainfekowana wirusem HIV. Anonymous zasłynęli także niechlubnie w Sieci, gdy wykradli kody źródłowe programów Norton Internet Security 2006 oraz Norton AntiVirus 2006, a sześć lat później udo-

stępnili je w mediach w odwecie za aresztowanie członków grupy hakerskiej LulzSec (Niemiec 2023).

Za założyciela Anonimowych uważa się Aubreya „Kirtanera" Cottle'a, hakera, badacza (...), inżyniera bezpieczeństwa komputerowego, inżyniera oprogramowania[8]. Oficjalnie grupa nie ma lidera i nie jest scentralizowana. Hakerzy komunikują się własnymi kanałami, nie wykonują czyichś poleceń. Struktura Anonymous przypomina nieco siatkę terrorystyczną. Anonimowi dołączają do akcji, które uznają za zgodne z ich kodeksem moralnym (Chwistek 2022f). Angażują się w konflikty polityczne, zbrojne, religijne i inne, nie będąc stroną. Ich broń stanowi Internet. Sprzeciwiają się przede wszystkim konsumpcjonizmowi, korupcji oraz wpływom Kościoła katolickiego na życie publiczne. Chcą, by użytkownicy Sieci uważali ich za „ludzi z klasy pracującej, szukających lepszej przyszłości dla ludzkości, którzy zgadzają się co do kilku podstawowych pryncypiów: wolnego dostępu do informacji, wolności wypowiedzi, brania przez firmy i rządy odpowiedzialności za ich działania, prawa do prywatności oraz anonimowości dla prywatnych obywateli" (Zaród 2017: 233–235). Anonymous podkreślają, że nie są organizacją, klubem ani też grupą, nie posiadają statutu, nie prowadzą dokumentacji, nie pobierają składek członkowskich (Szewczyk 2023). Kierują się mottem: „Obywatele nie powinni bać się swoich rządów. Rządy powinny bać się swoich obywateli" (Pracuj.pl, online). Ataki cybernetyczne mają spowodować destabilizację ich przeciwników poprzez – choćby chwilowe – odebranie im władzy nad społeczeństwem (Pracuj.pl, online). Działania Anonymous mają na celu nagłaśnianie problemów społecznych (Rudnicki 2022b). Choć nie mają przywódcy, potrafią skutecznie się jednoczyć (Niemiec 2023). Ostrzegają przed oszustami, działają dla idei, a ich kodeks moralny nie zakłada zysków finansowych. Niemniej włamania sieciowe dokonywane przez członków Anonymous, nawet przeprowadzane w słusznej sprawie, są – obiektywnie rzecz biorąc – aktami wandalizmu i mogą stanowić zagrożenie (Koch 2023).

Anonimowi walczą o wolność, sprzeciwiają się inwigilowaniu użytkowników Internetu, ukrywaniu niektórych przedsięwzięć rządu oraz agencji szpiegowskich. Opowiadają się przeciwko ograniczaniu wolności obywatelskich, w tym użytkowników Sieci; mówią: „nie" korupcji oraz ignorowaniu problemów społecznych i powiększaniu nierówności (Koch 2023). Zwalczają faszyzm, bronią wolności w Internecie. Za niedopuszczalne uznają szpiegowanie komputera – stwierdzają, że jest ono niezgodne z zasadą anonimowości i wolności użytkownika w Sieci (Niemiec 2023). Kolektyw Anonymous skupia wiele ugrupowań posiadających własną nazwę i symbolikę, zazwyczaj związaną z historią ich kraju bądź działalnością członków[9].

---

[8] W 2008 roku scjentolodzy sfotografowali Cottle'a, który po tym incydencie zaczął obawiać się o bezpieczeństwo swojej rodziny i postanowił zakończyć działalność Anonymous. Podjął próby nagłośnienia złej famy kolektywu, by zniechęcić do niego społeczność. Przeprowadził akcję, w której strona Fundacji Epilepsy została zapełniona migającymi animacjami, by osoby z epilepsją doznały ataków padaczkowych. Niedługo potem przeszedł na „hakerską emeryturę". W 2020 ponownie dołączył do grupy hakerów i był odpowiedzialny za obecność Anonymous na Twitterze. Zob. https://en.wikipedia.org/wiki/Aubrey_Cottle (dostęp 22.01.2023).

[9] Są to np. Legion of Doom (Legion Śmierci), Cult of the Dead Cow (Kult Zdechłej Krowy), Masters of Deception (Mistrzowie Oszustwa), Legion of Hackers (Legion Hakerów), Chaos Computer Club, TeaMp0ison LulzSec (działająca zaledwie 2 miesiące w 2011 r.) czy Syrian Electronic Army. Polski

Anonimowi zyskali znaczny rozgłos w trakcie protestów przeciw porozumieniu ACTA. To wtedy powstał *hacktivism*, kolektyw zaczęto kojarzyć z maską Guya Fawkesa[10]. W 2012 roku doszło do Marszu Miliona Masek, w którym każdy mógł wziąć udział zakładając maskę Fawkesa. Wkrótce też stała się ona znakiem rozpoznawczym Anonymous. Była wykorzystana w Arabskiej Wiośnie Ludów w latach 2010–2012 i podczas protestów w Hongkongu w latach 2019–2020. Anonimowi stali się swego rodzaju franczyzą dla wszystkich grup niezgadzających się na ograniczanie wolności obywatelskich (Rybakow, 2023).

Anonymous pozostają, jak dotąd, nieuchwytni. Haktywiści uderzają w CIA, FBI i policję (Matacz 2023). Anonimowi w cyberwalce atakują reżimy i państwa demokratyczne, sprzeciwiają się niesprawiedliwym decyzjom rządów, instytucji, firm (T.J., online). Jawnie głoszą, że ich cel stanowią agencje rządowe USA, Izraela, Tunezji, Ugandy i innych państw. Ważnym celem jest też Państwo Islamskie (ISIS). Grupa Anonymous zorganizowała wiele spektakularnych akcji, jak tzw. projekt Chanology, czyli serię zamachów komputerowych na Kościół Scjentologiczny (2008), „YouTube Porn Day" (2009), Operację Payback (2010), obronę WikiLeaks (2010), ataki na firmę HBGary (2011), Operację Sony (2011). Anonimowi mieli swój udział w przedsięwzięciu „Okupuj Wall Street" (2011), „największym w historii ataku na witryny rządowe" (Nowak, online) po zamknięciu Megaupload oraz Megavideo (2012). Zaznaczyli swą obecność w trakcie walki z ACTA w Polsce (2012) i „wojnie" z Donaldem Trumpem oraz Hillary Clinton (2016).

Anonimowi posługują się czterema hasłami: 1. „Jesteśmy Anonymous. Jesteśmy Legionem. Nie przebaczamy. Nie zapominamy. Spodziewajcie się nas"; 2. „Obywatele nie powinni bać się swoich rządów. Rządy powinny bać się swoich obywateli"; 3. „Anonymous to TY"; 4. „Witajcie, obywatele świata! Jesteśmy Anonymous". Te hasła brzmią niczym manifesty (Jabłońska 2023). Zawarty w sloganach przekaz jest czytelny, jasno sformułowany.

Agresja Rosji na Ukrainę spowodowała, że członkowie grupy Anonymous uderzyli zarówno w Kreml, organizacje rządowe i pozarządowe Rosji, wielkie firmy, jak i we Władimira Putina. Od początku rosyjskiej inwazji na Ukrainę haktywiści stawiali sobie za cel wywieranie presji na prezydencie Federacji Rosyjskiej i jego podwładnych, by wojska okupacyjne wycofały się z terenów Ukrainy. Tym samym obnażyli słabość rosyjskich zabezpieczeń (Rudnicki 2022a, online). Wysiłki Anonimowych nie przyniosły jednak spodziewanych rezultatów.

---

odłam Anonymous nosi nazwę Squad 303, który nawiązuje do Dywizjonu 303. O tym: https://forsal.pl/artykuly/588323,hakerzy-anonymous-wiecej-zapalu-niz-umiejetnosci.html (dostęp 22.01.2023) oraz Modzelewska 2023.

[10] Maska ta wywodzi się z filmu „V jak Vendetta", którego akcja rozgrywa się w totalitarnej Anglii, a jedyną osobą stawiającą opór systemowi jest – przebrany za Guya Fawkasa – V. Sam Fawkes był członkiem grupy spiskowców, która 5 listopada 1605 roku przeprowadziła nieudany zamach na budynek brytyjskiego parlamentu. Postać Fawkesa zyskała popularność dzięki komiksowi Alana Moore'a i Dawida Lloyda – „V jak Vendetta", ale większy rozgłos zapewniła ekranizacja w reżyserii Jamesa McTeigue'a. Bohater filmu zmagał się z brytyjskim totalitarnym, neofaszystowskim reżimem, używając metod klasycznego terroru. Zob. Koch 2023, Chwistek 2022f.

Analiza zawartości serwisu „Komputer Świat" w kontekście agresji Rosji na Ukrainę

W kategorii *Wiadomości hakerów do Władimira Putina* znalazło się dziesięć artykułów oraz dwa filmy jako załączniki do jednej publikacji. Były to materiały wideo, które zawierały komunikaty hakerów do prezydenta Rosji[11]. Z ich lektury wynika, że Anonymous są przeciwnikami zarówno Putina, jak i jego reżimu. Na oficjalnych kontach społecznościowych Anonymous zostały opublikowane filmy, w których hakerzy grożą szukaniem „brudów" na Putina. Ujawnienie znalezionych informacji przez Anonymous miałoby pokazać społeczeństwu rosyjskiemu, w jaki sposób ich przywódca zdobył władzę i co ukrywa przed narodem (Gołąbiowski 2022c). W odniesieniu do kwestii rosyjsko-ukraińskiej działania oznaczane są hashtagiem #OpRussia, co powinno ułatwić światową koordynację działań wymierzonych w rosyjskiego przywódcę i jego propagandę.

Prezydent Rosji nie odpowiedział na groźby hakerów. Jego konta społecznościowe nie zostały zhakowane ani sparaliżowane przez internetowych gigantów. Putin sam je usunął, a Facebook, Instagram oraz Twitter zablokował w całym kraju, co zbulwersowało Rosjan. Powstały wtedy alternatywne platformy społecznościowe, dedykowane wyłącznie społeczności rosyjskiej (B.a., 2022a), na których Putin prowadzi propagandę związaną z wojną w Ukrainie. Wyłączenie znanych stron społecznościowych nie było przypadkowe: w ten sposób Kreml walczy z internautami próbującymi zdemaskować rosyjską agitację antyukraińską.

Działania Putina miały jednak określone konsekwencje: Facebook, Instagram i Twitter nie zastosowały kar wobec swych użytkowników za propagowanie nienawiści skierowanej przeciwko przywódcy rosyjskiemu; wcześniej zamieszczanie tego typu treści groziło pozbawieniem możliwości komentowania i publikowania postów przez jakiś czas (z ang. *mute*) czy też tymczasowym zawieszeniem konta, a nawet jego usunięciem (tzw. ban). Dodatkowo Facebook zablokował profil rosyjskiego Ministerstwa Spraw Zagranicznych (Długosz 2022b). Także Google wprowadziło dla Rosjan ograniczenia w Sklepie Play. Rosyjskim użytkownikom uniemożliwiono nabywanie nowych programów i subskrypcji, realizowanie zakupów w aplikacji, a nawet pobieranie płatnych programów i gier po wcześniejszym dokonaniu zakupu. Dodatkowo zablokowano im możliwość aktualizacji płatnego oprogramowania. Ograniczenia nie obejmowały jednak darmowych aplikacji (Długosz 2022a).

Internetowa walka z propagandą kremlowską, a co za tym idzie, z polityką informacyjną w mediach rosyjskich, nie jest prowadzona wyłącznie przez hakerów, lecz również przez sieciowych gigantów. Do walki z rosyjską propagandą może przyłączyć się każdy użytkownik Internetu (Witoszka 2022b). W analizowanych publikacjach znajdują się także załączniki do oficjalnych kont Anonymous na YouTube, na których zostały opublikowane dwa filmy z groźbami skierowanymi do rosyjskiego przywódcy[12]. Słychać w nich jednak syntezator mowy, a nie prawdziwy głos człowieka. Z filmu

[11] Spis artykułów uwzględnionych w analizie znajduje się w aneksie.

[12] Zob. https://www.youtube.com/watch?v=cO4uRCkuJVg (dostęp 22.05.2024) oraz https://www.youtube.com/watch?v=UpYJ-Mw1trM (dostęp 22.05.2024).

wynika, że hakerzy planują przeprowadzenie akcji, której celem jest bezpośredni atak na prezydenta Rosji, zamierzają upublicznić informacje, które mają pogrążyć Putina zarówno w oczach obywateli jego państwa, jak i na arenie międzynarodowej (Gołąbiowski 2022c).

W pierwszym filmie (YouTube, 2022a) widać siedzącą postać w bluzie z kapturem i masce przypisanej organizacji Anonymous. W tle pojawiają się napisy symulujące kodowanie programu lub innej aplikacji. Później postać zostaje zastąpiona urywkami filmów nagranych przez osoby mieszkające w Ukrainie, które ukazują skutki agresji Rosji. Są to m.in. obrazy nalotów rosyjskich samolotów i helikopterów na ukraińskie miasta czy kadry z rosyjskimi czołgami sunącymi opuszczonymi ulicami ukraińskich miast. Anonymous dedykują film Putinowi, o czym informują w pierwszych sekundach materiału i podkreślają, że nie akceptują działań wojsk rosyjskich oraz poleceń wydanych przez szefa z Kremla. Zaznaczają, że Putin nie respektuje podstawowych praw człowieka, okazują podziw dla determinacji Ukraińców starających się odeprzeć ataki Rosjan. Nie potrafią zrozumieć celu wrogich ataków na ukraińską ludność cywilną. Negatywnie odnoszą się do agresji Federacji Rosyjskiej na Ukrainę, oskarżając o nią Putina. Ukazują prawdę o Rosjanach przebywających w więzieniach za protesty przeciwko wojnie w Ukrainie. Anonymous twierdzą ponadto, że nałożone na Federację Rosyjską sankcje uderzą nie w samego przywódcę państwa, lecz w obywateli, agresja zaś policji wymierzona w demonstrantów wywoła dalsze protesty, co z pewnością pogłębi ogólny chaos. Autorzy filmu przekonują, że inwazja na Ukrainę prócz zerwania międzynarodowych kontaktów rosyjskiego przywódcy ujawniła jego prawdziwe oblicze. Postępowanie Putina skutkowało m.in. zerwaniem z wieloletnią neutralnością przez kraje, które w związku z jego atakiem na Ukrainę dołączyły np. do NATO. Anonymous ostrzegają, że jeśli Putin będzie kontynuował swoje agresywne działania, zrobią wszystko, by stracił poparcie zarówno własnych obywateli, jak i państw prorosyjskich. Zapowiadają dokonanie wymierzonych w Putina cyberataków „z każdej strony świata". Deklarują gotowość do walki nie tylko z Putinem, lecz także z całym jego gabinetem władzy. Uprzedzają, że wyłączenie stron rządowych było zaledwie wstępem do cyberwojny. Obecny rząd Putina porównują z radą ministrów z okresu socjalistycznego. Twierdzą, że siła ich organizacji jest znacznie większa niż możliwości Putina (YouTube, 2022b).

Drugi film (YouTube, 2022b) rozpoczyna intro jak w informacyjnych programach telewizyjnych. Chwilę po nim na ekranie pojawia się postać w masce, która mówi, że Anonymous wciąż czekają na reakcję prezydenta Rosji na ich poprzedni film. Dodaje ona, że z powodu nasilającej się agresji Rosji wobec Ukrainy Anonimowi postanowili „zadedykować" prowadzoną przez siebie operację Putinowi. Przypominają o atakach z 2018 roku na instytucje rosyjskie. Zapytali także Putina, czy pamięta, kiedy stracił bazę danych związaną z Afganistanem, która należała do rosyjskiego Ministerstwa Obrony Cyberprzestrzeni. Omawiają zawartość przejętej przez nich bazy danych i informują, że są one już dostępne na Twitterze. Negatywnie oceniają zachowanie przywódcy Federacji Rosyjskiej wobec Finlandii i Szwecji, za które Anonymous „ukarało" Putina przejęciem i wyłączeniem rosyjskich stron rządowych. Hakerzy przedstawiają plan działania: najpierw zamierzają upublicznić zatajane przez lata informacje rangi państwowej, jak chociażby o zakrojonej na ogromną skalę korupcji. Anonymous

apelują do Putina, by przywrócił prawa ukraińskiej ludności i uczciwie przeprowadził referenda (YouTube, 2022b).

Ten film był nie tylko ostrzeżeniem dla prezydenta Rosji, lecz także wezwaniem skierowanym do Anonimowych z całego świata, by rozeznali się w kwestii majątku Putina. Anonymous podkreślili, że nie zapominają jego kłamstw, „jest już bowiem za późno, aby wszystko, co złe, zostało zapomniane" (YouTube, 2022a). Pod koniec filmu hakerzy kierują do prezydenta Federacji Rosyjskiej słowa: „Expect us…", co znaczy: „Oczekuj/spodziewaj się nas". Na ekranie pojawia się napis: „Putin. The world is watching you" (Putin. Świat cię obserwuje), a na dole – #OpRussia (YouTube 2022a). Materiały te są ostrzeżeniem dla Putina, Anonymous bowiem dysponują ogromną siłą oddziaływania. Wiele akcji zorganizowanych przez hakerów odbiło się przecież szerokim echem medialnym, a zamierzone cele – zostały osiągnięte (Chwistek 2021a).

Niedługo po opublikowaniu wspomnianych filmów Anonymous postanowili zhakować systemy elektroniczne zainstalowane na jachcie Putina. Włamując się do prywatnego układu, hakerzy zmienili oznaczenie jednostki, jak również dane lokalizacji, przez co wydawało się, że jacht rozbił się na Wyspie Węży. Organizacja hakerska potwierdziła, że była to celowa akcja wymierzona w prezydenta Rosji, a wypadek jachtu był mistyfikacją. Hakerzy zaakcentowali, że w ten sposób zagrozili kremlowskiemu przywódcy (Kotowski 2022j). Przedstawili także konsekwencje, które czekają Putina za ignorowanie posunięć hakerów nastawionych na ujawnianie informacji mogących podważyć autorytet głowy państwa, w tym ściśle tajne dane o majątku Putina; kwestia ta wciąż rodzi wiele teorii spiskowych (B.a. 2022b). Ujawnianie prawdy na temat przeszłości kremlowskiego dyktatora może doprowadzić do jego całkowitego upadku (Witoszka a, online).

Zhakowana została również aplikacja VKontakte – rosyjski odpowiednik Facebooka. Haktywiści posłużyli się tym komunikatorem, by rozesłać obywatelom Rosji rzetelne wiadomości na temat wojny w Ukrainie (m.in. o rzeczywistej liczbie ofiar obu stron konfliktu, uderzeniach w ukraińską ludność cywilną). Wiadomości te trafiły do kilkunastu milionów użytkowników. Ponadto haktywiści wezwali obywateli Federacji Rosyjskiej do protestowania przeciwko działaniom militarnym Putina. Administratorzy portalu szybko zareagowali na ten atak hakerski i w ciągu kilkunastu minut usunęli niepożądane wiadomości (Kotowski 2022a).

W cyberprzestrzeni nie brakuje oszustów. W Internecie wielokrotnie ogłaszano zbiórki pieniędzy na wsparcie działań hakerów. Anonymous ostro odcinają się od tego typu kłamliwych akcji i informują, że ich celem jest powstrzymanie prezydenta Rosji przed eskalacją wojny w Ukrainie, że nie zamierzają wzbogacać się na ludzkim cierpieniu. Anonymous chcą zmieniać świat na lepsze bez uzyskiwania korzyści majątkowych. Dlatego próby zbierania środków na ich działalność uznają za przykłady usiłowania wyłudzenia pieniędzy. Zachęcają jednocześnie do finansowego wspierania oficjalnych akcji na rzecz pomocy ludności ukraińskiej (Gołąbiowski 2022a).

Na podstawie analizy materiału można dojść i do takiego wniosku, że hakerzy starają się wpłynąć na szybsze zakończenie wojny rosyjsko-ukraińskiej. Nie uderzają w cywilów ani w żołnierzy, którzy wykonują rozkazy. Ich głównym celem jest przywódca Rosji, gdyż to na nim spoczywa odpowiedzialność za skutki konfliktu wojennego. Wierzą, że jeśli „pokonają" Putina, wojna zostanie zakończona. Informują lud-

ność cywilną, jak naprawdę wygląda sytuacja na rosyjsko-ukraińskim froncie. Walczą z dezinformacją.

W kategorii *Ataki hakerskie na rosyjski rząd* znalazło się czternaście artykułów. Z ich analizy wynika, że Anonymous ze swego konta na Twitterze oficjalnie wypowiedzieli cyberwojnę rządowi Federacji Rosyjskiej. Na początku haktywiści wyłączyli witryny związane z rosyjskim Ministerstwem Obrony, prezydentem Rosji oraz usługami internetowymi. Zhakowali strony: sovam.com, com2com.ru, ptt.ru, mil.ru, goverement.ru, kremlin.ru, rt.com. Mimo że deaktywowanie wymienionych witryn nie wpłynęło na działanie instytucji, uzmysłowiło internautom siłę Anonymous i umożliwiło ponadto dotarcie z prawdziwymi informacjami do obywateli Federacji Rosyjskiej na temat bieżącej sytuacji w Ukrainie (Kotowski 2022b).

Celem haktywistów był również «Роскомнадзор» – instytucja państwowa, która odpowiada za kontrolowanie i cenzurowanie mediów dostępnych na terenie Rosji. To właśnie na skutek jej działań nastąpiło zablokowanie Facebooka i innych internetowych gigantów. Ten organ odpowiada również za usuwanie materiałów medialnych, które zawierają m.in. takie słowa, jak „atak", „inwazja", „wojna". Grupa DDoSecrets (część kolektywu Anonymous) wykradła 800 GB danych z zasobów Federalnej Służby Nadzoru Komunikacji, Informatyki i Mediów, a następnie udostępniła je w Internecie. Pliki zawierały przede wszystkim informacje dotyczące Baszkorstostanu, republiki wchodzącej w skład Federacji Rosyjskiej. Na oficjalnej stronie grupy można było pobrać pliki, które zostały podzielone na dwie paczki. W pierwszej paczce znajdowały się dane dotyczące spraw kadrowych urzędu, a w drugiej – analizy prawne związane z decyzjami urzędowymi. Hakerzy ostrzegli także przed złośliwym oprogramowaniem, które może znajdować się w jednym z folderów do pobrania (Chwistek 2022b).

Następnie zaatakowano rosyjskie Ministerstwo Obrony i przejęto jego prywatne dane, które umieszczono na Twitterze Anonymous. Zablokowano witrynę internetową tego ministerstwa, co skutkowało kradzieżą danych z serwerów i udostępnieniem w Internecie m.in. numerów telefonów, maili oraz haseł rosyjskich oficjeli rządowych. Poza tym internauci postanowili zorganizować akcję, która polegała na wysyłaniu obywatelom Federacji Rosyjskiej spamu, złośliwego oprogramowania, jak również wpisywaniu mieszkańców Rosji na różnego typu listy, jak na przykład na listę osób wspierających finansowo Donalda Trumpa. Jednak w tym wypadku Twitter uznał wpis za niezgodny z zasadami serwisu i dostęp do tych danych został wstrzymany (Snoch 2022a).

Ofiarą Anonimowych stała się również rosyjska telewizja państwowa. Walcząc z rosyjską dezinformacją, po zhakowaniu telewizji przez kilkanaście godzin nadawano jedynie materiały stworzone przez ukraińskich reporterów. Przede wszystkim nagrania dotyczyły Kijowa i toczonych w nim walk. Rosjanom nie udało się powstrzymać hakerów i materiały filmowe ujrzały miliony odbiorców (Witoszka 2022a). Następnie hakerzy zablokowali stronę rosyjskiej agencji informacyjnej TASS, umieszczając na niej wiadomość skierowaną do obywateli Federacji Rosyjskiej, w której nawoływano do powstrzymania agresji na Ukrainę. W komunikacie została przedstawiona wizja przyszłości Rosji zamieniającej się w ciągu kilku najbliższych lat w Koreę Północną. Wpis szybko został zdjęty, a strona jeszcze przez dłuższy okres pozostawała zablokowana (Mileszko 2022). Zhakowana została także grupa mediowa, która skupiała po-

nad sto stacji radiowych nadających w eterze i Internecie (ok. 8 mln słuchaczy). Do Internetu trafiło 1,5 mln wiadomości (823 GB poufnych e-maili z załącznikami), będących własnością prywatnej grupy mediowej «Выбери Радио» (Sieja 2022a).

Haktywiści upublicznili ponadto bazę danych rosyjskiego Ministerstwa Rozwoju Gospodarki. Każdy internauta mógł przejrzeć wykradzione informacje w prosty sposób: wystarczyło pobrać darmową aplikację do zmiany VPN, zmienić lokalizację na Rosję i wszystkie dane stawały się ogólnodostępne (Kotowski 2022c). Anonimowi zdobyli również częstotliwości radiowe i kody Morse'a używane przez rosyjskie wojska i zamieścili w Sieci listy wywołań konkretnych oddziałów rosyjskich wojsk prowadzących operacje militarne na terenie Ukrainy. Dzięki tym informacjom Ukraińcy mogli rozpoznać poszczególne jednostki, komunikujące się ze sobą w danej chwili, a także odkryć ich lokalizacje. Wykradzione częstotliwości wojskowe pomogły Ukrainie w identyfikacji rodzajów wojsk, ich danych, nazw i modeli sprzętu, z jakiego korzystali Rosjanie, oraz narzędzia do szyfrowania połączeń. Jednak internauci wątpili niekiedy w autentyczność tych ujawnionych informacji (Kotowski 2022d).

Hakerzy włamali się także do systemu monitoringu Kremla, czego dowodem było nagranie zmontowane z urywków pochodzących z sal i telekonferencji z Moskwy, Krymu i kilku innych republik. Dotknięte atakiem zostały urządzenia w salach Kremla oraz system telekonferencji (Rudnicki 2022b). Hakerzy zamieścili również na swoim koncie na Twitterze skan dokumentu *O organizacji wydarzeń informacyjnych w Internecie*, który sporządziło rosyjskie Ministerstwo Obrony. Z treści dokumentu wynikało, że „zlecono przygotowanie propagandowych filmów, które w zafałszowany sposób ukazywałyby rzekomą brutalność ukraińskich żołnierzy wobec rosyjskich jeńców" (Frąckiewicz 2022). Prawdopodobnie dokument ten stanowił podstawę podjęcia działań mających na celu podniesienie morale rosyjskiej armii i pokazania, że rozpoczęcie „specoperacji" wobec Ukrainy było słusznym posunięciem. Na dokumencie widnieje podpis wiceministra obrony Federacji Rosyjskiej, generała Dmitrija Bułhakowa (Frąckiewicz 2022).

Zaatakowana została również rosyjska agencja ALET współpracująca z firmami energetycznymi, obsługująca zgłoszenia eksportowe i celne dotyczące materiałów energetycznych. Hakerzy oficjalnie poinformowali o zhakowaniu 1,1 mld e-maili (1,1 TB danych). Organizacja hakerska nie podała dotąd informacji o tej akcji, ale wykradzione treści ukazały się w Sieci (Snoch 2022b).

Anonymous włamali się ponadto do Rosyjskiej Agencji Kosmicznej, przejmując dokumenty o rosyjskiej misji na Księżyc o nazwie Łuna-27. Dzięki temu cały świat mógł przeczytać szczegółowy opis techniki komunikacji, która miała zostać wykorzystana w trakcie wysyłania w 2025 roku rosyjskiego łazika na satelitę Ziemi. Z opublikowanych plików można było dowiedzieć się, że początkowo misję Łuna-27 zaplanowano na 2014 rok we współpracy z Indiami, lecz katastrofa projektu Fobos-Grunt spowodowała odłożenie projektu w czasie, co skutecznie zniechęciło Indie do kooperacji z Rosją i ostatecznie Indie samodzielnie wysłały sondę (Chwistek 2021c).

Hakerzy upublicznili 200 tys. e-maili (446 GB) związanych z Ministerstwem Kultury w Rosji, urzędami państwowymi w Błagowieszczeńsku oraz gubernatorem regionu Twer. Podawali jednak w wątpliwość prawdziwość tych informacji i zalecali podchodzić do nich z ostrożnością (Chwistek 2021d).

Z kolei 9 maja 2022 roku, kiedy w Rosji obchodzono rocznicę zwycięstwa nad faszyzmem, Dzień Zwycięstwa, polska grupa haktywistów zaatakowała telewizję rosyjską. Hakerzy przeprowadzili akcję pod nazwą „Dzień Wstydu", która polegała na włamaniu się do rosyjskich środków masowego przekazu i walce z dezinformacją na temat wydarzeń w Ukrainie. Haktywiści wdarli się do rosyjskiego systemu EPG i obecne tam teksty zastąpili słowami: „Na waszych rękach krew ukraińskich matek i dzieci" (Rudnicki 2022c). Oprócz tego zhakowaniu uległy wybrane strony i platformy, w tym rosyjski YouTube. Anonymous umieścili również notki, że rosyjski rząd i telewizja kłamią. Nazwy wszystkich rosyjskich kanałów telewizyjnych zostały zmienione na „Blood is on your hands", czyli „Krew jest na waszych rękach" (Rudnicki 2022c).

Z analizy dziesięciu tekstów należących do kategorii *Ataki hakerskie na wybrane firmy w Rosji* wynika, że hakerzy zaatakowali firmy, które nie wycofały się z Rosji. Ich pierwszą ofiarą padło Nestle, któremu Anonymous wykradło 10 GB danych z ponad 50 tys. wpisów dotyczących klientów biznesowych współpracujących z tą firmą. W upublicznionych plikach można było znaleźć loginy, hasła oraz dane biznesowe. Materiały zostały dodane na specjalnie przygotowaną witrynę internetową (Kotowski 2022e).

Następnie haktywiści uderzyli w inne firmy: Leroy Merlin, Auchan, Decathlon. Usunęli rosyjskie strony internetowe marek należących do korporacji Association Familiale Mulliez, które przez kilka godzin były niedostępne, co spowodowało spore straty finansowe (Sieja 2022c). Hakerzy włamali się także do komputerów Banku Centralnego Federacji Rosyjskiej i ujawnili ponad 35 tys. dokumentów (28 GB) z korespondencją, międzynarodowymi porozumieniami handlowymi i transferami pieniężnymi czy raportami na temat gospodarki Rosji. Elwira Nabiullina, prezes Banku Centralnego, nie odniosła się do sprawy, złożyła jednak rezygnację ze stanowiska, której Putin nie przyjął (Chwistek e, online).

Hakerzy usunęli – wraz z kopią zapasową – ponad 65 TB danych Rosyjskiej Federalnej Agencji Transportu Lotniczego, które zawierały ważne dokumenty, jak rejestracja i certyfikacja samolotów czy poczta elektroniczna. Poza tym zablokowali tę stronę internetową na kilkanaście godzin. Rosyjska Federalna Agencja Transportu Lotniczego w oficjalnym komunikacie podała, że wynikłe problemy były związane z czasowym brakiem dostępu do Internetu i awarią systemów elektronicznych. Duplikaty utraconych dokumentów nie zostały znalezione (Ładan, online).

Anonymous dostali się także do zasobów sieciowych Rosyjskiego Kościoła Prawosławnego, a ściślej: do jego pionu charytatywnego. Przejęli 15 GB danych (57,5 tys. e-maili), które udostępnili dziennikarzom i badaczom, ponieważ uznali, że dane są zbyt wrażliwe, aby były ogólnodostępne w Internecie. Zhakowane zostały także Lipieckie Zakłady Mechaniczne odpowiadające za produkcję sprzętu wojskowego (Snoch 2022c). Po ataku na Rosyjski Kościół Prawosławny hakerzy opublikowali listę przedsiębiorstw z branży technologicznej, które pozostały na terenach Rosji. Marki te ostrzeżono, że ich dalsze funkcjonowanie na terenie Rosji będzie wiązało się z atakami hakerskimi na ich firmę. Na liście znaleźli się światowi liderzy technologiczni: Acer, Alibaba, Asus, BlaBlaCar, Cloudflare, Huawei, Lenovo, MSI, Tencent, Xiaomi. Większość z tych podmiotów to spółki europejskie. Wątpliwości wzbudzały jedynie spółki chińskie, ponieważ Chiny zaopatrują rosyjski przemysł obronny, a także handel

z nimi pozwala Rosji „przetrwać" międzynarodowe sankcje (Box 2022). Wymienione w tweecie przedsiębiorstwa w większości wycofały się z Rosji. Te, które nie zdecydowały się na taki krok, zostały zaatakowane przez hakerów (Kotowski 2022f).

Kolejnym celem Anonimowych stał się «Газпром» zajmujący się projektowaniem zakładów przetwórstwa gazu i obróbki materiałów petrochemicznych oraz rozwojem rafinerii naftowych. Anonymous zamieścili w sieci 728 GB danych, w których można było znaleźć ponad 768 tys. wiadomości przekazywanych między pracownikami Gazpromu (Kotowski 2022g). Włamali się do systemów informatycznych głównego operatora metra w Moskwie – «Метроспецтехника» i uzyskali dostęp do systemów sterowania oddymiania, klimatyzacji, baterii, a także planów budynków oraz raportów z każdego pociągu (Snoch 2022d, online). Hakerzy uderzyli ponadto w rosyjską firmę «Энерпред», która zajmuje się rynkiem urządzeń hydraulicznych, znajdujących zastosowanie w przemyśle energetycznym, petrochemicznym, węglowym, gazowym, budowlanym. Anonimowi opublikowali w Sieci aż 432 GB danych – 645 tys. e-maili oraz dokumenty (Snoch 2022e).

Również firma energetyczna «Электроцентромонтаж», specjalizująca się w tworzeniu, testowaniu, budowie i utrzymaniu urządzeń oraz obiektów do wytwarzania i przesyłania energii, przyciągnęła uwagę hakerów. Usługi tego giganta przemysłowego świadczone są w ponad dwudziestu pięciu regionach Rosji, a wśród klientów znajdują się elektrownie jądrowe w Kursku i Smoleńsku oraz rosyjskie linie kolejowe. «Электроцентромонтаж» współpracuje także ze światowymi potęgami, jak Siemens czy Schneider Electric. Po ataku hakerskim na tę spółkę wypłynęło ponad 1,2 mln e-maili (1,7 TB danych). Anonymous nie podali dokładnie, co znajduje się w tych dokumentach, jednak zachęcili dziennikarzy i badaczy do pobrania paczki plików, a następnie do dokładnego przejrzenia oraz przeanalizowania korespondencji, co może sugerować, że w udostępnionych materiałach było wiele interesujących treści dotyczących firmy energetycznej (Kotowski 2022h).

Hakerzy przeprowadzali ataki przede wszystkim na firmy, które nie wycofały się z Rosji. Uznali bowiem, że jest to z ich strony jednoznaczne ze wspieraniem rosyjskiej gospodarki, co przekładało się na działania militarne Rosji – w tym przypadku na działania wojenne na terytorium Ukrainy.

Do kategorii *Walka hakerów z dezinformacją i propagandą rosyjską* weszło pięć artykułów. Anonymous stworzyli narzędzie, które pozwalało na wysyłanie SMS-ów do losowo wybranego obywatela Federacji Rosyjskiej. W wiadomości znajdowała się informacja o kłamstwach Kremla, cenzurze obecnej w mediach rosyjskich, śmierci żołnierzy rosyjskich i ukraińskich na froncie oraz wezwanie do obalenia dyktatury Putina. Hakerzy podkreślali, że dołączenie do akcji jest dobrowolne, a dobrym sposobem na wzięcie w niej udziału stanie się zakup nowej karty SIM (Witoszka 2022b). Podobną akcję przeprowadzono z pocztą e-mail oraz na WhatsApp. Jej celem było wezwanie Rosjan do zaprotestowania przeciwko Putinowi i wojnie w Ukrainie (Kotowski 2022i). Rozsyłane wiadomości zostały przygotowane przez hakerów wcześniej, a informacje w nich zawarte miały pomóc w walce z kremlowską dezinformacją (Witoszka 2022c).

Hakerzy włamali się do rosyjskich drukarek podłączonych do Internetu, wysyłając im plik PDF z poleceniem ciągłego drukowania. W ten sposób powstało ponad 100 tys. kopii antyrządowych ulotek z informacjami, że Kreml oszukuje swoich oby-

wateli, a w Ukrainie trwa inwazja rosyjskich wojsk. Dodatkowo Rosjanie mogli przeczytać instrukcję, w której krok po kroku opisywano, jak ominąć nałożoną przez Putina cenzurę na Sieć. Na końcu ulotki umieszczono wezwanie do walki z rządami Putina (Sieja 2022b). Zhakowano poza tym bota używanego w Rosji w aplikacji Discord. Hakerzy przeprogramowali jego funkcje, przez co bot ukazywał gotowe wiadomości na temat konfliktu zbrojnego w Ukrainie. Przez ponad dwadzieścia cztery godziny, co pięć minut, „водка" wysyłał do wszystkich użytkowników serwerów informacje dotyczące przebiegu działań militarnych na froncie rosyjsko-ukraińskim. Za pośrednictwem bota przekazano ponad 70 mln wiadomości (Gołąbiowski 2022b).

Analiza artykułów dowodzi, że propaganda rosyjska jest wszechobecna. Tylko niewielka liczba obywateli Rosji jest świadoma, co w rzeczywistości dzieje się w Ukrainie. Hakerzy podjęli próbę uświadomienia Rosjan w kwestii panującej w ich państwie propagandzie i dezinformacji, wykorzystując do tego nie tylko zhakowane rosyjskie media publiczne, lecz także social media, komunikatory internetowe, maile i SMS-y.

Anonymous vs. propaganda rosyjska – podsumowanie

Wszystkie wyodrębnione w badaniu kategorie miały wspólny mianownik: antyrosyjskie działania i akcje ogólnoświatowe kolektywu hakerskiego Anonymous. Najwięcej artykułów w analizowanym okresie ukazało się w marcu 2022 roku – szesnaście, w kwietniu – jedenaście, a w lutym – dziesięć. To wskazuje, że najbardziej aktywnym czasem działań Anonymous był początek wojny rosyjsko-ukraińskiej. Dominowały publikacje dotyczące ataków hakerskich na Putina i jego rząd – głównych winowajców rozpętania pod koniec lutego 2022 „specjoperacji", która od samego początku miała cechy konfliktu zbrojnego.

Na podstawie analizy materiałów źródłowych zarysował się obraz silnego kolektywu hakerskiego, który sprzeciwił się militarnym posunięciom Rosji. Anonymous dowiedli, że Federacja Rosyjska nie może czuć się w pełni bezpieczna w cyberprzestrzeni i jest narażona na hakowanie wrażliwych baz danych. Od rozpoczęcia inwazji Rosji na Ukrainę Anonimowi wykradli i upublicznił ponad 12 mln rosyjskich plików i e-maili. Ich celem stało się wywieranie presji na podwładnych Putina, by jak najszybciej wycofano wojska z terenów Ukrainy (Rudnicki 2022a). Haktywiści przyczynili się do walki z rosyjską propagandą i dezinformacją. Podważyli na pewno w jakimś stopniu autorytet rosyjskiego władcy i jego rządu (Chwistek 2021a).

W 2014 roku Rosja rozpoczęła wojnę hybrydową z Ukrainą, która zakończyła się aneksją Krymu. Osiem lat później wybuchła wojna, która trwa do dzisiaj. Prowadzona w Rosji propaganda medialna powoduje, że większość jej obywateli nie ma świadomości, iż w rozpoczętej pod koniec lutego 2022 roku wojnie rosyjsko-ukraińskiej to Federacja Rosyjska jest agresorem, a nie Ukraina. Walka z tą propagandą i dezinformacją jest możliwa przede wszystkim za pomocą Sieci. Podjęli się jej hakerzy z całego świata, starając się ukazać obywatelom Rosji prawdę i dodatkowo atakując największe firmy, instytucje rządowe, a nawet samego Władimira Putina. Wymierzone w Rosję akcje hakerskie, którym przyświecał główny cel: powstrzymać inwazję na Ukrainę – były przeprowadzane regularnie. Wziąć w nich udział mógł każdy użytkownik Sieci, co

dowodzi, że Internet jest współczesną areną walk, a pojęcia takie jak cyberwojna, cyberterroryzm, cyberataki czy cyberprzestępczość znajdują zastosowanie na co dzień. „A jeśli przyszłe konflikty i wojny mają rozgrywać się na cyfrowej granicy, to w takim razie ich żołnierzami i partyzantami siłą rzeczy będą hakerzy" (Bendyk 2011: 10), co można było zaobserwować na przykładzie działalności Anonymous w kontekście agresji Rosji na Ukrainę.

Aneks

Tabela 1. Materiał analityczny z serwisu „Komputer Świat”

Kategoria	Autor	Data	Tytuł
Wiadomości hakerów do Putina	Łukasz Gołąbiowski	27.02.2022	Anonymous publikują wiadomość do Putina. „Szykujemy operację specjalnie dla Ciebie”
	B.a.	6.03.2022	Rosja tworzy własną internetową rzeczywistość
	Dominika Długosz	6.05.2022	Google wprowadza bolesne ograniczenia dla Rosjan
	Łukasz Gołąbiowski	27.02.2022	Anonymous o wojnie w cyberprzestrzeni z Rosją i Putinem. „Nie robimy tego dla pieniędzy”
	Bartosz Witoszka	27.02.2022	Anonymous zhakowali rosyjską telewizję państwową. Puszczono materiały z Ukrainy
	Adrian Kotowski	25.02.2022	Anonymous wypowiedzieli cyberwojnę rosyjskiemu rządowi. Nie działa wiele stron
	Adrian Kotowski	28.02.2022	Anonymous zhakowali jacht Putina. Wyznaczyli mu kurs do „piekła”
	Dominika Długosz	11.03.2022	Facebook nie będzie blokował gróźb śmierci wobec rosyjskich żołnierzy i Putina
	Bartosz Witoszka	13.03.2022	Anonymous przypominają, jak można dotrzeć z prawdą do Rosjan. „Anonymous to każdy z was”
	Michał Chwistek	18.03.2022	10 najgłośniejszych operacji Anonymous przeciwko Rosji Putina
	Adrian Kotowski	21.03.2022	Hakerzy zhakowali VKontakte i rozesłali do Rosjan informacje o wojnie w Ukrainie
Ataki hakerskie na rosyjski rząd	Adrian Kotowski	25.02.2022	Anonymous wypowiedzieli cyberwojnę rosyjskiemu rządowi. Nie działa wiele stron.
	Joachim Snoch	26.02.2022	Anonymous hakują rosyjskie Ministerstwo Obrony. Ogromny wyciek danych
	Bartosz Witoszka	27.02.2022	Anonymous zhakowali rosyjską telewizję państwową. Puszczono materiały z Ukrainy
	Tomasz Mileszko	28.02.2022	Hakerzy z Anonymous zablokowali rosyjską agencję informacyjną TASS
	Adrian Kotowski	02.03.2022	Anonymous zhakowali stronę rosyjskiego Ministerstwa Rozwoju Gospodarki. Baza danych trafiła do sieci.
	Michał Chwistek	11.03.2022	Anonymous wykradli i udostępnili 800 GB danych rosyjskiego urzędu cenzury Roskomnadzor
	Adrian Kotowski	17.03.2022	Anonymous twierdzą, że zdobyli częstotliwości radiowe i kody Morse'a używane przez rosyjskie wojska
	Maciej Frąckiewicz	29.03.2022	Anonymous chwalą się przechwyceniem rozkazu rosyjskiego generała

	Rafał Rudnicki	07.04.2022	Hakerzy Anonymous włamali się do wewnętrznego systemu monitoringu Kremla. „Teraz jesteśmy wewnątrz murów”
	Michał Chwistek	12.04.2022	Anonymous opublikowali kolejne rosyjskie maile. 200 tys. pochodzi z rosyjskiego Ministerstwa Kultury
	Michał Chwistek	25.04.2022	Anonymous opublikowali dokumenty dotyczące rosyjskiej misji na Księżyc
	Joachim Snoch	26.04.2022	Anonymous zhakowali rosyjską agencję celną ALET
	Rafał Rudnicki	09.05.2022	Polska grupa hakerów powiązanych z Anonymous bierze udział w akcji „Dzień wstydu”
	Rafał Rudnicki	02.06.2022	Anonymous atakują kolejny raz. Celem hakerów sieć, której klientami jest 8 mln Rosjan
Ataki hakerskie na wybrane firmy w Rosji	Adrian Kotowski	22.03.2022	Anonymous dotrzymali słowa. Twierdzą, że zhakowali Nestle za pozostanie w Rosji.
	Bartłomiej Sieja	24.03.2022	Anonymous zaatakowali strony Leroy Merlin, Auchan i innych marek, które nie wycofały się z Rosji
	Michał Chwistek	26.03.2022	Anonymous udostępnili 35 tys. dokumentów banku centralnego Rosji. Umowy, transakcje i raporty o stanie gospodarki
	Anna Ładan	31.03.2022	Ofensywa Anonymous: tym razem wymazali 65 TB danych Rosawiacji
	Joachim Snoch	03.04.2022	Anonymous zhakowali Rosyjski Kościół Prawosławny. Wyciekło 15 GB danych
	Adrian Kotowski	05.04.2022	Anonymous ujawnili listę celów. Będą atakować firmy, które nie wycofały się z Rosii.
	Adrian Kotowski	13.04.2022	Anonymous opublikowali 768 tys. maili spółki Gazpromu
	Joachim Snoch	20.04.2022	Hakerzy włamali się do systemów informatycznych rosyjskiego metra
	Joachim Snoch	25.04.2022	Rosyjska firma Enerpred kolejną ofiarą Anonymous
	Adrian Kotowski	29.04.2022	Anonymous zhakowali rosyjską firmę energetyczną. Do sieci wyciekło 1,2 mln maili
	Box	21.08.2022	Tak chińskie firmy pomagają Rosji obchodzić sankcje
Walka hakerów z dezinformacją i propagandą rosyjską	Bartosz Witoszka	07.03.2022	Anonymous opracowali nowe narzędzie. SMS do losowego Rosjanina sposobem na walkę z propagandą
	Adrian Kotowski	12.03.2022	Hakerzy stworzyli narzędzie do walki z propagandą. Pozwala wysłać wiadomość e-mail lub WhatsApp do losowego Rosjanina
	Bartosz Witoszka	13.03.2022	Anonymous przypominają jak można dotrzeć z prawdą do Rosjan. „Anonymous to każdy z was”
	Bartłomiej Sieja	22.03.2022	Anonymous włamali się do drukarek w Rosji. Powielają antyrządowe ulotki i instrukcje obejścia cenzury w sieci
	Łukasz Gołąbiowski	18.04.2022	Wódka na celowniku Anonymous. Rosyjski bot odsyłał do narzędzia polskich hakerów

Źródło: zestawienie własne.

Bibliografia / References

Bendyk, E. (2011). *Hakerstwo, pochwała wolności*. W: Jordan, T. *Hakerstwo*. Warszawa: Wydawnictwo Naukowe PWN: 7–15.

Castells, M. (2003). *Galaktyka Internetu. Refleksje nad Internetem, biznesem i społeczeństwem*. Poznań: Dom Wydawniczy Rebis.

Chantizis, F., Stais, I. (2022). *Hakowanie internetu rzeczy w praktyce. Przewodnik po skutecznych metodach atakowania IoT*. Gliwice: Wydawnictwo Helion.

Filipiak, M. (1999). *Od subkultury do kultury alternatywnej*. Lublin: Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej.

Gajda, J. (2009). *Antropologia kulturowa: Wprowadzenie do wiedzy o kulturze*. Kraków: Oficyna Wydawnicza Impuls.

Gordon, M. M. (1947). The Concept of the Sub-Culture and Its Application. *Social Forces*, 26: 40–42.

Jordan, T. (2011). *Hakerstwo*. Warszawa: Wydawnictwo Naukowe PWN.

Krajewski, M. (2005). *Kultury kultury popularnej*. Poznań: Wydawnictwo Naukowe Uniwersytetu im. Adama Mickiewicza.

Kroeber, A., Kluckhohn, C. (1952). *Culture: A Critical Review of Concepts and Definitions*. Cambridge: Havard University.

Li, V. (2023). *Bug Bounty Bootcamp. Przewodnik po tropieniu i zgłaszaniu luk w zabezpieczeniach*. Przeł. L. Lachowski. Gliwice: Wydawnictwo Helion.

Mitnick, K. (2019). *Duch w sieci. Moje przygody jako najbardziej poszukiwanego hakera wszech czasów.* Gliwice: Wydawnictwo Helion.

Pietrowicz, K. (2004). *Etyka hakerska Wyzwanie dla konsumeryzmu?*. W: Szlendak, T., Pietrowicz, K. (Red.). *„Na pokaz. O konsumeryzmie w kapitale bez kapitału"*. Toruń: Wydawnictwo Uniwersytetu Mikołaja Kopernika: 201–212.

Wark, McKenzie. (2004). *A Hacker Manifesto*. Cambridge: Harvad University Press.

Zaród, M. (2017). Hakerzy i kolektywy hakerskie w Polsce. Od operacjonalizacji do laboratoriów i stref wymiany. *Studia Socjologiczne*, 1: 225–252.

Źródła internetowe / Internet sources

AI, (2023). *Czym jest uczenie maszynowe?*. (Online) https://www.sap.com/poland/products/artificial-intelligence/what-is-machine-learning.html (dostęp 28.11.2023).

B. a. (2011). *Najgłośniejsze ataki cd.* (Online) https://www.benchmark.pl/testy_i_recenzje/anonymous-geneza-i-glosne-ataki-anonimowych/strona/15117.html (dostęp 24.02.2024).

B. a. (2012). *Hakerzy Anonymous: więcej zapału niż umiejętności.* (Online) https://forsal.pl/artykuly/588323,hakerzy-anonymous-wiecej-zapalu-niz-umiejetnosci.html (dostęp 22.01.2023).

B. a. (2016). *Anonymous wypowiadają „wojnę totalną" Trumpowi*. (Online) https://tvn24.pl/biznes/ze-swiata/wybory-w-usa-anonymous-wypowiada-wojne-totalna-trumpowi-ra627554-4468301 (dostęp 24.02.2024).

B. a. (2022a). *Rosja tworzy własną internetową rzeczywistość*. (Online) https://www.komputerswiat.pl/artykuly/rosja-tworzy-wlasna-internetowa-rzeczywistosc/dh2g0gl (dostęp 11.11.2022).

B. a. (2022b). *Największy sekret Kremla: ile wart jest majątek Putina.* (Online) https://www.forbes.pl/biznes/ile-wart-jest-majatek-putina-jakie-straty-poniesie-prezydent-rosji-wskutek-sankcji/c93ng12 (dostęp 20.04.2024).

B. a. (2022c). *Haker jako potencjalne zagrożenie dla twoich danych*. (Online) http://www.iniejawna.pl/pomoce/haker.html (dostęp 29.05.2022).

Bolanowski, J. (2012). *Protest przeciw ACTA, atak hakerów Anonymous, czyli powstanie styczniowe w internecie*. (Online) https://forsal.pl/artykuly/586784,protest-przeciw-acta-atak-hakerow-anonymous-czyli-powstanie-styczniowe-w-internecie.html (dostęp 24.02.2024).

Box. (2022). *Tak chińskie firmy pomagają Rosji obchodzić sankcje*. (Online) https://businessinsider.com.pl/gospodarka/tak-chinskie-firmy-pomagaja-rosji-obchodzic-sankcje/zh07424 (dostęp 30.11.2023).

Brzeziński, W. (2022). *Zanim hakerzy atakowali Rosję, czyli długa historia… hakowania!*. (Online) https://geekweek.interia.pl/raporty/raport-grunt-to-komunikacja/artykuly/news-zanim-hakerzy-atakowali-rosje-czyli-dluga-historia-hakowania,nId,5952881 (dostęp 29.05.2022).

Chwistek, M. (2022a). *10 najgłośniejszych operacji Anonymous przeciwko Rosji Putina*. (Online) https://www.komputerswiat.pl/wideo/wydarzenia/10-najglosniejszych-operacji-anonymous-przeciwko-rosji-putina/g6q31k9 (dostęp 12.11.2022).

Chwistek, M. (2022b). *Anonymous wykradli i udostępnili 800 GB danych rosyjskiego urzędu cenzury Roskomnadzor*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-wykradli-i-udostepnili-800-gb-danych-rosyjskiego-urzedu-cenzury/cyn7953 (dostęp 11.11.2022).

Chwistek, M. (2022c). *Anonymous opublikowali dokumenty dotyczące rosyjskiej misji na Księżyc*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/anonymous-opublikowali-dokumenty-dotyczace-rosyjskiej-misji-na-ksiezyc/fksvwx2 (dostęp 11.11.2022).

Chwistek, M. (2022d). *Anonymous opublikowali kolejne rosyjskie maile. 200 tys. Pochodzi z rosyjskiego Ministerstwa Kultury*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-opublikowali-kolejne-rosyjskie-maile-200-tys-pochodzi-z-rosyjskiego/lllq56g (dostęp 11.11.2022).

Chwistek, M. (2022e). *Anonymous udostępnili 35 tys. Dokumentów banku centralnego Rosji. Umowy, transakcje i raporty o stanie gospodarki*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/anonymous-udostepnili-35-tys-dokumentow-banku-centralnego-rosji-umowy-transakcje-i/v2wf705 (dostęp 12.11.2022).

Chwistek, M. (2022f). *Anonymous – historia i teraźniejszość. Dziś atakują Rosję, ale zaczynali znacznie bardziej „skromnie"*. (Online) https://www.komputerswiat.pl/artykuly/redakcyjne/anonymous-historia-i-terazniejszosc-dzis-atakuja-rosje-ale-zaczynali-znacznie/j5h12el (dostęp 22.01.2023).

Cioch, Ł. (2023). *Hackathony: na czym polegają i kto może na nich skorzystać?*. (Online) https://www.lcmedia.pl/hackathony-na-czym-polegaja-i-kto-moze-na-nich-skorzystac (dostęp 28.11.2023).

Długosz, D. (2022a). *Google wprowadza bolesne ograniczenia dla Rosjan. Chodzi o aplikacje na Androida*. (Online) https://www.komputerswiat.pl/aktualnosci/aplikacje/google-wprowadza-bolesne-ograniczenia-dla-rosjan-chodzi-o-aplikacje-na-androida/c2g2zzm (dostęp 11.11.2022).

Długosz, D. (2022b). *Facebook nie będzie blokował gróźb śmierci wobec rosyjskich żołnierzy i Putina*. (Online) https://www.komputerswiat.pl/aktualnosci/internet/facebook-nie-bedzie-blokowal-grozb-smierci-wobec-rosyjskich-zolnierzy-i-putina/qwjbw5w?utm_source=www.komputerswiat.pl_viasg_komputerswiat&utm_medium=referal&utm_campaign=leo_automatic&src-c=ucs&utm_v=2 (dostęp 11.11.2022).

Frąckiewicz, M. (2022). *Anonymous chwalą się przechwyceniem rozkazu rosyjskiego generała*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/anonymous-chwala-sie-przechwyceniem-rozkazu-rosyjskiego-generala/mt2kteq (dostęp 11.11.2022).

Frymorgen, B. (2016). *„Anonymous" grozi Trumpowi: Ujawnimy twoje powiązania z rosyjską mafią*. (Online) https://www.rmf24.pl/raporty/raport-wybory-prezydenckie-w-usa-2016/fakt/news-anonymous-grozi-trumpowi-ujawnimy-twoje-powiazania-z-rosyjsk,nId,2338506#crp_state=1 (dostęp 24.02.2024).

Gazetaprawna.pl (2022). *Haker: Czarny, Szary, a może Biały. Co to jest „white hacking" i czy jest legalny?*. (Online) https://prawo.gazetaprawna.pl/artykuly/1447091,white-hacking-odpowiedzialnosc-karna.html (dostęp 29.05.2022).

Gibbs, S. (2016). *Anonymous collective declares 'total war' on Donald Trump, again*. (Online) https://www.theguardian.com/technology/2016/mar/15/anonymous-declares-total-war-on-donald-trump-again (dostęp 24.02.2024).

Gołąbiowski, Ł. (2022a). *Anonymous o wojnie w cyberprzestrzeni z Rosją i Putinem. „Nie robimy tego dla pieniędzy"*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-o-wojnie-w-cyberprzestrzeni-z-rosja-i-putinem-nie-robimy-tego-dla-pieniedzy/542tn8r (dostęp 11.11.2022).

Gołąbiowski, Ł. (2022b). *Wódka na celowniku Anonymous. Rosyjski bot odsyłał do narzędzia polskich hakerów*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/wodka-na-celowniku-anonymous-rosyjski-bot-odsylal-do-narzedzia-polskich-hakerow/vx86485 (dostęp 12.11.2022).

Gołąbiowski, Ł. (2022c). *Anonymous publikują wiadomość do Putina. „Szykujemy operację specjalnie dla ciebie"*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/anonymous-publikuja-wiadomosc-do-putina-szykujemy-operacje-specjalnie-dla-ciebie/qng6m3q (dostęp 11.11.2022).

Górski, M. (2022). *Usłyszał o nich cały świat. Mija 35 lat od hakerskiego ataku „Solidarności"*. (Online) https://bydgoszcz.tvp.pl/49861584/hakerski-atak-solidarnosc (dostęp 29.05.2022).

Hosenball, M. (2016). *Hacker who exposed Hillary Clinton's email server expected to plead guilty.* (Online) https://www.reuters.com/article/idUSKCN0YF2KW/ (dostęp 24.02.2024).

HUT. (2024). (Online) https://cdaction.pl/newsy/anonymous-kontra-sony-czyli-wojna-hakerow-z-korporacja (dostęp 24.02.2024).

Jabłońska, K. (2023). *Kim są Anonymous i czym się zajmują?*. (Online) https://www.radiokrakow.pl/aktualnosci/kim-sa-anonymous-i-czym-sie-zajmuja (dostęp 24.01.2023).

Jankowski, P. (2022). *Największe ataki hakerskie na serwisy: Steam, PlayStation Network, Xbox Live*. (Online) https://www.benchmark.pl/aktualnosci/ataki-hakerskie-na-steam-playstation-network-xbox-live.html (dostęp: 29.05.2022).

Kłoskowska, A. (1980). *Kultura masowa*. Warszawa: Państwowe Wydawnictwo Naukowe.

Koch, M. (2023). *Idee są kuloodporne. Historia Anonymous.* (Online) https://isportal.pl/idee-sa-kuloodporne-historia-anonymous/ (dostęp 22.01.2023).

Kotowski, A. (2022a). *Hakerzy zhakowali VKontakte i rozesłali do Rosjan informacje o wojnie w Ukrainie*. (Online) https://www.komputerswiat.pl/aktualnosci/internet/hakerzy-zhakowali-vkontakte-i-rozeslali-do-rosjan-informacje-o-wojnie-w-ukrainie/4nclcy2 (dostęp 11.11.2022).

Kotowski, A. (2022b). *Anonymous wypowiedzieli cyberwojnę rosyjskiemu rządowi. Nie działa wiele stron*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/anonymous-wypowiedzieli-cyberwojne-rosyjskiemu-rzadowi-nie-dziala-wiele-stron/phwns5v (dostęp 11.11.2022).

Kotowski, A. (2022c). *Anonymous zhakowali stronę rosyjskiego Ministerstwa Rozwoju Gospodarki. Baza danych trafiła do sieci*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zhakowali-strone-rosyjskiego-ministerstwa-rozwoju-gospodarki-baza-danych/0h14j6g (dostęp 11.11.2022).

Kotowski, A. (2022d). *Anonymous twierdzą, że zdobyli częstotliwości radiowe i kody Morse'a używane przez rosyjskie wojska*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-twierdza-ze-zdobyli-czestotliwosci-radiowe-i-kody-morsea-uzywane-przez/y6j3wmd (dostęp 11.11.2022).

Kotowski, A. (2022e). *Anonymous dotrzymali słowa. Twierdzą, że zhakowali Nestle za pozostanie w Rosji*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-dotrzymali-slowa-twierdza-ze-zhakowali-nestle-za-pozostanie-w-rosji/ehvybxy (dostęp 12.11.2022).

Kotowski, A. (2022f). *Anonymous ujawnili listę celów. Będą atakować firmy, które nie wycofały się z Rosji*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-odnosza-sie-do-masakry-w-buczy-i-firm-ktore-nadal-wspolpracuja-z-rosja/ty42hsh (dostęp 12.11.2022).

Kotowski, A. (2022g). *Anonymous opublikowali 768 tys. maili spółki Gazpromu*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/anonymous-opublikowali-768-tys-maili-spolki-gazpromu/ccv9lge (dostęp 12.11.2022).

Kotowski, A. (2022h). *Anonymous zhakowali rosyjską firmę energetyczną. Do sieci wyciekło 1,2 mln maili*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zhakowali-rosyjska-firme-energetyczna-do-sieci-wycieklo-12-mln-maili/rblqnmk (dostęp 12.11.2022).

Kotowski, A. (2022i). *Hakerzy stworzyli narzędzie do walki z propagandą. Pozwala wysłać wiadomość e-mail lub WhatsApp do losowego Rosjanina*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/hakerzy-stworzyli-narzedzie-do-walki-z-propaganda-pozwala-wyslac-wiadomosc-e-mail-lub/f637sq9 (dostęp 12.11.2022).

Kotowski, A. (2022j). *Anonymous zhakowali jacht Putina. Wyznaczyli mu kurs do „piekła"*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zhakowali-jacht-putina-wyznaczyli-mu-kurs-do-piekla/eg8zc6r (dostęp 11.11.2022).

Kozłowski, A. (2023). *„Dzisiaj świat hakerom przyklaskuje". Rozmowa z dr Karoliną Małagocką o grupie Anonymous*. (Online) https://polskieradio24.pl/5/1222/Artykul/2916555,dzisiaj-swiat-hakerom-przyklaskuje-rozmowa-z-dr-karolina-malagocka-o-grupie-anonymous (dostęp 24.01.2023).

Ładan, A. (2022). *Ofensywa Anonymous: tym razem wymazali 65 TB danych Rosawiacji*. (Online) https://www.computerworld.pl/news/Ofensywa-Anonymous-tym-razem-wymazali-65-TB-danych-Rosawiacji,437364.html?utm_source=news&utm_campaign=polecane&utm_medium=tags (dostęp 12.11.2022).

Matacz, M. (2023). *Nad Anonymous nikt nie ma kontroli*. (Online) https://forsal.pl/lifestyle/technologie/artykuly/8375912,nad-anonymous-nikt-nie-ma-kontroli.html (dostęp 24.01.2023).

Mileszko, T. (2022). *Hakerzy z Anonymous zablokowali rosyjską agencję informacyjną TASS*. (Online) https://www.komputerswiat.pl/aktualnosci/internet/hakerzy-z-anonymous-zablokowali-rosyjska-agencje-informacyjna-tass/yj04clf (dostęp 11.11.2022).

Modzelewska, K. (2023). *Anonymous z polskim pierwiastkiem. Haker zdradza, jak Squad 303 stał się częścią legendarnego kolektywu*. (Online) https://www.dobreprogramy.pl/anonymous-moze-byc-kazdy-z-nas-haker-zdradza-jak-stac-sie-czescia-legendarnego-kolektywu,6809808245303936a (dostęp 22.01.2023).

Murek, M. (2015). *Historia hakerów – od robaka w komputerze do zaawansowanych cyberbroni.* (Online) https://geekweek.interia.pl/news-historia-hakerow-od-robaka-w-komputerze-do-zaawansowanych-cy,nId,1837681 (dostęp 28.04.2022).

Niemiec, W. (2023). *Co wiadomo o grupie Anonymous?.* (Online) https://gospy.pl/blog/205_co-wiadomo-o-grupie-anonymous.html (dostęp 22:01.2023).

Nowak, A. (2023). *Megaupload znika z sieci. Anonymous atakują w odwecie*. (Online) https://di.com.pl/megaupload-znika-z-sieci-anonymous-atakuja-w-odwecie-wideo-42994 (dostęp 24.01.2023).

PAP/AK. (2011). *Anonymous grożą atakiem na nowojorską giełdę.* (Online) https://www.forbes.pl/wiadomosci/hakerzy-z-anonymous-chca-zaatakowac-wall-street/5frs5v4 (dostęp 24.02.2024).

Pracuj.pl. (2023). *Hakerzy Anonymous – co robią i dlaczego nie znajdziesz takich ofert pracy?*. (Online) https://porady.pracuj.pl/zycie-zawodowe/hakerzy-anonymous-co-robia-i-dlaczego-nie-znajdziesz-takich-ofert-pracy/ (dostęp 22.01.2023).

Raymond, E. (2017). *Jak zostać Hackerem?*. Przeł. M. Pętlicki. (Online) https://docer.pl/doc/n5c05n5 (dostęp 28.04.2023).

Rudnicki, R. (2022a). *Anonymous podsumowują swoje działania podczas wojny. „Pokazali słabość rosyjskich zabezpieczeń"*. (Online) https://www.komputerswiat.pl/aktualnosci/internet/anonymous--podsumowuja-swoje-dzialania-podczas-wojny-pokazali-slabosc-rosyjskich/ew9h0r1 (dostęp 24.01.2023).

Rudnicki, R. (2022b). *Ataki hakerskie Anonymous. Oto 10 najsłynniejszych akcji „haktywistów"*. (Online) https://www.komputerswiat.pl/artykuly/redakcyjne/ataki-hakerskie-anonymous-oto-10-najslynniejszych-akcji-haktywistow/w0zp9t7#slajd-1 (dostęp 22.01.2023).

Rudnicki, R. (2022c). *Hakerzy Anonymous włamali się do wewnętrznego systemu monitoringu Kremla. „Teraz jesteśmy wewnątrz murów"*. (Online) https://www.komputerswiat.pl/aktualnosci/wydarzenia/hakerzy-anonymous-wlamali-sie-do-wewnetrznego-systemu-monitoringu-kremla-teraz/4mhl5w8 (dostęp 11.11.2022).

Rudnicki, R. (2022d). *Polska grupa hakerów powiązanych z Anonymous bierze udział w akcji „Dzień wstydu". Zhakowano m.in. rosyjską telewizję*. (Online) https://www.komputerswiat.pl/aktualnosci/internet/polska-grupa-hakerow-powiazanych-z-anonymous-bierze-udzial-w-akcji-dzien-wstydu/m06kex3 (dostęp 11.11.2022).

Rybakow, D. (2023). *Pierwsza cyberwojna światowa. Anonymous przeciwko Rosji*. (Online) https://www.lrt.lt/pl/wiadomosci/1261/1735171/pierwsza-cyberwojna-swiatowa-anonymous-przeciwko-rosji (dostęp 22.01.2023).

Sieja, B. (2022a). *Anonymous atakują kolejny raz. Celem hakerów sieć, której klientami jest 8 mln Rosjan*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-atakuja-kolejny-raz-celem-hakerow-siec-ktorej-klientami-jest-8-mln-rosjan/m8mdtbm (dostęp 11.11.2022).

Sieja, B. (2022b). *Anonymous włamali się do drukarek w Rosji. Powielają antyrządowe ulotki i instrukcje obejścia cenzury w sieci*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-wlamali-sie-do-drukarek-w-rosji-powielaja-antyrzadowe-ulotki-i-instrukcje/0kq0591 (dostęp 12.11.2022).

Sieja, B. (2022c). *Anonymous zaatakowali strony Leroy Merlin, Auchan i innych marek, które nie wycofały się z Rosji*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zaatakowali-strony-leroy-merlin-auchan-i-innych-marek-ktore-nie-wycofaly/7glc2md (dostęp 12.11.2022).

Snoch, J. (2022a). *Anonymous hakują rosyjskie ministerstwo obrony. Ogromny wyciek danych*. (Online) https://www.komputerswiat.pl/aktualnosci/internet/anonymous-hakuja-rosyjskie-ministerstwo-obrony-ogromny-wyciek-danych/thcesd3 (dostęp 11.11.2022).

Snoch, J. (2022b). *Anonymous zhakowali rosyjską agencję celną ALET*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zhakowali-rosyjska-agencje-celna-alet/5h6p687 (dostęp 11.11.2022).

Snoch, J. (2022c). *Anonymous zhakowali Rosyjski Kościół Prawosławny. Wyciekło 15 GB danych*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zhakowali-rosyjski-kosciol-prawoslawny-wycieklo-15-gb-danych/ll7v2hk (dostęp 12.11.2022).

Snoch, J. (2022d). *Hakerzy włamali się do systemów informatycznych rosyjskiego metra*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/hakerzy-wlamali-sie-do-systemow-informatycznych-rosyjskiego-metra/3mvg4ye (dostęp 12.11.2022).

Snoch, J. (2022e). *Rosyjska firma Enerpred kolejną ofiarą Anonymous*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/rosyjska-firma-enerpred-kolejna-ofiara-anonymous/6w9qzpt (dostęp 12.11.2022).

Svitlyk, Y. (2023). *Kim jest Anonymous? Historia hakerów, którzy zmieniają świat*. (Online) https://root-nation.com/pl/articles-pl/pl-kim-jest-anonymous-historia-hakerow/ (dostęp 22.01.2023).

Szewczyk, A. (2023). *Anonymous: Wojownicy w słusznej sprawie*. (Online) https://www.vogue.pl/a/anonymous-haktywisci-walcza-z-rosja (dostęp 24.01.2023).

T.J. (2023). Anonymous. *Kim są i jakie spektakularne akcje przeprowadzili*. (Online) https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/8406223,anonymous-kim-sa-i-jakie-spektakularne-akcje-przeprowadzili.html (dostęp 22.01.2023).

Warzecha, S. (2023). *Anonymous. Od internetowych trolli do wirtualnej potęgi*. (Online) https://weszlo.com/anonymous-sylwetka-historia (dostęp 22.01.2023).

Wiedzo Znawca. (2022). *Kultura hakerska*. (Online) https://e-tg.pl/wzmianki/kultura-hakerska/ (dostęp 07.05.2022).

Witoszka, B. (2022a). *Anonymous opracowali nowe narzędzie. SMS do losowego Rosjanina sposobem na walkę z propagandą*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-opracowali-nowe-narzedzie-sms-do-losowego-rosjanina-sposobem-na-walke-z/drdemjs (dostęp: 12.11.2022).

Witoszka, B. (2022b). *Anonymous przypominają, jak można dotrzeć z prawdą do Rosjan. „Anonymous to każdy z was"*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-przypominaja-jak-mozna-dotrzec-z-prawda-do-rosjan-anonymous-to-kazdy-z-was/2wy2xbk (dostęp 12.11.2022).

Witoszka, B. (2022c). *Anonymous zhakowali rosyjską telewizję państwową. Puszczono materiały z Ukrainy*. (Online) https://www.komputerswiat.pl/aktualnosci/bezpieczenstwo/anonymous-zhakowali-rosyjska-telewizje-panstwowa-puszczono-materialy-z-ukrainy/hb83852 (dostęp 11.11.2022).

YouTube (2022a). (Online) https://www.youtube.com/watch?v=cO4uRCkuJVg (dostęp 22.05.2024).

YouTube (2022b). (Online) https://www.youtube.com/watch?v=UpYJ-Mw1trM (dostęp 22.05.2024).

Competing interests: The authors declare that they have no conflict of interests.