DOI: 10.31648/sp.8252

Marcin Kowalczyk
Uniwersytet Warmińsko-Mazurski w Olsztynie
ORCID: 0000-0003-2900-1464
marcin.kowalczyk@uwm.edu.pl

Haktywizm w świetle regulacji prawnych – cyfrowi anarchiści czy bojownicy o wolność?

Wstęp

Celem rozważań ujętych w artykule jest próba oceny działalności nieformalnych grup sprzeciwu obywatelskiego działających w przestrzeni Internetu. Istotne zagadnienie badawcze, któremu należałoby się przyjrzeć, dotyczy rozstrzygnięcia, czy działania owych sieciowych aktywistów (w artykule określanych mianem haktywiści – pojęcie rozwinięte w kolejnych akapitach artykułu) należy postrzegać jako czynności zagrożone sankcjami karnymi, czy też w szczególnie w odniesieniu do niedawnych wydarzeń związanych chociażby z udziałem grupy Anonymous w cyberkonflikcie towarzyszącym wojnie w Ukrainie – jako działania uzasadnione wyższą koniecznością walki z wszelkimi przejawami niesprawiedliwości, cenzury i ograniczania swobód obywatelskich.

Pojęcie haktywizm powstało z połączenia dwóch słów: haking (ang. *hacking*) oraz aktywizm[1]. Samo określenie „hakować" lub „hakowanie" czy nawet „haker" (jako osoba zdolna do hakowania) występuje często w pejoratywnym kontekście. Określenia te można utożsamiać z czymś nielegalnym lub wątpliwym pod względem ustanowionych norm prawnych, a to dlatego że „haking w przekazach medialnych zaczął być kojarzony z nielegalnym włamaniem do komputera"[2]. W podobny sposób można postrzegać środowisko hakerów, jednakże ich wizerunek obok skrajnie pejoratywnego, w którym to hakerzy są postrzegani jako „włamywacze" lub „przestępcy" dokonujący nielegalnych ingerencji w infrastrukturę sieciową[3], może być umiarkowanie korzystny. W tym drugim przypadku hakerzy są postrzegani jako pasjonaci nowych tech-

[1] P. Taylor, *From hackers to hacktivists: speed bumps on the global superhighway?*, „New Media & Society" 2005, vol. 7(5), s. 625–646.

[2] T. Jordan, *Activism! Direct action, hacktivism and the future of society*, London 2002, s. 120.

[3] A. Chandler, *The changing definition and image of hackers in popular discourse*, „International Journal of the Sociology of Law" 1996, vol. 24, s. 229–251.

nologii, tworzący nowe i/lub usprawniający istniejące rozwiązania teleinformatyczne[4].

Przy porównywaniu obszaru działań hakerów i haktywistów warto zwrócić uwagę na to, że hakerzy działają głównie w przestrzeni systemów teleinformatycznych. Z kolei haktywiści w swoim obszarze działań uwzględniają zarówno środowisko sieciowe, jak i rzeczywistą przestrzeń społeczną[5]. Istotne są również motywy działań wymienionych grup. Haktywistom – w odróżnieniu od hakerów – nie zależy na wyrządzeniu szkody osobistej bądź majątkowej poprzez ingerencję w systemach teleinformatycznych (i odnoszenie własnych korzyści). Dla haktywistów ingerencja w systemy informatyczne staje się jedynie formą rozszerzania działań ze świata fizycznego, charakterystycznych dla różnorodnych form nieposłuszeństwa obywatelskiego. A zatem działania, takie jak atak DDoS (ang. *Distributed Denial of Service*)[6] na daną witrynę (np. nadawany z Rosji prokremlowski anglojęzyczny serwis informacyjny Russia Today[7]), w istocie mogą być odpowiednikiem dokonywanych w środowisku fizycznym protestów w charakterze np. strajku okupacyjnego (ang. *sit-ins*)[8].

Na przestrzeni rozwoju ruchu haktywistów (ale częściowo również hakerów) warto wymienić kilka istotnych dokumentów stanowiących ich podwaliny ideologiczne. Pierwszy z nich, określony mianem *Hacker Manifesto*, został opublikowany przez Loyda Blankenshipa w 1986 r., czyli jeszcze przed epoką upowszechnienia komercyjnego Internetu[9]. Dekadę później, w 1996 r. John Perry Barlow opublikował w sieci *Declaration of Independence of Cyberspace*, jako odpowiedź na amerykańską ustawę The Telecommunications Act of 1996. Ustawa miała wprowadzić istotne zmiany w funkcjonowaniu telewizji kablowej oraz sieci teleinformatycznej, których celem miało być pobudzenie konkurencji w sektorze usług telekomunikacyjnych. Haktywiści zmiany te postrzegali jednak jako formę ingerencji państwa w obszarze cyberprzestrzeni, wskazując że „rządy nie mogą i nie będą zawłaszczać przestrzeni Internetu"[10]. W podob-

[4] V. Karagianopoulos, *Living with hacktivism: from conflict to symbiosis*, London 2018.

[5] P. Taylor, op. cit., s. 625–646.

[6] C. Auty, *Political hacktivism: tool of the underdog or scourge of cyberspace?*, „Aslib Proceedings: New Information Perspectives" 2004, vol. 56(4), s. 212–221; M. Sauter, *„LOIC will tear us apart": the impact of tool design and media portrayals in the success of activist DDOS attacks*, „American Behavioral Scientist" 2013, vol. 57(7), s. 983–1007.

[7] D. Milmo, *Anonymous: the hacker collective that has declared cyberwar on Russia*, „The Guardian", 27.02.2022, https://www.theguardian.com/world/2022/feb/27/anonymous-the-hacker-collective-that-has-declared-cyberwar-on-russia?CMP=Share_iOSApp_Other (data dostępu: 13.09.2022).

[8] T. Jordan, T. Paul, *Hacktivism and cyberwars: rebels with a cause?* London 2004; T. Jordan, op. cit.

[9] L. Blankenship, *The Hackers Manifesto – Hacker Text*, [w:] *The Hackers Manifesto by the Mentor – Hacker Text*, darknet.org.uk, 4.09.2017, https://www.darknet.org.uk/2010/04/the-conscience-of-a-hacker-aka-the-hackers-manifesto-by-the-mentor/ (data dostępu: 13.09.2022).

[10] A. Greenberg, *It's been 20 years since this man declared cyberspace independence*, „Wired", 8.02.2016, https://www.wired.com/2016/02/its-been-20-years-since-this-man-declared-cyberspace-independence/ (data dostępu: 13.09.2022).

nym tonie wypowiadali się autorzy manifestu *The Hacktivismo Declaration*, opublikowanego w 2001 r. przez grupę haktywistów z organizacji The Cult of the Dead Cow. W dokumencie haktywiści wskazywali na potrzebę swobodnego dostępu do materiałów wydawanych przez władze publiczne: „Jeżeli rządzący nie są w stanie obronić Interentu, wówczas zrobimy to my”[11].

Haktywizm jako forma cyfrowego nieposłuszeństwa obywatelskiego

W filozofię działań haktywistów wpisuje się walka z wszelkimi przejawami niesprawiedliwości społecznej i mobilizowanie społeczności internautów do akcji protestów wymierzonych w instytucje postrzegane jako krzywdzące i niesprawiedliwe. Zgodnie z wcześniej przywołanym opisem haktywizm można rozpatrywać w kategoriach pojęciowych: „elektronicznego/cyfrowego nieposłuszeństwa obywatelskiego” (ang. *electronic civil disobedience*), „nowego nieposłuszeństwa obywatelskiego” czy też „nieposłuszeństwa obywatelskiego 2.0” (ang. *civil disobedience 2.0*)[12]. Samo pojęcie „nieposłuszeństwo obywatelskie” zostało spopularyzowane w Stanach Zjednoczonych w latach 50. i 60. ubiegłego wieku za sprawą ruchu pokojowego protestu w obronie równych praw obywatelskich i walki z segregacją rasową w stanach amerykańskiego południa. Symbolem ruchu nieposłuszeństwa obywatelskiego był pastor Martin Luther King organizujący słynny marsz protestacyjny z miejscowości Selma do Montgomery (stolicy stanu Alabama) w marcu 1965 r.[13] Inną równie symboliczną postacią ruchu obywatelskiego nieposłuszeństwa jest afroamerykańska działaczka Rosa Parks. Jej pierwsza forma protestu z grudnia 1955 r. polegała na nieustąpieniu miejsca białemu pasażerowi w autobusie w Montgomery w stanie Alabama (w stanie tym obowiązywała segregacja rasowa). Jej aresztowanie i skazanie przez sąd na karę grzywny oraz więzienia w zawieszeniu doprowadziło do bojkotu podróży autobusami przez kolorową ludność Montgomery oraz przyczyniło się do zakwestionowania przez Amerykański Sąd Najwyższy w wyroku z 13 listopada 1956 r. zasadności stosowania segregacji rasowej w autobusach, jako niezgodnej z amerykańską Konstytucją. Bojkoty ustąpiły dopiero po decyzji Sądu Najwyższego[14].

---

[11] *The Hacktivismo Declaration*, 4.07.2001, https://nettime.org/Lists-Archives/nettime-l-0107/msg00065.html (data dostępu: 13.09.2022). Znamienna jest data wydania manifestu: 4 lipca, czyli Dzień Niepodległości – amerykańskie święto narodowe [uwaga autora].

[12] C. Delmas, *Is hacktivism the new civil disobedience*? „Raisons Politiques” 2018, vol. 1, nr 69, s. 63–81, https://www.cairn.info/revue-raisons-politiques-2018-1-page-63.htm (data dostępu: 13.09.2022).

[13] B. Harris Combs, *From Selma to Montgomery. The long march to freedom*, New York 2013.

[14] *Rosa Parks*, „History”, 19.01.2022, https://www.history.com/topics/black-history/rosa-parks (data dostępu: 13.09.2022).

Tabela 1
Podział aktywności społecznych (ang. *activist repertoires*) zarówno w świecie rzeczywistym (*offline*), jak i w sieci (*online*)

Rodzaj aktywności	Offline	Online
Działania konwencjonalne	Aktywizm przykłady: głosowanie, prowadzenie i włączanie się do kampanii wyborczych, pokojowe protesty uliczne, bojkoty	Cyberaktywizm przykłady: e-głosowanie, organizacja zbiórek wyborczych i wpłacanie na owe zbiórki, składanie i podpisywanie e-petycji
Działania transgresyjne	Nieposłuszeństwo obywatelskie przykłady: strajki okupacyjne (ang. *sit-ins*), barykadowanie, tworzenie zaangażowanego graffiti, dzikie strajki (ang. *wildcat strikes*), kolportowanie prasy podziemnej, teatr o charakterze opozycyjnym, sabotaż	Haktywizm przykłady: hakowanie witryn internetowych, przekierowanie na inne witryny, ataki DDoS, kradzież danych, parodiowanie witryn, wirtualny sabotaż, tworzenie oprogramowania
Działania gwałtowne	Terroryzm przykłady: ataki bombowe skierowane na rządzących, uprowadzanie osób prominentnych, działania ekoterrorystyczne (np. *tree spiking*)	Cyberterroryzm przykłady: przejęcie kontroli lotów, hakowanie elektrowni skutkujące brakiem zasilania/ocieplania w porze zimowej etc.

Źródło: A. Samuel, *Hacktivism and the future of political participation*, Cambridge MA 2004.

Haktywizmu nie można utożsamiać z działaniami konwencjonalnymi, zarówno w przestrzeni fizycznej (aktywizm), jak i w cyberprzestrzeni (cyberaktywizm). Z drugiej strony haktywizmu nie można również jednoznacznie utożsamiać z działaniami gwałtownymi, takimi jak terroryzm oraz cyberterrorym. Haktywizm należy do kategorii działań transgresyjnych związanych z przekraczaniem przyjętych konwencjonalnych form protestu wobec instytucji postrzeganych jako niesprawiedliwe i dyskryminujące. Może przybierać formę hakowania witryn internetowych, przekierowania na inne witryny, ataków DDoS, kradzieży danych, parodiowania witryn, wirtualnego sabotażu czy też tworzenia własnego nielicencjonowanego oprogramowania. Odpowiednikiem haktywizmu w świecie fizycznym są przejawy nieposłuszeństwa obywatelskiego, takie jak: strajki okupacyjne (ang *sit-ins*), barykadowanie, tworzenie zaangażowanego graffiti, dzikie strajki (ang. *wildcat strikes*), polegające na wszczynaniu przez pracowników akcji protestacyjnej bez wcześniejszych uzgodnień i zapowiedzi wobec pracodawcy, kolportowanie prasy podziemnej, teatr o charakterze opozycyjnym, sabotaż. W tabeli 1 zawarto zestawienie najważniejszych charakterystyk aktywności społecznych online oraz offline, z podziałem na działania konwencjonalne, transgresyjne i gwałtowne.

Tabela 2

Przykłady najbardziej znanych grup haktywistów

Nazwa	Cel ataków	Metody	Cechy wyróżniające daną grupę
Anonymous	Na początku działalności: • Użytkownicy grupy dyskusyjnej 4chan • Znane osobistości ze środowiska online W późniejszej działalności: • Aktywizm o podłożu ideologicznym, np. ataki na Kościół Scjentologiczny • Kampanie, których celem jest ochrona wolności w Internecie, np. Stop Online Piracy (SOPA), Protect Intellectual Property Right (PIPA) • Odpowiedź na akcje militarne, takie jak agresja Rosji na Ukrainę z lutego 2022 (oraz wcześniejsze manewry na Krymie) lub operacja „Filar Obrony" przeprowadzona przez wojsko izraelskie w Strefie Gazy • Ataki online na organizację terrorystyczną ISIS, sztab Donalda Trumpa podczas prezydenckiej kampanii wyborczej w USA w 2016 r., witryny Ku Klux Klan (KKK) – szczególnie w okresie protestów Black Lives Matter (BLM) w 2020 r.	• *Pranks* (tłum. z ang. 'psoty') • Nękanie online • *Doxxing* (wyszukiwanie informacji o danej osobie w zasobach sieci) • Ataki DDoS	• Grupa kojarzona ze współczesnym definiowaniem haktywizmu • Charakterystyczne maski Guy'a Fawkesa (uśmiechnięta twarz z wąsikiem i bródką) noszone przez członków i zwolenników Anonymous stały się symbolem haktywizmu
Wikileaks/ Edward Snowden	Odpowiedzialny za wyciek do mediów tysięcy dokumentów, w których zawarto dane dotyczące praktyki inwigilacji przez amerykańskie służby wywiadowcze, które to Snowden postrzegał jako naruszenie prawa do prywatności obywateli USA	• Pobranie i zgromadzenie dokumentów pochodzących z amerykańskiej Agencji Bezpieczeństwa Narodowego (NSA)	• Wciąż nie został ujęty przez amerykańskie władze (poszukiwany listem gończym) • Uzyskał tymczasowy azyl, a następnie (od 26 września 2022 r.) obywatelstwo Federacji Rosyjskiej

cd tabeli 2

LulzSec	• Fox.com • Grupa medialna PBS • Przedsiębiorcy z rynku gamingowego, m.in. Nintendo, Playstation (systemy zabezpieczeń, witryna Playsta- • tion), Bethesda Studios	• Kradzież i rozpowszechnianie prywatnych danych • Paraliżowanie witryn i systemów online	• Atak na witrynę afiliowaną przez amerykańskie FBI, zwróciło uwagę służb wywiadowczych na grupę haktywistów i doprowadziło ostatecznie do jej upadku • Część członków grupy LulzSec została aresztowana i osądzona przez amerykański wymiar sprawiedliwości
Impact Team	Portal randkowy Ashley Madison – dla osób będących w stałych związkach, który to grupa haktywistów uznała za niemoralny	• Kradzież danych ponad 32 mln użytkowników portalu • Żądanie usunięcia portalu • Ostatecznie – otwarty wyciek danych	• Członkowie grupy utrzymywali, że musieli upublicznić dane użytkowników portalu, ponieważ są oni „niewiernymi łajdakami niezasługującymi na zachowanie anonimowości”
Redhack	Instytucje państw bliskowschodnich podczas Arabskiej Wiosny (2010) oraz protestów antyrządowych w Stambule (protestów Gezi) w 2013 r.	• Ataki DDoS • Wyciek danych	• adykalnie lewicowe ugrupowanie • Postrzegają siebie jako grupę marksistowsko-leninowską
Cyber Berkut	Witryny NATO oraz ukraińskich instytucji rządowych	• Ataki DDoS • Wyciek danych	• Prorosyjska grupa hakerska

cd tabeli 2

The Red Hacker Alliance	Planowany atak na CNN (któremu udało się zapobiec)	• Blokowanie witryn • Zakłócanie infrastruktury	• Jedna z najlepiej znanych grup haktywistów, działająca od lat 90. XX w.
The Chaos Computer Club (CCC)	Wszelkie przejawy cenzury w Internecie oraz projekty związane z testowaniem broni nuklearnej	• Blokowanie witryn • Zakłócanie infrastruktury teleinformatycznej	• Jedna z pierwszych grup haktywistów
Worms Against Nuclear Killers	Projekt związany z wysłaniem sondy Galileo na orbitę okołoziemską	• Infekowanie komputerów wirusami	• Z powodu ataków hakerskich projekt stracił pół miliona USD
Di5s3nSi0N	Witryna Amaq – serwis agencji informacyjnej należącej do ISIS	• Ataki DDoS • Wyciek danych	• Haktywiści upublicznili dane subskrybentów serwisu Amaq

Źródło: A. Pawlicka, M. Choraś, M. Pawlicki, *The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good*, „Personal and Ubiquitous Computing" 2021, vol. 25.

Wśród najbardziej popularnych organizacji zrzeszających haktywistów należy wymienić grupę Anonymous czy też serwis Wikileaks założony przez Juliana Assange'a. Wśród innych organizacji pojawiających się w poniższym zestawieniu należy również wskazać LulzSec, Impact Team, Redhack, Cyber Berkut, The Red Hacker Alliance, The Chaos Computer Club (CCC), Worms Against Nuclear Killers, Di5s3nSi0N. W tabeli 2 scharakteryzowano wymienione grupy haktywistów, wskazując kolejno: cel ataków, stosowane przez nich metody działań w sieci oraz cechy wyróżniające daną grupę.

Regulacje prawne dotyczące haktywizmu

Kwestię penalizacji działań związanych z cyberprzestępstwami uwzględniono w konwencji budapeszteńskiej zawartej przez Radę Europejską w 2001 r.[15], sygnowanej przez 67 państw. Zgodnie jej z treścią art. 5 „każde z państw sygnatariuszy (strona Konwencji) przyjmuje takie środki ustawodawcze i inne, jakie mogą być niezbędne do uznania za przestępstwo w jej prawie krajowym, popełnione umyślnie, następujących działań: poważne, bezprawne utrudnianie funkcjonowania systemu komputerowego poprzez wprowadzanie, przekazywanie, uszkadzanie, usuwanie, pogarszanie, zmienianie lub wypieranie pierwotnego charakteru danych komputerowych"[16]. Według tak przyjętej definicji cyberprzestępstwa należałoby zatem penalizować również poprzez działania haktywistów, dokonujących – jako choćby formy protestu przeciwko danej organizacji – ataków DDoS. Skutkiem owych ataków nie musi być trwałe uszkodzenie systemów teleinformatycznych, często natomiast dochodzi do pogorszenia parametrów technicznych owych systemów. To dość radykalne stanowisko jest jednak przeciwstawiane pojęciu „wolność zgromadzeń i zrzeszania się" zawartemu w art. 11 brytyjskiej ustawy o prawach człowieka (ang. *Human Rights Act*) z 1998 r.[17] Zgodnie z treścią art. 11 „Każdy człowiek ma prawo do swobodnego pokojowego zgromadzania się oraz do swobodnego zrzeszania się z innymi, w tym prawo do tworzenia i przystępowania do związków zawodowych dla ochrony swoich interesów"[18]. Organy państwa nie mogą zatem uniemożliwiać wyrażania przez obywateli niezadowolenia w formie protestów, zarówno w przestrzeni fizycznej jak i online. Tym samym organy państwa nie powinny penalizować działalności haktywistów, skupiającej się na różnorakich formach protestu w cyberprzestrzeni.

[15] Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).

[16] Art. 5. Naruszenie integralności systemu, Konwencja Rady Europy o cyberprzestępczości, sporządzona w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. z 2015 r., poz. 728).

[17] *Human Rights Act*, Legislation.gov.uk, 1998 (data dostępu: 13.09.2022).

[18] Art. 11. Freedom of assembly and association, *Human Rights Act*, Legislation.gov.uk, 1998 (data dostępu: 13.09.2022).

Ponadto w obrębie Wspólnoty Europejskiej wprowadzono szereg istotnych regulacji odnoszących się do sfery bezpieczeństwa teleinformatycznego państw członkowskich. Wśród nich należy wymienić:

- strategię Unii Europejskiej w zakresie cyberbezpieczeństwa (ang. *The EU's Cybersecurity Strategy for the Digital Decade*)[19], przyjętą przez Komisję Europejską w dniu 16 grudnia 2020 r. W dokumencie tym wskazano na potrzebę wdrożenia strategii zapewniającej większą odporność organizacji i instytucji publicznych na cyberataki, czyniąc owe instytucje mniej podatnymi również na skutki działań haktywistów;
- dyrektywę Parlamentu Europejskiego i Rady Europejskiej z dnia 12 sierpnia 2013 r. dotyczącą ataków na systemy informatyczne, zastępującą decyzję ramową Rady 2005/222/WSiSW[20], wyznaczającą ramy prawne dla państw członkowskich Wspólnoty Europejskiej w odniesieniu do ustawodawstwa dotyczącego cyberataków. Zgodnie z treścią owej dyrektywy wszelkie formy ataków DDoS należy zaliczyć do kategorii cyberprzestępczości (ang. *cybercrime*). Oznacza to, że haktywizm może podlegać sankcjom karnym w państwach członkowskich Wspólnoty;
- dyrektywę Parlamentu Europejskiego i Rady Europejskiej z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej (ang. *Network and Information Security [NIS] Directive*)[21] oraz wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady Europejskiej z dnia 16 grudnia 2020 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylającą dyrektywę (UE) 2016/1148 (ang. *NIS2 Directive Proposal*)[22]. Propozycja dyrektywy NIS2 pojawiła się jako odpowiedź na rosnące zagrożenie instytucji i państw członkowskich cyberatakami. W dokumencie podkreślono potrzebę zwiększenia poziomu zabezpieczeń systemów cybernetycznych przed potencjalnymi atakami. Jednocześnie ataki DDoS potraktowano w dokumencie jako formę cyberprzestępstwa. Tym samym haktywiści stosujący tego rodzaju strategię działań muszą się liczyć z odpowiedzialnością karną, jako potencjalni cyberprzestępcy, a niekoniecznie jako ruch społecznego sprzeciwu działający w przestrzeni Internetu.

---

[19] Wspólny komunikat do Parlamentu Europejskiego i Rady, strategia UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, Bruksela, 16.12.2020, EUR-Lex, Dokument 52020JC0018 (JOIN/2020/18 final).

[20] Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Bruksela, 12.08.2013 (Dz.U UE L 2013.218.8).

[21] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.U. UE L 2016.194.1).

[22] Wniosek Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, uchylająca dyrektywę (UE) 2016/1148, Bruksela, 16.12.2020, EUR-Lex, Dokument 52020PC0823 (COM/2020/823 final).

W polskim prawodawstwie problematykę działań o charakterze cyberprzestępczym uregulowano w Kodeksie karnym (w art. 267 § 2 oraz art. 269a). W art. 269a tegoż kodeksu scharakteryzowano działania o charakterze przestępstw komputerowych oraz przestępstw godzących w bezpieczeństwo systemów informatycznych: „Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5”[23]. W celu umożliwienia prowadzenia legalnych działań przez etycznych hakerów (określanych również mianem pentesterów), w kwietniu 2017 r. wprowadzono do Kodeksu karnego art. 269c. Zgodnie z treścią owego art. „nie podlega karze za przestępstwo określone w art. 267 § 2 lub art. 269a, kto działa wyłącznie w celu zabezpieczenia systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej albo opracowania metody takiego zabezpieczenia i niezwłocznie powiadomił dysponenta tego systemu lub sieci o ujawnionych zagrożeniach, a jego działanie nie naruszyło interesu publicznego lub prywatnego i nie wyrządziło szkody”[24]. Przepis ten należałoby przeciwstawić treści art. 267 § 2 k.k, zgodnie z którym czyn karalny popełnia ten, kto bez uprawnienia uzyskał dostęp do całości lub części systemu informatycznego[25]. Podobnie jak w przypadku regulacji na gruncie prawa międzynarodowego, nie można jednoznacznie rozstrzygnąć, czy działania haktywistów można kategoryzować jako etyczne hakowanie, niezagrożone sankcjami prawnymi. Działaniom tym nie można jednak odmawiać społecznej słuszności[26]. Argumenty na korzyść działań haktywistów pojawiają się w kolejnej części niniejszych rozważań.

Cyfrowi anarchiści czy bojownicy o wolność – przykład Anonymous

Grupa Anonymous zainicjowała swoją aktywność w 2003 r. na internetowym forum dyskusyjnym 4chan[27]. Uczestnicy Anonymous[28] określają swój

[23] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz.U. z 2022 r., poz. 1138, 1726, 1855), dalej jako k.k.

[24] Ibidem.

[25] Ibidem.

[26] N. Bochyńska, *Cyberprzestępczość a haktywizm. Jak prawo podchodzi do hakerów w białych kołnierzykach?*, CyberDefence24, 16.04.2022, https://cyberdefence24.pl/cyberbezpieczenstwo/cybermagazyn-cyberprzestepczosc-a-haktywizm-jak-prawo-podchodzi-do-hakerow-w-bialych-kolnierzykach (data dostępu: 27.10.2022).

[27] *4chan*, https://www.4chan.org/ (data dostępu: 27.09.2022).

[28] *@YourAnonCentral*, https://twitter.com/YourAnonCentral (data dostępu: 27.09.2022); *@TheAnonMovement*, https://twitter.com/theanonmovement?lang=en (data dostępu: 27.09.2022); *@YourAnonOne*, https://twitter.com/youranonone?lang=en (data dostępu: 27.09.2022)

ruch społeczny jako ruch o charakterze „anarchistycznym", cyfrowy „globalny mózg" (ang. *global brain*) lub zbiorową świadomość (ang. *hivemind*)[29]. Członkowie i zwolennicy Anonymous w przestrzeni fizycznej (np. podczas protestów ulicznych) mogą występować w charakterystycznych maskach Guy'a Fawkesa (postaci historycznej – jednego ze spiskowców, który w listopadzie 1605 r. usiłował wysadzić brytyjską Izbę Lordów) z charakterystyczną bródką i wąsikiem[30].

Pierwsze znaczące działania grupa Anonymous przeprowadziła w 2007 r., dokonując ataków DDOS na witrynę organizacji Kościoła Scjentologicznego. Powodem tych działań miała być zastosowana przez Kościół Scjentologiczny cenzura w sieci[31]. Inne znaczące działania grupy Anonymous uwzględniają cyberataki wymierzone w operatorów płatniczych PayPal oraz Visa w związku z uniemożliwianiem dokonywania wpłat online na kontrowersyjny serwis Wikileaks[32]. Kolejne warte uwzględnienia działania Anonymous są związane ze sprzeciwem dotyczącym wprowadzenia ustawy ACTA w roku 2012. Przeprowadzono wówczas serię ataków na witryny organizacji komercyjnych i rządowych m.in. w USA, Polsce, Irlandii, Słowenii i we Francji. Haktywiści z grupy Anonymous doprowadzili do wycieku adresów e-mail, loginów i haseł, a nawet szczegółów dotyczących życia prywatnego osób publicznych, w tym polityków głosujących za przyjęciem kontrowersyjnej ustawy. Ponadto haktywiści z Anonymous zaatakowali witrynę amerykańskiej agencji wywiadowczej CIA oraz upublicznili zakodowaną telekonferencję z udziałem amerykańskiej FBI oraz brytyjskiego Scotland Yardu[33]. Na fali organizowanych się na masową skalę protestów, zarówno w przestrzeni fizycznej, jak i wirtualnej, Parlament Europejski zdecydował się na odrzucenie projektu ustawy ACTA, powołując się na argument naruszenia prawa dotyczącego swobodnego dostępu do informacji[34].

W ostatnich latach grupa Anonymous przeprowadziła szereg kampanii określanych mianem „Ops", takich jak: Op Syria[35], OpLiberation[36], OpLastResort[37],

---

[29] *Hivemind*, macmillan dictionary, https://www.macmillandictionary.com/dictionary/british/hivemind (data dostępu: 27.09.2022).

[30] L. Konzack, *The Guy Fawkes Mask as visual communication of the Internet Group Anonymous*, „International Journal of Internet Trolling and Online Participation" 2015, vol. 1, nr 2, s. 53–68.

[31] P. Olson, *We are Anonymous*, London 2013.

[32] J. Uitermark, *Complex contention: analyzing power dynamics within Anonymous*, „Social Movement Studies" 2017, vol. 16(4), s. 403–417.

[33] D. Svydrenko, W. Możgin, *Hacktivism of the Anonymous Group as a fighting tool in the context of Russia's war against Ukraine*, „Future Human Image" 2022, vol. 17, s. 42–43.

[34] Ibidem.

[35] *@OpSyria*, https://twitter.com/opsyria (data dostępu: 27.09.2022).

[36] *@OpLiberation*, https://twitter.com/opliberation?lang=en (data dostępu: 27.09.2022).

[37] *@OpLastResort*, https://twitter.com/oplastresort?lang=en (data dostępu: 27.09.2022).

#OpKillingBay[38], #OpIsrael[39], OpGreenRights[40], #OpFreePalestine[41] czy Op_Russia[42]. Równie istotna była aktywność grupy Anonymous w okresie protestów na tle rasowym (ang. *Black Lives Matter* – BLM), odbywających się zarówno w USA, jak i m.in. w państwach Europy. Protesty były spowodowane społecznym wzburzeniem po śmierci George'a Floyda w wyniku działań funkcjonariuszy policji z Minneapolis w maju 2020 r.[43] W ostatnich latach szczególnie uwidoczniły się działania grupy Anonymous jako odpowiedź na pełzający od 2014 r. konflikt między Rosją i Ukrainą, zapoczątkowany aneksją Krymu i utworzeniem pod protektoratem i przy militarnym wsparciu Rosji tzw. separatystycznych republik w regionach Doniecka i Ługańska[44].

Tuż po zbrojnej agresji Rosji na Ukrainę 24 lutego 2022 r. grupa Anonymous wydała komunikat, w którym wypowiedziała cyberwojnę rosyjskim władzom. Była to odpowiedź na agresję Rosji na suwerenne państwo[45]. W wyniku działań Anonymous sparaliżowano Roscosmos – instytucję odpowiedzialną za nadzór nad rosyjskimi satelitami w przestrzeni okołoziemskiej. Ponadto już w pierwszych dniach rosyjskiej napaści na Ukrainę haktywiści z Anonymous przeprowadzili udane ataki DDoS na rosyjskie witryny działającego na zlecenie Kremla anglojęzycznego serwisu informacyjnego Russia Today (RT), witryny rosyjskich ministerstw i agend rządowych, w tym Ministerstwa Obrony, czy też witrynę Gazpromu. Skutecznie tymczasowo zablokowano możliwość skorzystania z witryn: sovam.com, com2com.ru, ptt.ru, mail.ru, goverement.ru, kremlin.ru, oraz rt.com. Ponadto 26 lutego 2022 r. haktywiści uzyskali dostęp do kanałów rosyjskiej telewizji państwowej, nadając przekaz z kanałów telewizji ukraińskiej – tym samym informując rosyjską opinię publiczną o faktycznym przebiegu rosyjskiej agresji na sąsiedni kraj[46]. W kolejnych miesiącach grupa Anonymous przeprowadziła kilka kolejnych włamań do systemów teleinformatycznych na terenie Rosji. Wśród nich można wymienić zaatakowanie rosyjskiego serwisu taksówkowego Yandex Taxi i przekierowanie wszystkich moskiewskich taksówek na wykonanie kursu z tego samego adresu, co

---

[38] *@OpKilIingBay*, https://twitter.com/OpKilIingBay (data dostępu: 27.09.2022).

[39] *@Op_Israel*, https://twitter.com/op_israel?lang=en (data dostępu: 27.09.2022).

[40] *@OpGreenRights*, https://twitter.com/opgreenrights?lang=en (data dostępu: 27.09.2022).

[41] *@OpFreePalestin3*, https://twitter.com/opfreepalestin3 (data dostępu: 27.09.2022).

[42] *@Op_Russia*, https://twitter.com/op_russia?lang=en (data dostępu: 27.09.2022).

[43] K. Jones, J.R C. Nurse, S. Li, *Out of the Shadows: Analyzing Anonymous' Twitter resurgence during the 2020 Black Lives Matter Protests*, „Proceedings of the Sixteenth International AAAI Conference on Web and Social Media" (ICWSM 2022), s. 417–428, https://ojs.aaai.org/index.php/ICWSM/article/view/19303 (data dostępu: 27.09.2022).

[44] D. Svydrenko, W. Możgin, op. cit., s. 40.

[45] *The Anonymous collective is officially in cyber war against the Russian government*, @YourAnonOne, 24.02.2022, https://twitter.com/youranonone/status/1496965766435926039 (data dostępu: 27.09.2022); *Anonymous: OpRussia*, anon2world, 27.02.2022, https://www.youtube.com/watch?v=kcb2yudJ29c (data dostępu: 27.09.2022).

[46] D. Svydrenko, W. Możgin, op. cit., s. 44-45.

doprowadziło do kompletnej destabilizacji ruchu ulicznego w stolicy Rosji[47], czy też włamanie się do kamer monitorujących siedzibę rosyjskich władz na Kremlu[48].

Podsumowanie

We wskazanym kontekście poczynania grupy Anonymous podczas wojny w Ukrainie należy postrzegać jako formę działań o charakterze cyberwojennym. W tym przypadku można mówić o uzasadnionym działaniu w słusznej sprawie i rozszerzeniu działań z fizycznego pola walki na obszar cyberprzestrzeni – czyli wojnie hybrydowej. Istotnym celem haktywistów staje się również demaskowanie nieprawdy poprzez pokazywanie rosyjskiej opinii publicznej prawdziwego obrazu wojny w Ukrainie. W tej konkretnej sytuacji nie można powoływać się na argument działań o charakterze cyberprzestępczym, które powinny podlegać sankcjom karnym. Grupa Anonymous i inni zaangażowani w konflikt w Ukrainie haktywiści działają w jednej ze zdefiniowanych przez NATO przestrzeni teatru działań wojennych (poza tradycyjnymi obszarami lądu, powietrza i wody), czyli cyberprzestrzeni[49].

W przedstawionym kontekście działania Anonymous można traktować nie tylko jako formę aktywności cyberwojennej, ale również jako akt cyfrowego nieposłuszeństwa obywatelskiego, przybierającego formę pozbawionych przemocy protestów i wymierzonych w instytucje oraz osoby dokonujące nieetycznych i nielegalnych działań[50]. Zresztą haktywiści z Anonymous wyraźnie rozróżniają, że ich działania są wymierzone w opresyjny reżim w Rosji, nie zaś w obywateli tego państwa. Świadczą o tym następujące komunikaty umieszczane w mediach społecznościowych: „Chcemy, aby obywatele Rosji zdali sobie sprawę, że bardzo dobrze wiemy, jak trudno jest sprzeciwić się dyktatorowi w obawie przed represjami”[51]. Haktywiści przesłali również krótką wiadomość

---

[47] *Atak hakerski w Moskwie. Anonymous spowodował ogromny korek*, Polska Agencja Prasowa, 2.09.2022, https://www.pap.pl/aktualnosci/news%2C1414407%2Catak-hakerski-w-moskwie--anonymous-spowodowal-ogromny-korek.html (data dostępu: 27.09.2022).

[48] *Anonymous* włamali się do monitoringu Kremla. „Nie powstrzymacie nas. Jesteśmy w środku”, Polska Agencja Prasowa, 7.04.2022, https://www.pap.pl/aktualnosci/news%2C1148661%-2Canonymous-wlamali-sie-do-monitoringu-kremla-nie-powstrzymacie-nas-jestesmy (data dostępu: 27.09.2022).

[49] J. Worona, *Cyberspace in international law*, Białystok 2017, s. 45–46.

[50] S. Wray, *On electronic civil disobedience*, „Peace Review” 1999, vol. 11, s. 107–111, https://doi.org/10.1080/10402659908426237.

[51] *Ukraińskie media: grupa Anonymous zhakowała rosyjskie państwowe kanały telewizyjne*, Polska Agencja Prasowa, 6.03.2022, https://www.pap.pl/aktualnosci/news%2C1105172%2Cukrainskie-media-grupa-anonymous-zhakowala-rosyjskie-panstwowe-kanaly (data dostępu: 27.09.2022); https://www.ukrinform.ua/rubric-world/3422289-hakeri-anonymous-povidomili-pro-zlam-derzavnih-telekanaliv-rf.html (data dostępu: 27.09.2022).

skierowaną do Władimira Putina o następującej treści: „Związek Radziecki upadł wiele lat temu, ale świat nie zapomniał o brutalności tego reżimu. Ludzie z całego świata będą stawiać opór na każdym kroku. To nie jest wojna, którą wygracie”[52].

Wciąż nie została rozstrzygnięta kwestia ochrony wolności wypowiedzi jako forma sprzeciwu haktywistów wobec wielkich korporacji i instytucji publicznych oraz rządów poszczególnych państw. W tym przypadku, zgodnie ze wskazaną w artykule treścią aktów prawnych, haktywizm niebezpiecznie zbliża się do działań o charakterze cyberprzestępczym. Jednakże ten spór może zostać w przyszłości przeważony na korzyść argumentów dotyczących ochrony wolności słowa, prawa do zgromadzeń i pokojowych protestów, a przede wszystkim prawa do informacji przysługującego obywatelom wolnych, demokratycznych państw, które stanowi motto działania haktywistów.

Wykaz literatury

Auty C., *Political hacktivism: tool of the underdog or scourge of cyberspace?*, „Aslib Proceedings: New Information Perspectives” 2004, vol. 56(4).

Chandler A., *The changing definition and image of hackers in popular discourse*, „International Journal of the Sociology of Law” 1996, vol. 24.

Harris Combs B., *From Selma to Montgomery. The long march to freedom,* Routledge, New York 2013.

Jones K., Nurse J.R.C., Li S., *Out of the Shadows: Analyzing Anonymous' Twitter resurgence during the 2020 Black Lives Matter Protests*, „Proceedings of the Sixteenth International AAAI Conference on Web and Social Media” (ICWSM 2022).

Jordan T., *Activism! Direct action, hacktivism and the future of society*, Reaktion Books, London 2002.

Jordan T., Paul T., *Hacktivism and cyberwars: rebels with a cause?* Routledge, London 2004.

Karagianopoulos V., *Living with hacktivism: from conflict to symbiosis*, Palgrave Macmillan, London 2018.

Konzack L., *The Guy Fawkes Mask as visual communication of the Internet Group Anonymous*, „International Journal of Internet Trolling and Online Participation” 2015, vol. 1, nr 2.

Olson P., *We Are Anonymous*, William Heinemann, London 2013.

Pawlicka A., Choraś M., Pawlicki M., *The stray sheep of cyberspace a.k.a. the actors who claim they break the law for the greater good*, „Personal and Ubiquitous Computing” 2021, vol. 25.

Samuel A., *Hacktivism and the future of political participation*, Harvard University, Cambridge MA 2004.

Sauter M., *„LOIC will tear us apart": the impact of tool design and media portrayals in the success of activist DDOS attacks*. „American Behavioral Scientist” 2013, vol. 57(7).

Svydrenko D., Możgin W., *Hacktivism of the Anonymous Group as a fighting tool in the context of Russia's war against Ukraine*, „Future Human Image” 2022, vol. 17.

[52] Ibidem.

Taylor P., *From hackers to hacktivists: speed bumps on the global superhighway?* „New Media & Society" 2005, vol. 7(5).
Uitermark J., *Complex contention: analyzing power dynamics within Anonymous*. „Social Movement Studies" 2017, vol. 16(4).
Worona J., *Cyberspace in international law*, WPiA UwB, Białystok 2017.
Wray S., *On electronic civil disobedience*, „Peace Review" 1999, vol. 11.

Summary

Hacktivism from a legal perspective – digital anarchists or freedom fighters?

Keywords: cybercrime law, hacktivism, online civil disobedience, Anonymous, cyberwar, cybercrime, war in Ukraine.

The aim of this article is to present the legal regulation of hacktivism – digital forms of civil disobedience. The article characterises the most important groups of hacktivists, indicating their methods of online activities. It also discusses European Community legislation relating to cybercrime and the possible criminalisation of hacktivist activities. The article concludes with a description of the activities of the Anonymous group, actively supporting cyber warfare against Russia during the war in Ukraine, and a discussion regarding the justification of these activities in light of current legal norms and the assumptions pertaining to cyberwarfare.