„dot.pl" - czasopismo Rejestru domeny .pl

Ukryte zasoby Internetu a terroryzm

Krzysztof Kaczmarek
Politechnika Koszalińska, Wydział Humanistyczny
ORCID: https://orcid.org/0000-0001-8519-1667
E-mail: puola@tlen.pl

Streszczenie

Powszechność korzystania z Internetu nie oznacza pełnej znajomości jego zawartości. Znaczna część zasobów sieci nie jest indeksowana i tym samym pozostaje niedostępna dla większości użytkowników. Artykuł analizuje wpływ tych nieindeksowanych zasobów na bezpieczeństwo cyfrowe. W szczególności badany jest ich związek z terroryzmem oraz przestępczością. Hipoteza badawcza zakłada, że ukryte zasoby Internetu znacząco wpływają na poziom bezpieczeństwa społeczeństw i państw. Do weryfikacji tej hipotezy zastosowano przegląd literatury, analizę jakościową treści dostępnych w dark webie oraz metodę desk research. Wyniki badań wskazują na istotne zagrożenia związane z działalnością terrorystyczną oraz nielegalnym handlem w ciemnej sieci, a także na wyzwania związane z monitorowaniem i zwalczaniem tych zagrożeń przy użyciu zaawansowanych technologii, w tym sztucznej inteligencji.

Słowa kluczowe: deep web, darknet, terroryzm, sztuczna inteligencja

Received: 25.04.2024
Accepted: 24.05.2024
Published: 27.05.2024

Cite this article as:
K. Kaczmarek
"Ukryte zasoby Internetu a terroryzm"

DOT.PL, no. 1/ 2024,
10.60097/DOTPL/189286

Corresponding author:
Krzysztof Kaczmarek
Politechnika Koszalińska,
Wydział Humanistyczny
E-mail: puola@tlen.pl

Hidden Internet Resources and Terrorism

Abstract

The widespread use of the Internet does not mean full knowledge of its content. A significant part of the network resources is not indexed and therefore remains inaccessible to most users. The article examines the impact of these nonindexed resources on digital security. In particular, their relationship with terrorism and crime is examined. The research hypothesis assumes that hidden Internet resources significantly influence the level of security of societies and countries. To verify this hypothesis, a literature review, qualitative analysis of content available on the Dark Web and the desk research method were used. Research results indicate significant threats related to terrorist activities and illegal trade on the Dark Web, as well as the challenges associated with monitoring and combating these threats using advanced technologies, including artificial intelligence.

Keywords: deep web, darknet, terrorism, artificial intelligence

Wstęp

Trywializmem jest stwierdzenie, że funkcjonowanie współczesnych społeczeństw i państw opiera się na dostępie do Internetu[1]. Cyfrowy świat wydaje się być naturalnym środowiskiem współczesnego człowieka. Należy jednak zauważyć, że nie wszystkie zasoby Internetu są powszechnie dostępne. Znaczna część treści jest nieindeksowana i ukryta przed standardowymi wyszukiwarkami, a dostęp do nich wymaga specjalnych uprawnień[2]. Najczęściej używane wyszukiwarki nie docierają do większości danych w Internecie, a sieć szybko pogłębia się zyskując dodatkowy wymiar. Uważa się, że większość informacji jest ukryta w głębokiej sieci (ang. *deep web*)[3]. Można przyjąć, że poszukiwanie informacji w Internecie to przeszukiwanie sieci powierzchownej lub przeszukiwanie ukrytej sieci. Pierwsza jest publicznie i bezpośrednio dostępna oraz

[1] K. Huczek, *Cyfrowi tubylcy i cyfrowi imigranci. O społecznych wyzwaniach i zagrożeniach w cyberprzestrzeni*, „Cybersecurity and Law", 2023, nr 10(2), pp. 415.
[2] K. Kaczmarek, *Darknet jako przedmiot badań nauk społecznych*, „Cybersecurity and Law", 2020, nr 4(2), pp.106.
[3] L. Ismailova, V. Wolfengagen, S. Kosikov, *A Semantic Model for Indexing in the Hidden Web*, „Procedia Computer Science", 2021, nr 190, pp. 324-325.

posiada adres statyczny. Natomiast druga jest ukryta i jest dostępna jedynie poprzez rejestrację, a interfejs wyszukiwania i dostęp są często płatne[4]. Zatem, najogólniej ujmując, ukryte zasoby Internetu to te, które nie są dostępne dla konwencjonalnych wyszukiwarek.

W związku z tym można przyjąć, że znaczna część cyfrowej przestrzeni stanowi, dla części osób korzystających w jakiejkolwiek formie z Internetu, obszar nieznany. Skutkuje to tym, że poruszanie się po ukrytych zasobach sieci może stanowić wyzwanie dla bezpieczeństwa informacji i danych. Należy jednocześnie zauważyć, że cyberprzestrzeń generuje pewne problemy i ryzyka, których liczba zwiększa się wraz z postępującym w dziedzinie ICT postępem[5], a kompetencje cyfrowe są jednym z ważniejszych wyznaczników jakości życia[6]. Zagrożenia te wynikają przede wszystkim z postępującego uzależniania funkcjonowania społeczeństw od bezawaryjnego dostępu do sieci. Dotyczy to również bezpieczeństwa. Taki stan rzeczy jest wykorzystywany przez zewnętrzne podmioty do wywierania wpływu na zachowania społeczne czy przeprowadzania cyberataków[7].

W tym miejscu należy podkreślić, że również sieci elektroenergetyczne są elementem cyberbezpieczeństwa[8]. W kontekście napiętej sytuacji międzynarodowej, zmian klimatycznych i możliwości wystąpienia ekstremalnych zjawisk pogodowych czy kryzysu energetycznego należy brać pod uwagę również możliwość fizycznego uszkodzenia infrastruktury teleinformatycznej lub elektroenergetycznej. W takich przypadkach, oparte na dostępie do informacji, funkcjonowanie społeczeństw może zostać zakłócone[9].

W przeciwdziałaniu cyfrowym zagrożeniom jednym z najważniejszych elementów jest świadomość ich istnienia. Tymczasem jednym z największych problemów związanych z

[4] S. Kaur, A. Singh, G. Geetha, X. Cheng, *IHWC: intelligent hidden web crawler for harvesting data in urban domains*, "Complex & Intelligent Systems", 2023, nr 9(4), pp. 3636.
[5] A. Bencsik, M. Karpiuk, M. Kelemen, E. Włodyka, *Cybersecurity in the Visegrad Group Countries*, "Lex Localis Press", Maribor 2023, pp. 89.
[6] A. Bencsik, M. Karpiuk, N. Strizzolo, *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law", 2024, nr 11(1), pp. 259.
[7] M. Karpiuk, *Crisis management vs. cyber threat*, „Sicurezza, terrorismo e società", 2022, nr 16, pp. 121.
[8] E. M. Włodyka, K. Kaczmarek, *Cyber Security of Electrical Grids – A Contribution to Research*, „Cybersecurity and Law", 2024, nr 2(12), pp. 268.
[9] M. Karpiuk, W. Pizło, K. Kaczmarek, *Cybersecurity Management – Current State And Directions Of Change*, "International Journal of Legal Studies", 2023, nr 2, pp. 660.

zapewnieniem bezpieczeństwa (w tym cyberbezpieczeństwa) jest skuteczność postrzegania sygnałów ostrzegawczych[10]. Dotyczy to zarówno zagrożeń związanych ze złośliwym oprogramowaniem jak i z wywieraniem wpływu na użytkowników Internetu. Może to odnosić się zarówno do szeroko rozumianej ingerencji w procesy wyborcze w państwach demokratycznych[11], czy rozpowszechniania mogących wywoływać niepokoje społeczne fałszywych informacji. Tymczasem w większości europejskich państw problem fake newsów jest traktowany jako część systemów medialnych[12].

W tym kontekście istotna jest analiza wpływu ukrytych zasobów Internetu na cyberbezpieczeństwo. Przede wszystkim deep web oraz dark web oferują środowisko, w którym mogą powstawać i rozwijać się różnorodne zagrożenia, takie jak handel nielegalnymi towarami i usługami, wymiana złośliwego oprogramowania, czy planowanie oraz organizowanie cyberataków i zamachów terrorystycznych.

Celem niniejszego artykułu jest analiza wpływu nieindeksowanych zasobów Internetu na bezpieczeństwo. Natomiast hipoteza badawcza zakłada, że zasoby i środowisko ukrytej sieci (deep web i dark web) znacząco wpływają na poziom cyfrowego bezpieczeństwa społeczeństw i państw.

W celu jej weryfikacji zastosowano następujące metody badawcze: przegląd literatury i dostępnych źródeł internetowych. Przeprowadzona została również analiza jakościowa treści dostępnych w dark webie. Natomiast metoda desk research pozwoliła na uporządkowanie informacji dotyczących skuteczności cyfrowych narzędzi pozwalających na monitorowanie ukrytych zasobów Internetu.

Typologia zasobów Internetu i wyzwania bezpieczeństwa dla jego warstw

Ze względu na dostępność zasobów Internet można podzielić na trzy warstwy:

[10] B. Ćwik, *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review", 2017, nr 3, pp. 28.
[11] E. M. Włodyka, *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce*, [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, M. Karpiuk [ed.], Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024, pp. 116.
[12] K. Wasilewski, *Fake News and the Europeanization of Cyberspace*, "Polish Political Science Yearbook", 2021, nr 50(4).

- Internet powierzchniowy (ang. *Surface Web*) – publicznie dostępny, indeksowany przez standardowe wyszukiwarki takie jak Google czy Bing. Zawiera strony internetowe, blogi, portale społecznościowe i informacyjne, itp.
- Głęboka sieć (ang. *Deep Web*) – zawiera zasoby nieindeksowane przez standardowe wyszukiwarki, które są dostępne za pomocą specjalnych uprawnień lub rejestracji. Mogą to być bazy danych lub płatne serwisy.
- Ciemna sieć (ang. *Dark Web, Dark Net*) – część głębokiej sieci dostępna jedynie za pomocą specjalnego oprogramowania (np. TOR), celowo ukryta. Chociaż nie gwarantuje, pozwala na zachowanie anonimowości. Zawiera anonimowe fora, nielegalne rynki, strony z nielegalnym oprogramowaniem.

Przed każdą z tych warstw stoją inne, chociaż wiążące się ze sobą, wyzwania bezpieczeństwa. Dla Internetu powierzchniowego są one najczęściej związane z phishingiem, malware, atakami XSS (ang. *Cross-Site Scripting*), utratą prywatności przez cookies[13]. W przypadku głębokiej sieci wyzwania te dotyczą naruszenia danych, nieautoryzowanego dostępu i działalności przestępczej[14]. Natomiast wyzwania bezpieczeństwa związane z dark web dotyczą anonimowości ułatwiającej przestępczą działalność, kradzieży tożsamości (handel skradzionymi dokumentami i danymi osobowymi) i cyberbezpieczeństwa (handel cyfrowymi narzędziami umożliwiającymi przeprowadzanie cyfrowych ataków)[15]. Każda z warstw Internetu wymaga unikalnego podejścia do zarządzania bezpieczeństwem, które uwzględnia jej specyficzne zagrożenia i ryzyka.

Darknet

Darknet, jako najbardziej ukryta część deep web, jest miejscem, w którym kluczowa jest anonimowość. Jej rozmiar, nieindeksowana, fragmentaryczna i wielowarstwowa zawartość sprawiają, że wykrywanie w niej przestępstw jest skrajnie trudne, a w wielu przypadkach niemożliwe. Dodatkowo ekosystem ciemnej sieci jest wysoce

[13] G. A. Khan, *The Web Layers: Security Challenges and Solutions in Surface, Deep and Dark Web*, SSRN 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4722851, dostęp: 19.05.2024.
[14] ibidem.
[15] ibidem.

nieprzewidywalny – każdego dnia stare strony znikają i pojawiają się nowe[16]. Należy również podkreślić, że aby znaleźć określoną zawartość w dark web należy korzystać z katalogów lub dedykowanych wyszukiwarek. W katalogach najłatwiej można spotkać adresy stron z nielegalnymi towarami i usługami. Jednocześnie transakcje odbywają się przy wykorzystaniu kryptowalut, które pozwalają użytkownikom na zachowanie anonimowości. Najczęściej są to oferty sprzedaży kradzionych lub fałszywych dokumentów, kart płatniczych, nielegalnych leków i narkotyków czy hakerów do wynajęcia[17]. Jednak można tam znaleźć również, zapewniające anonimowość, strony do kontaktu ze służbami wywiadowczymi państw, np. z amerykańską Centralną Agencją Wywiadowczą[18].

Dostęp do dark web sam w sobie nie jest nielegalny, choć ta część sieci jest często kojarzona z nielegalną działalnością ze względu na jej anonimowy charakter. Jednak technologia i sieci tworzące dark web nie są niezgodne z prawem. Natomiast legalność działań podejmowanych w darknecie zależy od charakteru tych działań i jurysdykcji, której podlegają. Natomiast ciemna sieć to złożona i różnorodna część Internetu, która pozostaje owiana tajemnicą i często źle rozumiana przez ogół społeczeństwa. Jej technologie prywatności i anonimowości oferują kluczowe korzyści w zakresie ochrony wolności słowa, prywatności i umożliwienia bezpiecznej komunikacji, zwłaszcza w środowiskach, w których jest ona zagrożona. Jednakże zdolność dark web do anonimizowania użytkowników i działań stwarza również poważne wyzwania, ponieważ może ułatwiać nielegalne i szkodliwe działania. Jest oczywiste, że ciemna sieć będzie nadal ewoluować, podobnie jak narzędzia i metody dostępu do niej, charakter prowadzonych w niej działań oraz ramy prawne i etyczne regulujące jej wykorzystanie.

W zwalczaniu przestępstw w darknecie coraz większe zastosowanie znajdują technologie sztucznej inteligencji (AI), które stają się coraz skuteczniejsze w analizie danych zarówno z powierzchniowego jak i ciemnego Internetu. Algorytmy uczenia maszynowego są

[16] S. Nazah et. al., *Evolution of Dark Web Threat Analysis and Detection: A systematic Approach*, "Ieee Access", 2020, nr 8, pp. 171815.
[17] *OnionLinks*, http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/ (adres w Dark Web), dostęp: 19.05.2024.
[18] Central Intelligence Agency, http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/ (adres w Dark Web), dostęp: 19.05.2024.

wykorzystywane do automatycznego łączenia profili użytkowników na różnych forach, analizując podobieństwa w nazwach użytkowników, treściach i sieciach kontaktów. AI pomaga w identyfikacji i powiązaniu tożsamości osób działających w ciemnej sieci z ich tożsamościami w powierzchniowym Internecie[19].

Jednak istotne jest to, że dark web pozwala na zachowanie anonimowości, ale jej nie gwarantuje. Pozwalają na to cyfrowe narzędzia są jedynie narzędziami, których sposób i efektywność wykorzystania zależą jedynie od użytkowników. Jednocześnie wydaje się, że istnieją lub wkrótce powstaną narzędzia pozwalające na monitorowanie tej części sieci. Nie będą natomiast powszechnie dostępne.

Terrorystyczna aktywność w Darknecie

Terroryści są aktywni na różnych platformach internetowych od końca lat 90. XX wieku. Jednak surface web okazała się zbyt ryzykowna dla poszukujących anonimowości terrorystów: można ją było monitorować, śledzić, a użytkowników lokalizować. W związku z tym po atakach w Paryżu z listopada 2015 r. organizacje terrorystyczne przeniosły znaczną część swojej aktywności do darknetu. Jednym z przykładów wykorzystywania ciemnej sieci przez terrorystów jest działalność tzw. państwa islamskiego (ang. Islamic State of Iraq and Syria, ISIS), które wykorzystywało dark web do rekrutacji bojowników, planowania ataków oraz rozpowszechniania propagandy. Dzięki ciemnej sieci, organizacja ta mogła skutecznie prowadzić globalną kampanię terroru[20].

Jednak aktywność tego typu organizacji w Darknecie polega nie tylko na przygotowywaniu ataków, ale również na zdobywaniu środków finansowych na swoją działalność. W związku z tym podjętych zostało wiele działań mających na celu monitorowanie tej części Internetu.

[19] K. Foy, *Artificial intelligence is helping investigators fight crime on the dark web*, Lincoln Laboratory, Massachusetts Institute of Technology, 2019, https://www.ll.mit.edu/news/artificial-intelligence-helping-investigators-fight-crime-dark-web, dostęp: 19.05.2024.

[20] G. Weimann, *Going Darker? The Challenge of Dark Net Terrorism*, Woodrow Wilson International Center for Scholars, Washington, 2021, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf, dostęp: 22.05.2024.

Jedną z inicjatyw mających na celu analizę i zwalczanie nielegalnej działalności prowadzonej w Darknecie był, współfinansowany przez unijny program Horyzont 2020, projekt DANTE (Darknet Advanced Network Technology and Exploitation). Był to europejski projekt badawczo-rozwojowy, który miał na celu opracowanie narzędzi i technologii pozwalających na monitorowanie, analizę i wykrywanie nielegalnych działań w ciemnej sieci.

Główne cele projektu DANTE obejmowały:

- zbieranie i analizowanie danych: opracowanie technologii do zbierania danych z różnych źródeł w ciemnej sieci, w tym z ukrytych usług i forów dyskusyjnych;
- wykrywanie i śledzenie: rozwijanie algorytmów do identyfikacji podejrzanych działań i śledzenia nielegalnych transakcji oraz komunikacji;
- analiza danych: stosowanie zaawansowanych technik analizy danych, w tym analizy big data i sztucznej inteligencji, w celu odkrywania wzorców i powiązań między różnymi podmiotami w ciemnej sieci;
- współpraca międzynarodowa: promowanie współpracy między agencjami rządowymi, organami ścigania i instytucjami badawczymi na całym świecie w celu skuteczniejszej walki z przestępczością w ciemnej sieci[21].

System powstały w ramach projektu DANTE jest obecnie wykorzystywany między innymi do:

- wykrywania i monitorowania źródeł istotnych danych związanych z terroryzmem w powierzchniowej, głębokiej sieci i ciemnej sieci;
- dokładnego i szybkiego wykrywania, analizy i kategoryzacji wielojęzycznych treści podejrzanych o terroryzm;
- zakrojonych na szeroką skalę analiz czasowych trendów terrorystycznych;
- podsumowywania w czasie rzeczywistym wielojęzycznych i multimedialnych treści związanych z terroryzmem;
- wykrywania dezinformacji w internetowych treściach;

[21] D. Cohen et al., *DANTE: A framework for mining and monitoring darknet traffic,* "Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security", 2020, Proceedings, Part I 25, Springer International Publishing, https://doi.org/10.48550/arXiv.2003.02575

- wykrywania i monitorowania osób oraz łączenie pseudonimów z osobami fizycznymi;
- dokładnej i szybkiej identyfikacji internetowych społeczności i grup terrorystycznych;
- przechwytywania, przechowywania i zabezpieczania odpowiednich danych do dalszej analizy kryminalistycznej[22].

Rozwój sztucznej inteligencji sprawia, że powstaje coraz więcej, opartych na jej algorytmach, cyfrowych narzędzi, które są w stanie samodzielnie monitorować i analizować ruch w Darknecie[23]. Można zatem przyjąć, że istnieją skuteczne narzędzia zwalczania terroryzmu i innych przestępstw w ciemnej sieci. Należy jednak przeanalizować zarówno ich możliwości jak i efektywność wykorzystywania.

Podsumowanie

Istniejące cyfrowe narzędzia pozwalają na monitorowanie darknetu, jednak ich efektywność jest ograniczona, o czym świadczy liczba i dostępność znajdujących się w tej części sieci sklepów z nielegalnymi towarami. Narzędzia te, mimo że są technologicznie zaawansowane, nie są w stanie skutecznie przeciwdziałać nielegalnym i niebezpiecznym aktywnościom.

Jednym z głównych problemów jest skala i złożoność darknetu, który charakteryzuje się dużą anonimowością użytkowników oraz dynamicznie zmieniającą się strukturą. Sklepy z nielegalnymi towarami często zmieniają swoje adresy, co utrudnia ich namierzanie i stałe monitorowanie. Dodatkowo wiele transakcji odbywa się za pomocą kryptowalut, co dodatkowo utrudnia śledzenie przepływu środków finansowych.

Narzędzia do monitorowania darknetu, takie jak zaawansowane systemy analizy danych oraz algorytmy sztucznej inteligencji, pozwalają na identyfikowanie wzorców i trendów, jednak ich efektywność jest ograniczona przez konieczność ciągłej aktualizacji i adaptacji do nowych metod stosowanych przez przestępców i organizacje terrorystyczne. Istotnym

[22] DANTE, *DANTE- Detecting and analysing terrorist-related online contents and financing activities*, https://www.h2020-dante.eu/, dostęp: 22.05.2024.
[23] Q. Abu Al-Haija et al., *Machine-Learning-Based Darknet Traffic Detection System for IoT Applications*, "Electronics", 2022, nr 11(4), 556, pp. 7.

wyzwaniem jest również współpraca międzynarodowa. Darknet jest zjawiskiem globalnym, co wymaga skoordynowanych działań różnych państw i organizacji międzynarodowych. Jednak brak jednolitych standardów prawnych i różnice w podejściu do ochrony prywatności i wolności obywatelskich stanowią dodatkowe wyzwanie.

Narzędzia monitorujące są często stosowane reaktywnie, a nie proaktywnie. Oznacza to, że działania podejmowane są dopiero po wykryciu nielegalnych działań, co daje przestępcom przewagę czasową na zatarcie śladów. Ponadto, ograniczone zasoby finansowe i kadrowe organów ścigania sprawiają, że monitorowanie darknetu nie jest priorytetem w porównaniu do innych działań operacyjnych.

W celu poprawy efektywności monitorowania darknetu konieczne jest inwestowanie w rozwój technologii oraz szkolenie specjalistów z zakresu cyberbezpieczeństwa. Współpraca publiczno-prywatna oraz wymiana informacji między sektorem technologicznym a organami ścigania mogą znacząco przyczynić się do zwiększenia skuteczności działań. Ważne jest również prowadzenie badań naukowych nad nowymi metodami analizy danych i algorytmami sztucznej inteligencji, które mogą pomóc w identyfikacji i śledzeniu aktywności kryminalnej i terrorystycznej.

Należy również podkreślić, że jednym z działań, których celem jest zapobieganie atakom terrorystycznym jest monitoring i analiza całego Internetu w czasie rzeczywistym. W kontekście napiętej sytuacji międzynarodowej badania nad opracowaniem takich narzędzi powinny być jednym z priorytetów państw demokratycznych. Należy bowiem brać pod uwagę to, że reżimy totalitarne działają w zupełnie odmiennej od zachodniej, kulturze politycznej i prawnej.

Tocząca się w cyberprzestrzeni wojna i mający tam miejsce wyścig zbrojeń powodują, że zagrożenia związane ze wszystkimi warstwami Internetu będą miały coraz większy wpływ na funkcjonowanie nie tylko społeczeństw i państw, ale i jednostek. Narzędzia pozwalające na monitorowanie głębokiej sieci mogą być wykorzystywane również przez ugrupowania terrorystyczne w celu zdobycia informacji lub pozyskania środków finansowych. Pozwalają one również na naruszenie integralności danych, w tym tych, które są kluczowe dla bezpieczeństwa państwa. Natomiast narzędzia pozwalające na

monitorowanie darknetu, wykorzystane przez reżimy totalitarne, mogą spowodować utratę osobowych źródeł informacji. W związku z tym sposoby analizy całej, łącznie z ciemną, sieci, nie powinny być powszechnie znane, a wykorzystywane narzędzia dostępne. Powinny one być traktowane tak jak technologie wojskowe, którymi w znacznym stopniu są. Podejście takie pozwala na postawienie hipotezy, że tego rodzaju narzędzia już istnieją. Natomiast brak widoczności efektów zwalczania rynku nielegalnych towarów i usług w ciemnej sieci może wynikać z konieczności ukrywania istnienia takich narzędzi. Jednak mogą one zostać (lub są) wykorzystywane w celu przeciwdziałaniu wielkoskalowym zagrożeniom takim jak hybrydowe operacje państw totalitarnych.

Bibliografia

Abu Al-Haija, Q., Krichen, M., Abu Elhaija, W., *Machine-Learning-Based Darknet Traffic Detection System for IoT Applications*, "Electronics", 2022, nr11(4), 556, pp. 1-19.

Bencsik, A., Karpiuk, M., Kelemen, M., Włodyka, E., *Cybersecurity in the Visegrad Group Countries*, Lex Localis Press, Maribor 2023.

Bencsik, A., Karpiuk, M., Strizzolo, N., *Information Society Services and Their Cybersecurity*, „Cybersecurity and Law", 2024, nr 11(1), pp. 258-270.

Central Intelligence Agency, http://ciadotgov4sjwlzihbbgxnqg3xiyrg7so2r2o3lt5wz5ypk4sxyjstad.onion/ (adres w Dark Web) , dostęp: 19.05.2024.

Cohen, D., et al., *DANTE: A framework for mining and monitoring darknet traffic. Computer Security–ESORICS 2020: 25th European Symposium on Research in Computer Security, ESORICS 2020, Guildford, UK, September 14–18, 2020, Proceedings, Part I 25*, Springer International Publishing, 2020, https://doi.org/10.48550/arXiv.2003.02575.

Ćwik, B., *Postrzeganie zagrożeń w systemach bezpieczeństwa organizacji*, „Modern Management Review", 2017, nr 3, pp. 27-37.

DANTE, *DANTE- Detecting and analysing terrorist-related online contents and financing activities*, https://www.h2020-dante.eu/, dostęp: 22.05.2024.

Foy, K., *Artificial intelligence is helping investigators fight crime on the dark web*, Lincoln Laboratory. Massachusetts Institute of Technology 2019, https://www.ll.mit.edu/news/artificial-intelligence-helping-investigators-fight-crime-dark-web, dostęp: 19.05.2024.

Huczek, K., *Cyfrowi tubylcy i cyfrowi imigranci. O społecznych wyzwaniach i zagrożeniach w cyberprzestrzeni*, „Cybersecurity and Law", 2023, nr 10(2), pp. 414-429.

Ismailova, L., Wolfengagen, V., Kosikov, S., *A Semantic Model for Indexing in the Hidden Web*, „Procedia Computer Science", 2021, nr 190, pp. 324-331.

Kaczmarek, K., *Darknet jako przedmiot badań nauk społecznych*, „Cybersecurity and Law", 2020, nr 4(2), pp. 105-113.

Karpiuk M., *Crisis management vs. cyber threat*, „Sicurezza, terrorismo e società", 2022, nr 16(2), pp. 113-123.

Karpiuk M., Pizło W., Kaczmarek K., *Cybersecurity Management – Current State And Directions Of Change*, „International Journal of Legal Studies", 2023, nr 2, pp. 645-663.

Kaur, S., Singh, A., Geetha, G., Cheng, X., *IHWC: intelligent hidden web crawler for harvesting data in urban domains*, "Complex & Intelligent Systems", 2023, nr 9(4), pp. 3635-3653.

Khan, G. A., *The Web Layers: Security Challenges and Solutions in Surface, Deep and Dark Web*, SSRN 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4722851, dostęp: 19.05.2024.

Nazah, S., et. al., *Evolution of Dark Web Threat Analysis and Detection: A systematic Approach* "Ieee Access", 2020, nr 8, pp. 171796-171819.

OnionLinks, http://s4k4ceiapwwgcm3mkb6e4diqecpo7kvdnfr5gg7sph7jjppqkvwwqtyd.onion/ (adres w Dark Web), dostęp: 19.05.2024.

Wasilewski, K., *Fake News and the Europeanization of Cyberspace*, „Polish Political Science Yearbook", 2021, nr 50(4).

Weimann, G., *Going Darker? The Challenge of Dark Net Terrorism*, Woodrow Wilson International Center for Scholars, Washington 2021, https://www.wilsoncenter.org/sites/default/files/media/documents/publication/going_darker_challenge_of_dark_net_terrorism.pdf, dostęp: 22.05.2024.

Włodyka E. M., *Polaryzacja, kohabitacja czy integracja? Wyzwania cyberbezpieczeństwa procesów wyborczych w Polsce* [in:] *Cyberbezpieczeństwo. Aspekty krajowe i międzynarodowe*, M. Karpiuk (red.), Wydawnictwo Akademii Sztuki Wojennej, Warszawa 2024.

Włodyka, E. M., Kaczmarek, K., *Cyber Security of Electrical Grids – A Contribution to Research*, „Cybersecurity and Law", 2024, nr 2(12), 22. 260-272.