DANIEL MIDER
ORCID: 0000-0003-2223-5997

EWA ALEKSANDRA ZIEMAK
ORCID: 0000-0003-2516-3247

DOI: 10.4467/20801335PBW.21.003.13560

Technologie wspierające prywatność – ideologia, prawo, wdrożenia

Związek technologii kryptograficznych z terroryzmem był przedmiotem analiz prowadzonych pod koniec lat 90. XX w.[1] Obszernych opracowań doczekały się również powiązania między Internetem a terroryzmem[2]. W anglo- i polskojęzycznej literaturze przedmiotu brakuje natomiast analiz skupionych na ocenie praktycznego wykorzystania w działalności terrorystycznej dostępnych i szeroko używanych narzędzi informatycznych. Nie pozwala to na realną ocenę zagrożeń, jakie stwarza mariaż kryptoanarchizmu i terroryzmu. Niebezpieczeństwa z tym związane są sygnalizowane ogólnikowo, brakuje pogłębionych analiz (zazwyczaj poprzestaje się na stwierdzeniu popartym przykładami, że w działalności terrorystycznej Internet jest wykorzystywany do szerzenia propagandy, prowadzenia rekrutacji i zdobywania środków finansowych, bez choćby pobieżnego omówienia używanych narzędzi informatycznych)[3].

Autorzy niniejszego artykułu postawili następujące pytania badawcze:

- Jakimi zasobami koncepcyjnymi i technologicznymi mogą dysponować radykalni zwolennicy prywatności w Internecie oraz cyberprzestępcy?

---

[1] D.E. Denning, W.E. Baugh, *Encryption and evolving technologies: Tools of organized crime and terrorism*, Washington 1997, s. 1–64.

[2] United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes*, New York 2012; N. Malik, *Terror in the Dark. How terrorists use encryption, the darknet, and cryptocurrencies*, Millbank 2018; B. Clifford, H. Powell, *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram*, Washington 2019; C. Dion-Schwarz, D. Manheim, P.B. Johnston, *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats*, Santa Monica 2019.

[3] United Nations Office on Drugs and Crime, *The use of the Internet*…, s. 3.

- Jak można skategoryzować środki chroniące prywatność – jakie obszary komunikacji oraz działań w Internecie one obejmują?
- Jaki jest potencjał technologii wspierających prywatność w sytuacjach zastosowania ich do działań niezgodnych z prawem?
- Jaki jest zakres ochrony prawnej użytkowników technologii wspierających prywatność?
- Czy na podstawie analizy wybranych rozwiązań można stworzyć zestaw modelowych charakterystyk technologii wspierających prywatność?

Sformułowane pytania prowadzą do postawienia następującej tezy: Internet, dzięki któremu pojawiły się nowe sposoby komunikowania się, dał jednostkom – zwykłym obywatelom – ogromne, niespotykane wcześniej możliwości wywierania politycznego wpływu. To doprowadziło do powstania asymetrii pod tym względem między władzą a użytkownikiem technologii wspierających prywatność. Wspomniane możliwości stały się podstawą do sformułowania przez Andrew L. Shapiro wniosku o pojawieniu się „rewolucji kontroli" (*control revolution*[4]) – zjawiska rozproszenia władzy i przekazywania jej od elit do „końcowych użytkowników", czyli obywateli. Jej źródłem jest potencjał komunikacyjny Internetu[5]. W związku z postawioną tezą oraz pytaniami badawczymi autorzy artykułu sformułowali cztery hipotezy cząstkowe:

1. Technologie chroniące prywatność obejmują najważniejsze obszary związane z wymianą oraz przechowywaniem informacji i wartości: komunikację internetową, przechowywanie informacji oraz wymianę handlową.
2. Technologie chroniące prywatność stwarzają zabezpieczenia, które są trudne lub niemożliwe do złamania, zarówno przez przestępców, jak i służby dyspozycyjne.
3. Prawo jest instrumentalnie wykorzystywane do zwiększania ochrony informatycznej narzędzi wspierających prywatność.
4. Zestaw modelowych cech technologii wspierających prywatność nie powinien ograniczać się wyłącznie do cech o charakterze technicznym, lecz obejmować także walory ergonomiczne (łatwość instalacji i używania), społeczne (dostateczne wsparcie oraz promocja i popularyzacja produktu informatycznego), konstrukcyjno-organizacyjne (decentralizacja lub co najmniej federalizacja) i własnościowe (otwartoźródłowość).

[4] Prawie wszystkie słowa i zwroty obcojęzyczne użyte w artykule pochodzą z języka angielskiego, dlatego Redakcja nie podaje tej informacji za każdym razem. Informacja pojawia się jedynie w przypadku wyrazów obcych pochodzących z języka innego niż angielski (przyp. red.).

[5] A.L. Shapiro, *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York 1999, s. 13.

Ideologiczno-doktrynalne fundamenty technologii chroniących prywatność

Ochrona prywatności nabrała nowego charakteru w latach 80. XX w. wskutek rozwoju technologii informatycznych. Uformował się wówczas ruch społeczny, którego doktrynalnym podłożem było przekonanie o wadliwej ochronie prawa do prywatności przez instytucje państwowe. Twierdzono, że sprzeniewierzyły się one potrzebie dbania o tę wartość i stanowią pod tym względem największe zagrożenie obywatela. To wówczas pojawiło się określenie *Privacy Enhancing Technologies* (dalej: PET), oznaczające ogół rozwiązań technicznych zapewniających użytkownikom pełną prywatność i wyłączną kontrolę nad danymi, które tworzą i przesyłają. Na przełomie lat 80. i 90. XX w. uformowała się grupa Cypherpunks (nazwa powstała *ad hoc*, w wyniku sytuacyjnego żartu), organizująca comiesięczne spotkania poświęcone prywatności oraz kontroli informacji prowadzonej przez rząd i korporacje. Impulsem do powstania tej grupy stał się artykuł Davida Chauma *Security without Identification: Transaction Systems to Make Big Brother Obsolete*[6] opublikowany w połowie lat 80. Nieco później pojawiła się nazwa ruchu – kryptoanarchizm. Wprowadził ją w 1992 r. Timothy C. May, amerykański pisarz, inżynier elektronik, dawny pracownik firmy Intel[7]. Jest on autorem innych publikacji ważnych dla środowiska kryptoanarchistycznego, m.in. *Cyphernomicon*[8] oraz *True Nyms and Crypto Anarchy*[9]. May jest również autorem najbardziej radykalnej koncepcji kryptoanarchizmu – tzw. rynku zabójców (*assassination market*), która pokazuje stopień determinacji w dążeniu do drastycznego ograniczenia informacyjnych apetytów państw[10]. Istotne znaczenie dla rozwoju ruchu miał treściwy manifest Chucka Hammilla *Od kuszy do kryptografii, czyli psucie państwu szyków przy pomocy techniki*[11] (tytuł oryginału: *From Crossbows to Cryptography. Thwarting the State via Technology*), w którym autor argumentował, że nieskrępowane dzielenie się informacją jest silniejszym sposobem oddziaływania na władze państwowe niż przemoc. Ważnym wkładem wydaje się również praca zbiorowa zatytułowana *Crypto Anarchy, Cyberstates, and Pirate Utopias*[12]. Obecnie ruch kryptoanarchistyczny stał się mniej radykalny, jednocześnie poddał się częściowej instytucjonalizacji.

---

[6] D. Chaum, *Security without Identification. Transaction Systems to Make Big Brother Obsolete*, „Communications of the ACM" 1985, nr 10, s. 1030–1044.

[7] T.C. May, *The Crypto Anarchist Manifesto*, Activism.net, 22 X 1992 r., https://www.activism.net/cypherpunk/crypto-anarchy.html [dostęp: 20 XII 2018].

[8] T.C. May, *Cyphernomicon. Cypherpunks FAQ and More, Version 0.666*, 10 IX 1994 r., http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html [dostęp: 20 XII 2018].

[9] T.C. May, *True Nyms and Crypto Anarchy*, grudzień 2001 r., http://www.isfdb.org/cgi-bin/title.cgi?195636 [dostęp: 20 XII 2018].

[10] T.C. May, *Cyphernomicon*…

[11] Ch. Hammill, *Od kuszy do kryptografii, czyli psucie państwu szyków przy pomocy techniki*, tłum. J. Sierpiński, „Kultura i Historia" 2007, nr 11, bez paginacji, http://www.kulturaihistoria.umcs.lublin.pl,/archives/701 [dostęp: 20 XII 2018].

[12] *Crypto Anarchy, Cyberstates, and Pirate Utopias*, P. Ludlow (red.), Cambridge 2001.

Warto wskazać następującą triadę: Electronic Frontier Foundation (https://www.eff.org/) powstałą w latach 90. XX w., Free Software Foundation (https://www.fsf.org/), założoną w 1985 r. przez Richarda Stallmana, amerykańskiego informatyka i hakera, legendę ruchu wolnego oprogramowania, oraz CryptoRights Foundation. Wszystkie wymienione organizacje to amerykańskie organizacje pozarządowe, które w istotny sposób, zarówno pod względem technicznym, jak i społecznym, przyczyniły się do zwiększenia bezpieczeństwa informacyjnego indywidualnych użytkowników.

Liczny i silny ruch na rzecz prywatności stworzył – co można dostrzec z perspektywy czasu – treści mało obszerne, o niezbyt wysokim poziomie merytorycznym i nieznane szerszej grupie odbiorców. Jest to cecha charakterystyczna technologii wspierających prywatność – ich zaplecze ideologiczne jest ubogie w treści oraz niewyszukane merytorycznie. Nie stanowi to jednak o jego wartości, gdyż w jego ramach powstały i powstają liczne „technologie wolności" przeznaczone do praktycznego aplikowania. Tematyka dotycząca technologii wspierających prywatność stała się przedmiotem obszernych publikacji o charakterze syntetycznym[13].

Za cezurę w sferze ochrony prywatności jednostki należy uznać rok 1976. Wówczas dwaj niezależni amerykańscy matematycy – Whitfield Diffie i Martin E. Hellman – stworzyli rewolucyjny system szyfrowania danych[14], którego złamanie zajęłoby setki lat nawet agencjom rządowym dysponującym nieograniczonymi środkami[15]. Opisali go w publikacji zatytułowanej *New Directions in Cryptography*, co wywołało liczne reperkusje, w tym prawne. Znaczenie opracowanej przez nich metody szyfrowania asymetrycznego (klucz publiczny, klucz prywatny)[16] najtrafniej ujął niezależny dziennikarz i specjalista z zakresu cyberbezpieczeństwa Jacob Applebaum, współautor (m.in. z Julianem Assangem) książki *Cypherpunks. Freedom and the Future of the Internet*. Napisał on: *Silna kryptografia może opierać się nieograniczonemu stosowaniu przemocy. Żadna siła przymusu nigdy nie rozwiąże problemu matematycznego* (w oryginale: *Strong cryptography can resist an unlimited application of violence. No amount of coercive force will*

[13] Zob. *Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents*, G.W. van Blarkom, J.J. Borking, J.G.E. Olk (red. nauk.), Haga 2003; *Privacy-enhancing technologies. The path to anonimity*, R. Hes, J.J. Borking (red. nauk.), Haga 2000 r.; Yang Wang, A. Kobsa, *Privacy-Enhancing Technologies*, w: *Handbook of Research on Social and Organizational Liabilities in Information Security*, M. Gupta, R. Sharman (red. nauk.), New York 2009; *Protecting privacy in practice. The current use, development and limits of Privacy Enhancing Technologies in data analysis*, A. Noble (red. nauk.), The Royal Society, marzec 2019 r., https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy-enhancing-technologies-report.pdf [dostęp: 5 VIII 2020].

[14] Ch. Makdad, *"God Rewards Fools" – Whitfield Diffie and Martin Hellman's Stand to Revolutionize Cryptography*, The Eagle Eye News, https://tyroneeagleeyenews.com/wpcontent/uploads/2017/05/Makdad_Senior_TyroneAreaHighSchool_PA.pdf [dostęp: 1 VIII 2020].

[15] W. Diffie, M.E. Hellman, *New Directions in Cryptography*, „IEEE Transactions on Information Theory" 1976, nr 6, s. 644–654.

[16] W. Gogłoza, *Cypherpunks, WikiLeaks i widmo kryptograficznej anarchii*, https://wgogloza.com/umcs/informatyka-prawnicza/cypherpunks/ [dostęp: 20 XII 2018].

ever solve a math problem)[17]. A zatem siłą gwarantującą ochronę jednostki w zakresie prywatności nie mają być prawo i instytucje powołane na jego podstawie, lecz bezstronne prawa kryptografii, niepodatne na manipulację czy naciski.

Uregulowania prawne dotyczące ochrony prywatności

Technologie zwiększające czy też chroniące prywatność to złożony fenomen – prawny, socjologiczny i informatyczny jednocześnie. Jako fundament nowożytnej dyskusji na temat prywatności w kategoriach prawnych wskazuje się publikację amerykańskich prawników Samuela D. Warrena oraz Louisa D. Brandeisa zatytułowaną *The Right to Privacy*[18]. Autorzy zwrócili w niej uwagę na sferę życia wymagającą uregulowania z uwagi na okoliczności zaistniałe wskutek rozwoju społecznego. Obecnie prawo do prywatności lokuje się pośród praw człowieka pierwszej generacji i jest ono przedmiotem powszechnych i licznych uregulowań na poziomie prawodawstwa międzynarodowego oraz prawodawstw krajowych. Pośrednio sformułowano je w: art. 12 *Powszechnej deklaracji praw człowieka* z 10 grudnia 1948 r.[19], art. 17 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych* z 16 grudnia 1966 r.[20], art. 8 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności* z 4 listopada 1950 r.[21] oraz w art. 7 i 8 *Karty Praw Podstawowych Unii Europejskiej* z 7 grudnia 2000 r.[22] Wymienione akty określają jako bezprawną każdą arbitralną ingerencję w – co najistotniejsze z punktu widzenia niniejszej analizy – korespondencję i (lub) komunikację oraz formułują instytucjonalne prawo do ochrony prawnej przeciwko zamachowi na wskazane dobro.

Ochronę prywatności w prawie europejskim gwarantuje rozporządzenie Parlamentu Europejskiego i Rady UE z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych[23]. W art. 5 ust. 1 wskazanego rozporządzenia zostały sformułowane zasady dotyczące przetwarzania danych osobowych.

---

[17] J. Assange i in., *Cypherpunks. Freedom and the Future of the Internet*, New York–London 2012, s. 5.

[18] S.D. Warren, L.D. Brandeis, *The Right to Privacy*, „Harvard Law Review" 1890, nr 5, s. 193–220.

[19] *Powszechna Deklaracja Praw Człowieka (Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana 10 grudnia 1948 r.)*.

[20] *Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r.* (DzU z 1977 r. nr 38 poz. 167).

[21] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2* (DzU z 1993 r. nr 61 poz. 284).

[22] Dz. Urz. UE C 83 z 30 III 2010 r., s. 389.

[23] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)* (Dz. Urz. UE L 119 z 4 V 2016 r., s. 1).

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");
b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu");
c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");
d) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");
e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania");
f) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

To (…) *administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność")*[24]. W art. 6 ust. 1 rozporządzenia wskazano warunki, które muszą być spełnione, aby przetwarzanie było zgodne z prawem. Są one następujące:

a) osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym celu lub większej liczbie określonych celów,
b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy,
c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze,
d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej,
e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub

[24] Tamże, art. 5 ust. 2.

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

W tym kontekście należałoby również zwrócić uwagę na terytorialny zakres stosowania omawianego rozporządzenia. Zgodnie z art. 3:

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:
   a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
   b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.
3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

Jest to istotna zmiana dotycząca poszerzenia zakresu obowiązywania terytorialnego w porównaniu z chociażby poprzednio obowiązującą dyrektywą 95/46/WE, która posługiwała się bardzo ogólnym wyrażeniem „prowadzenie działalności gospodarczej".

Natomiast w Polsce zagadnienia dotyczące ochrony bezpieczeństwa reguluje ustawa o ochronie danych osobowych[25], która czasami odsyła do głównego aktu unijnego w zakresie ochrony danych, jakim jest omawiane wcześniej rozporządzenie Parlamentu i Rady UE. Ochronę wolności i tajemnicy komunikowania się gwarantuje art. 49 oraz – częściowo – art. 51 Konstytucji Rzeczpospolitej Polskiej[26], a także prawo karne (art. 267 *Kodeksu karnego*[27]), cywilne (art. 23 *Kodeksu cywilnego*[28]) oraz prawo autorskie (art. 82

[25] *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (t.j.: DzU z 2019 r. poz. 1781).

[26] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r*. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

[27] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

[28] *Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny* (t.j.: DzU z 2019 r. poz. 1145, ze zm.).

i 83 ustawy o prawie autorskim i prawach pokrewnych[29]). Jednak te prawa mogą być i faktycznie są ograniczane w sytuacji konfliktu z innymi wartościami, zwłaszcza bezpieczeństwem osobistym oraz szeroko pojętym bezpieczeństwem państwa. Ograniczenia, o których mowa, są sformułowane w wymienionych aktach (m.in. w art. 31 Konstytucji RP czy w art. 8 wspomnianej konwencji o ochronie praw człowieka i podstawowych wolności)[30]. Pomiędzy prawem do prywatności a bezpieczeństwem istnieje zatem nieusuwalny antagonizm.

Typologia technologii chroniących prywatność

Wartościowej, chociaż fragmentarycznej wiedzy na temat technologii chroniących prywatność dostarczają materiały publicystyczne i studia przypadków. Analiza literatury przedmiotu pokazuje, że terroryści wykorzystują w praktyce trzy grupy technologii wspierających prywatność.

Pierwsza z nich to oprogramowanie tworzone wyłącznie na potrzeby grup terrorystycznych, a konkretnie – najsilniejszej i najliczniejszej takiej grupy, tj. islamskich terrorystów. Opracowali oni własne narzędzia informatyczne. Przykładem jest Mojehedeen Secrets istniejący od 2007 r., przygotowany jako alternatywa dla Pretty Good Privacy i służący do szyfrowania korespondencji przesyłanej z użyciem poczty elektronicznej za pomocą popularnego algorytmu RSA[31] . Z kolei Tashfeer al-Jawwal, program powstały w 2013 r., umożliwia szyfrowanie urządzeń mobilnych. Jest to produkt Global Islamic Media Front, organizacji związanej z Al-Kaidą oraz innymi grupami terrorystycznymi. Ważnym, dynamicznie rozwijanym programem jest Amn al-Mujahed (opracowany w 2013 r.). Ma on zastosowanie uniwersalne – służy do szyfrowania poczty elektronicznej, wiadomości SMS oraz czatów.

Do drugiej grupy należą rozwiązania, które bazują na istniejących technologiach komunikacyjnych na zasadzie najprostszego, a jednocześnie możliwie najbardziej skutecznego użycia. Można je określić potocznym, używanym w socjolekcie internautów wyrażeniem *life hack*, oznaczającym niewyrafinowany, ale błyskotliwy sposób na coś. Korzystanie z nich wymaga znajomości technik inwigilacyjnych oraz infiltracyjnych stosowanych przez służby dyspozycyjne, przed którymi fakt komunikacji lub jej treść mają pozostać ukryte. Za przykład może posłużyć technika *dead dropping*, znana już od co najmniej trzech dekad. Polega ona na stworzeniu na koncie poczty elektronicznej wiadomości roboczej i niewysyłaniu jej, lecz

[29] *Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych* (t.j.: DzU z 2019 r. poz. 1231).

[30] M. Pryciak, *Prawo do prywatności*, „Wrocławskie Studia Erazmiańskie" 2010, nr 4, s. 211–229.

[31] Algorytm Rivesta-Shamira-Adlemana – jeden z pierwszych i obecnie najpopularniejszych asymetrycznych algorytmów kryptograficznych z kluczem publicznym, zaprojektowany w 1977 r. przez Rona Rivesta, Adiego Shamira oraz Leonarda Adlemana. Bezpieczeństwo szyfrowania opiera się na trudności faktoryzacji dużych liczb złożonych. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

podaniu odbiorcy danych logowania do danego konta poczty. Pozwala to na uniknięcie analizy i trasowania[32] takiej wiadomości, co jest czynione na przykład przez oprogramowanie inwigilacyjne Stanów Zjednoczonych należące do grupy PRISM[33]. W toku śledztwa dotyczącego zamachów w Paryżu w listopadzie 2015 r., podczas których zginęło 137 osób (w tym siedmiu sprawców), a ponad 300 zostało rannych, przypuszczano, że terroryści do komunikacji w celu zaplanowania zamachów użyli konsoli PlayStation 4. Istnieje kilka możliwości wysyłania trudnych do monitorowania wiadomości za pośrednictwem usługi gier online PlayStation Network (PSN) oraz prowadzenia rozmów głosowych lub komunikowania się za pomocą określonej gry. Dokumenty ujawnione przez Edwarda Snowdena w 2013 r. dowodzą, że Agencja Bezpieczeństwa Narodowego (dalej: NSA) i Centralna Agencja Wywiadowcza Stanów Zjednoczonych monitorowały takie gry, jak World of Warcraft, aby infiltrować komunikację islamskich terrorystów[34]. Konsola PlayStation 4 jest systemem prostym, ale trudnym do kontrolowania, trudniejszym do inwigilacji przez służby dyspozycyjne niż względnie bezpieczny komunikator WhatsApp. Innym przykładem może być używanie w latach 90. XX w. przez grupy pedofilów globalnego systemu grup dyskusyjnych Usenet[35]. Ich członkowie wymieniali się na forach dyskusyjnych zakazanymi treściami. Usenet był już wówczas starą technologią komunikacyjną, powstał bowiem w 1976 r. Postrzegany (błędnie) jako technologia schyłkowa, nie był w kręgu zainteresowania służb dyspozycyjnych. Technika wymiany zakazanych treści była banalnie prosta – plik graficzny lub filmowy zamieniano na tekst i w takiej postaci wklejano na forum. Wystarczyło skopiować wklejony blok tekstu i zastosować właściwe rozszerzenie pliku (np. jpg lub mpg), by uzyskać ukryte treści i odtworzyć je na komputerze lokalnym.

Trzecią grupę stanowi oprogramowanie powstałe w ramach szeroko rozumianego ruchu kryptoanarchistycznego. Jest ono powszechnie używane przez entuzjastów prywatności, dysydentów, ekstremistów, przestępców i cyberprzestępców oraz

---

[32] Trasowanie – wyznaczanie trasy i wysłanie nią pakietu danych w sieci komputerowej. Trasowanie ma na celu dostarczenie danych w sposób najbardziej optymalny. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

[33] D. Greene, *NSA Mass Surveillance Programs. Unnecessary and Disproportionate*, Electronic Frontier Foundation, 2014 r., https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf [dostęp: 1 VIII 2020].

[34] J. Austin, *'Traitor' Edward Snowden 'taught ISIS Paris terrorists how to avoid detection'*, „Express", 18 XI 2015 r., https://www.express.co.uk/news/world/620270/Traitor-Edward-Snowden-taught-ISIS-Paris-terrorists-avoid-detection-NSA-CIA-John-Brennan [dostęp: 2 VIII 2020]; J. Titcomb, *Did Paris terrorists really use PlayStation 4 to plan attacks?*, „The Telegraph", 16 XI 2015 r., https://www.telegraph.co.uk/technology/video-games/playstation/11997952/paris-attacks-playstation-4.html [dostęp: 1 VIII 2020]; S. Harris, *CIA's Ex-No. 2 Says ISIS 'Learned From Snowden'*, „Daily Beast", 12 VII 2017 r., https://www.thedailybeast.com/cias-ex-no-2-says-isis-learned-from-snowden [dostęp: 2 VIII 2020].

[35] E. Quayle, M. Taylor, *Paedophiles, Pornography and the Internet: Assessment Issues*, „British Journal of Social Work" 2002, nr 7, s. 863–875.

terrorystów – słowem wszystkich tych, którzy z różnych powodów pragną chronić zgromadzone dane oraz prowadzoną komunikację. Jest to zbiór narzędzi zróżnicowanych, jednak można z niego wyodrębnić oprogramowanie najpowszechniej używane i najbardziej przydatne wymienionym grupom (wydaje się, że jest to pośredni wskaźnik skuteczności takich narzędzi).

Na potrzeby artykułu oraz uniwersalnego systematyzowania narzędzi informatycznych wspierających prywatność zostaną wyróżnione trzy typy oprogramowania. Jednocześnie należy wskazać, że w literaturze przedmiotu istnieje kilka konkurencyjnych, ale niedoskonałych (co najmniej z punktu widzenia niniejszego artykułu) taksonomii technologii wspierających prywatność[36]. Na ogół wyróżnia się w nich dwa typy takich technologii – w wersji *soft* jest dopuszczane użycie jako pośrednika anonimizującego tzw. zaufanej trzeciej strony (*trusted third party*, TTP), natomiast w wersji *hard* usługa komunikacyjna musi być zdecentralizowana. Jak łatwo przewidzieć, terroryści koncentrują się na technologiach drugiego rodzaju ze względu na ich znacznie większe bezpieczeństwo.

Za podstawę wyodrębnienia trzech typów technologii wspierających prywatność przyjęto funkcję, jaką pełnią[37]. Pierwszy, podstawowy typ to technologie zapewniające anonimową lub pseudonimową komunikację (pozyskiwanie, przesyłanie, propagowanie informacji). Jako przykłady posłużyły: sieć anonimizująca The Onion Router (dalej: Tor)[38], sieć Freenet oraz dwa systemy operacyjne zaprojektowane do bezpiecznej i anonimowej komunikacji – Linux Tails oraz Whonix. Drugi typ to technologie wykorzystywane do anonimowej wymiany handlowej (zwykle wspomaganej siecią Tor), trudnej lub niemożliwej do skontrolowania. Przeanalizowano wykorzystanie takich systemów anonimowych kryptowalut, jak Monero, Zcash i Dash (tzw. *private coins*). Trzeci z typów technologii wspierających prywatność to bezpieczne przechowywanie informacji z użyciem zaawansowanych rozwiązań kryptograficznych. Za egzemplifikację posłużył program szyfrujący VeraCrypt.

Wyżej wymienione programy należą do rodziny tzw. wolnego oprogramowania (*free software*). Wolność oprogramowania niesie ze sobą istotne konsekwencje dla jakości świadczonych usług w zakresie prywatności. Warto zatem przyjrzeć się koncepcji wolności oprogramowania, jaka ukształtowała się przez ponad dwie dekady jej istnienia. Wolne oprogramowanie włącza cztery następujące uprawnienia, nazywane „wolnościami": wolność 0 – do wykorzystania programu w dowolnym celu (w tym komercyjnym), wolność 1 – do analizy kodu źródłowego, wolność 2 –

---

[36] Yun Shen, S. Pearson, *Privacy Enhancing Technologies: A Review*, HP Laboratories, sierpień 2011 r., https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf [dostęp: 1 VIII 2020]; G. Danezis, S. Gürses, *A critical review of 10 years of Privacy Technology*, Proceedings of Surveillance Cultures: A Global Surveillance Society, kwiecień 2010 r., https://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf [dostęp: 1 VIII 2020].

[37] Por. J. Heurix i in., *A taxonomy for privacy enhancing technologies*, „Computers & Security" 2015, t. 53, s. 1–17.

[38] Tor Project, https://www.torproject.org/ [dostęp: 1 VIII 2020].

do rozpowszechniania kopii (dowolnymi kanałami i w dowolnych ilościach), wolność 3 – do rozwijania oprogramowania (wolność 1 stanowi warunek niezbędny tej wolności). Anglojęzyczne określenie *free* odnosi się do wolności (*freedom*), nie zaś do darmowości (*for free*). Należy zatem rozumieć, że jest to oprogramowanie bez restrykcji lub z niewielką ich liczbą; jest więc zarówno „libre" (z hiszp. wolny, niezależny – przyp. red.), jak i „gratis". W praktyce oznacza to jednak także darmowość. Pojęcia *free software* nie należy mylić z pojęciem program otwartoźródłowy (*open source software*). O ile pierwsze z nich odnosi się do zagadnień ideologicznych, o tyle drugie – do technicznych. Jest ono pojęciem uproszczonym, zostało zawężone do konkretnego, materialnego pożytku, bez dyskusji o kwestiach światopoglądowych i etycznych. Otwartość kodu źródłowego oprogramowania oznacza, że jest ono dostępne dla analizy, a to ogranicza możliwość wprowadzenia do funkcji programu tzw. tylnych drzwi (*backdoors*) lub złotych kluczy (*golden keys*), czyli rozwiązań umożliwiających ominięcie zabezpieczających funkcji programu. Toczy się dyskusja dotycząca zasadności wprowadzania takich rozwiązań, pojawił się w niej nawet postulat konieczności ich wdrażania ze względu na potencjalne możliwości użycia takiego oprogramowania w działalności terrorystycznej[39].

Analiza wybranych narzędzi chroniących prywatność

Poniżej przeanalizowano narzędzia wspierające prywatność pod kątem ich przydatności do działalności komunikacyjnej, handlowej oraz magazynowania informacji przez ugrupowania terrorystyczne i cyberprzestępcze. Podano również uzasadnienia dotyczące wyboru poszczególnych narzędzi. Wybór najczęściej był podyktowany obserwowanym zainteresowaniem środowisk terrorystycznych i ekstremistów politycznych określonymi narzędziami informatycznymi[40].

Anonimowa komunikacja w Internecie

Niekwestionowanym liderem rozwiązań stosowanych w technologiach wspierających prywatność w zakresie komunikacji i dostępu do informacji jest wspomniana już sieć Tor. W literaturze przedmiotu jej wykorzystanie (zarówno faktyczne, jak i na poziomie hipotez i spekulacji) przez terrorystów oraz szerzej – w celach przestępczych –

[39] J.A. Lewis, D.E. Zheng, W.A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data*, Lanham–Boulder–New York–London 2017, s. 3.

[40] Zainteresowani systematycznym przeglądem narzędzi wspierających prywatność mogą skorzystać z witryny Privacy Tools, https://www.privacytools.io/ [dostęp: 1 VIII 2020]. Znajdują się tam systematyczny przegląd i ewaluacja produktów informatycznych wspierających prywatność w następujących kategoriach: dostawcy, przeglądarki, oprogramowanie, usługi, systemy operacyjne.

ma swoją długą i bogatą historię[41]. Związki sieci Tor z terroryzmem[42], pedofilią[43] i cyberprzestępczością[44] są w literaturze przedmiotu uznawane za oczywiste. Dlatego autorzy niniejszego artykułu skoncentrowali się na zagadnieniu dotyczącym możliwości i zakresu anonimizacji użytkownika tej sieci.

Projekt sieci anonimizującej Tor ujawniono i udostępniono jego kod źródłowy do użytku cywilnego we wrześniu 2003 r. Pierwotnie był to projekt militarny – pracowało nad nim Laboratorium Badawcze Marynarki Wojennej Stanów Zjednoczonych (United States Naval Research Laboratory). Aktualnie Tor działa na licencji BSD, jest zarządzany przez Fundację Tor Project, a kod źródłowy ma charakter otwarty, co daje częściową gwarancję transparentności projektu w postaci braku tzw. tylnych drzwi. Tor stwarza możliwość ukrycia tożsamości (geolokalizacji) konsumenta treści (tj. zwykłego użytkownika) oraz dostarczyciela treści. Umożliwia to w dwóch wymiarach: korzystania z Internetu powierzchniowego (tzw. *clearnetu*) oraz korzystania z domeny specjalnej sieci Tor – .onion. Komunikacja w sieci zachodzi z użyciem niezależnych i wielowarstwowo szyfrowanych pakietów (stąd określenie „trasowanie cebulowe" oraz nazwa projektu i domeny, w której on działa, „sieć cebulowa"). Szyfrowanie odbywa się z użyciem protokołu Diffiego-Hellmana. Połączenia z Internetem powierzchniowym odbywają się za pomocą obwodu (*circuit*) złożonego z trzech węzłów pośredniczących (kolejno: węzeł wejściowy, tj. *entry guard,* węzeł pośredniczący, tj. *middle relay*, oraz węzeł wyjściowy, tj. *exit relay*). Z kolei w usłudze ukrytej połączenie następuje za pośrednictwem sześciu węzłów (trzech dla konsumenta treści i trzech dla dostarczyciela treści). W tym przypadku kontakt z usługą ukrytą różni się od kontaktu z usługą realizowaną w Internecie powierzchniowym tym, że to usługa ukryta inicjuje połączenie (za pomocą tzw. punktu spotkania – *rendezvous point*). Ponadto usługi nigdy nie są dostępne bezpośrednio, tylko przy użyciu swoistych „skrzynek kontaktowych", które określa się mianem węzłów katalogowych. Aktualnie istnieje ponad 1400 węzłów oznaczonych flagą HSDir (*hidden service directory*), które wspólnie i na zasadzie konsensusu ogłaszanego w krótkich interwałach czasowych tworzą rozproszoną tablicę skrótów

[41] G. Weimann, *Terror on the Internet: The New Arena, The New Challenges*, Washington 2006; G. Weimann, *Terrorism in Cyberspace: The Next Generation,* New York 2015; B. Berton, *The dark side of the web: ISIL's one-stop shop?*, raport European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 1 VIII 2020]; N. Malik, *Terror in the Dark*, raport Henry Jackson Society, Londyn 2015 r., http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf [dostęp: 1 VIII 2020]; G. Weimann, *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict & Terrorism" 2016, nr 3, s. 195–206.

[42] N. Malik, *Terror in the Dark. How terrorists use encryption, the darknet, and cryptocurrencies*, Millbank 2018; G. Weimann, *Terrorist Migration to the Dark Web*, „Perspectives on Terrorism" 2016, nr 3, s. 40–44.

[43] K.V. Acar, *Child abuse materials as digital goods: Why we should fear new commercial forms*, „Economics Discussion Papers" 2017, nr 15, bez paginacji.

[44] D. Mider, *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 154–190.

(*distributed hash table*, DHT). To oznacza, że nigdy żadna strona kontaktu nie może poznać swojej lokalizacji.

Stan sieci Tor jest monitorowany, a wyniki obserwacji są publikowane. Monitoring jest zapewniany przez dziewięć zaufanych serwerów (od 2019 r.), znanych jako węzły katalogowe. Każdy z nich jest kontrolowany przez inną organizację. Taka budowa sieci Tor częściowo eliminuje problem zaufanej trzeciej strony (jest ich wiele, zatem podwyższa to koszty ewentualnego naruszenia anonimowości użytkownika).

Sieć Tor cieszy się globalnie rosnącą popularnością – według Tor Metrics korzysta z niej ponad 2 mln użytkowników dziennie, ma ona ponad 6 tys. węzłów, a ruch przekracza 200 Gbit/s[45]. Jej użytkownicy znajdują się głównie w Stanach Zjednoczonych, Rosji, Niemczech, Francji, Wielkiej Brytanii, Holandii i Indonezji. W tym kontekście należy zwrócić uwagę na pewien paradoks techniczny. Otóż warunkiem anonimowości w sieci Tor jest korzystanie z niej przez wiele osób, czego nie uwzględniono przy jej projektowaniu.

Najważniejszą cechą charakterystyczną jest ograniczona anonimizacja typów połączeń w sieci Tor – szyfrowane, a przez to anonimowe, są połączenia ze stronami www, polecenia powłoki systemowej (*shell*) oraz komunikatory internetowe (*instant messaging*). To oznacza, że anonimizacja następuje wyłącznie przy przeglądaniu stron internetowych, wydawaniu zdalnych rozkazów w linii poleceń oraz komunikowaniu za pomocą czatów. Z Tor należy korzystać z użyciem wtyczki HTTPS Everywhere wbudowanej w przeglądarkę, wymuszającej szyfrowanie komunikacji pomiędzy użytkownikiem a stroną internetową. Użytkownik pozostaje wówczas w pełni bezpieczny wobec następujących podmiotów:

- **hakerów** (którzy uzyskali dostęp do sieci domowej użytkownika) – znają lokalizację użytkownika i wiedzą, że używa on sieci Tor, nie wiedzą jednak, z jaką stroną się łączy, nie poznają jego loginu i hasła oraz nie dowiedzą się, jakie dane pobiera;
- **dostawców usług internetowych** (a pośrednio służb) – jw.;
- **służb dyspozycyjnych** (*via clearnet*) – jw.;
- **służb dyspozycyjnych** (*via* węzeł wyjściowy Tor) – jw., jednak nie poznają lokalizacji użytkownika;
- **usługodawców** (dostarczycieli treści, właścicieli serwera, a pośrednio służb) – poznają wszystkie informacje (i tak powinno być), z wyjątkiem lokalizacji użytkownika korzystającego z danych.

Mechanizmy anonimizacyjne mogą zostać usprawnione za pomocą usługi przekaźników mostkowych (*bridges*) oraz transportu wtykowego (*pluggable transport*).

Mosty (ich pełna nazwa to przekaźniki mostkowe) są przekaźnikami (węzłami wejściowymi) sieci Tor, które nie są wymienione w głównym katalogu Tora. Ponieważ nie ma ich pełnej publicznej listy, to nawet jeśli dostawca usług internetowych filtruje połączenia do wszystkich znanych przekaźników sieci Tor, prawdopodobnie nie będzie

[45] Tor Metrics, https://metrics.torproject.org/ [dostęp: 1 VIII 2020].

w stanie zablokować wszystkich mostów. Mają one zatem zastosowanie w sytuacji, gdy węzły wejściowe sieci Tor są blokowane (cenzura). Z przekaźnika mostkowego można korzystać na dwa sposoby: przez włączenie takiej opcji w samej przeglądarce Tor (wybór odbywa się automatycznie) albo przez wybór samodzielnie uzyskanego węzła (informację pozyskuje się po wysłaniu prośby na adres e-mail: bridges@torproject.org, wyłącznie jednak ze skrzynki założonej u jednego z dwóch dostawców: Riseup lub Gmail).

Transport wtykowy wprowadzono w celu obejścia mechanizmu cenzury. Mosty mogą być bowiem blokowane po rozpoznaniu ruchu charakterystycznego dla transmisji sieci Tor. Zwykle służą do tego specjalne urządzenia instalowane u dostawców usług internetowych, które analizują ruch sieciowy i wykrywają tę sieć, a po jej wykryciu blokują przepływ ruchu. Transport wtykowy manipuluje całym ruchem w sieci Tor między klientem a jego pierwszym przeskokiem, tak że nie można go zidentyfikować jako połączenia sieci Tor. Obecnie transport wtykowy jest realizowany za pomocą mechanizmów obfs4 (od *obfuscate*, tj. zaciemniać) oraz meek-azure. Rozwiązanie maksymalizuje bezpieczeństwo użytkownika (dostawca Internetu nie wie, że użytkownik korzysta z sieci Tor), jednak jakość połączenia (transmisja danych) maleje. Działanie tego mechanizmu polega na symulowaniu, jakoby użytkownik korzystający z Tora przeglądał dużą stronę internetową (np. Microsoft). Mechanizm meek-azure jest polecany użytkownikom z Chin, obfs4 zaś – do zastosowań globalnych.

Zdecentralizowana anonimowa sieć dystrybucji informacji – Freenet. Jest to sieć, która nie ma żadnego serwera sterującego ruchem lub przechowującego rejestr adresów, jej zasoby są więc całkowicie rozproszone. Pomysłodawcą i autorem Freenetu jest Ian Clarke. Sieć została napisana w języku Java, jest rozwijana od marca 2000 r. Zapewnia ona prywatność, ale nie anonimowość. Jej działanie jest następujące: komputery połączone w sieć są równorzędne i każdy z nich jest jednocześnie serwerem danych (węzłem komunikacyjnym). Jest to topologia siatki (*full mesh*), a więc bezserwerowa, dzięki temu, że instalując Freenet, każdy użytkownik udostępnia część przestrzeni swojego dysku twardego na potrzeby działania całości sieci. Ta przestrzeń jest ściśle odizolowana od reszty zasobów znajdujących się na komputerze, a użytkownik nie ma możliwości sprawdzenia, co jest zdeponowane, a także przesyłane przez jego komputer. Jest to architektura rozproszonej sieci peer-to-peer (P2P), jednak z tą zasadniczą różnicą, że po wprowadzeniu pliku do sieci użytkownik traci kontrolę nad jego lokalizacją. Dane w losowych interwałach są losowo przenoszone z jednego komputera (węzła sieci) na inny, a ich pobieranie nigdy nie odbywa się bezpośrednio. Adresowanie dokonuje się za pomocą kluczy będących kryptograficznymi funkcjami skrótu, nieodzwierciedlającymi fizycznej lokalizacji zasobu[46].

Warto wspomnieć w tym miejscu o projekcie, który łączy zalety sieci Tor i Freenet, a jednocześnie nie ma ich wad. Jest to Invisible Internet Project (dalej: I2P) powstały

[46] Oficjalna strona projektu Freenet: https://freenetproject.org/author/freenet-project-inc.html [dostęp: 1 VIII 2020]; D. Mider, *Czarny i czerwony*…, s. 158–159.

w 2003 r., jednak do chwili obecnej nie osiągnął on statusu RTM (*release to manufacting*, tj. stabilny i gotowy do wypuszczenia na rynek)[47].

Systemy operacyjne zogniskowane na prywatności pochodzą z rodziny systemów GNU Linux wykorzystujących sieć Tor (najczęściej w wersji ulepszonej, bardziej zaawansowanej i niedostępnej dla zwykłych użytkowników Tora). Należą do nich przede wszystkim Linux Tails[48] oraz Whonix[49]. Nowość w zakresie rozwiązań informatycznych (zarówno pod względem konstrukcji, jak i wykorzystania sieci Tor) stanowi system operacyjny Qubes OS[50], jednak ze względu na wymagania związane z kompetencjami użytkowników (na etapie instalacji, ale przede wszystkim użytkowania) nie jest to rozwiązanie, które szybko się upowszechni. Wśród innych dystrybucji systemu GNU Linux skoncentrowanych na bezpieczeństwie i w znacznym stopniu chroniących prywatność należy wskazać przede wszystkim system Debian, który istnieje od ćwierć wieku i jest uznawany za bezpieczny i stabilny. Skupia on liczną, szybko reagującą społeczność użytkowników, programistów i specjalistów w dziedzinie bezpieczeństwa. Spośród innych systemów warto wymienić Arch, Alpine i Fedorę. Każdy z nich w pewien sposób zapewnia bezpieczeństwo, ale wymaga to wiedzy, umiejętności i wysiłku ze strony użytkownika.

Wspomniane systemy Linux Tails i Whonix oparte na GNU Linux Debian jako kompleksowe rozwiązania zapewniające swoim użytkownikom maksymalną anonimowość i niewykrywalność zajmują niezwykle ważne miejsce.

Linux Tails[51] to system operacyjny polecany wśród cyberprzestępców i terrorystów[52]. Agencja Bezpieczeństwa Narodowego USA jednoznacznie klasyfikuje jego użytkowników jako ekstremistów[53]. Wśród nich znajduje się m.in. Państwo Islamskie (ISIS)[54]. Początki Linux Tails sięgają pierwszej połowy 2009 r. Powstał on jako połączenie systemów Linux Incognito LiveCD (projekt wstrzymany w 2010 r.) i Amnesia, a został opracowany przez zespół anonimowych hakerów finansowanych przez Free Press Foundation, Debian, Mozillę oraz Tor Project. Przy jego tworzeniu inspirowano się również projektami Live Privatix oraz Liberté Linux. Tails to akronim od The Amnesic Incognito Live System, w której to nazwie wskazano najważniejsze cechy produktu.

---

47 Oficjalna strona projektu Invisible Internet Project: http://www.i2p2.de/en/ [dostęp: 1 VIII 2020].

48 Linux Tails, https://tails.boum.org/ [dostęp: 1 VIII 2020].

49 Whonix. Privacy & Anonimity OS, https://www.whonix.org/ [dostęp: 1 VIII 2020].

50 Qubes OS, A Reasonably Secure Operating System, https://www.qubes-os.org/ [dostęp: 1 VIII 2020].

51 Omawiana, aktualna wersja to 4.9. z 13 VII 2020 r.

52 J. Appelbaum i in., *NSA targets the privacy-conscious*, ARD 1 Das Erste, 3 VII 2014 r.

53 H. Arora, *NSA classifies Linux Journal readers, Tor and Tails Linux users as "extremists"*, 4 VII 2014 r., https://static.techspot.com/community/topics/nsa-classifies-linux-journal-readers-tor-and-tails-linux-users-as-extremists.203649/page-3 [dostęp: 1 VIII 2020].

54 B. Goodwin, *Islamic State supporters shun Tails and Tor encryption for Telegram*, „Computer Weekly", 8 I 2017 r., https://www.computerweekly.com/news/450419581/Islamic-State-supporters-shun-Tails-and-Tor encryption-for-Telegram [dostęp: 1 VIII 2020].

„Amnesic" należy rozumieć jako wbudowany mechanizm usuwania informacji, które potencjalnie mogą doprowadzić do identyfikacji użytkownika. Linux Tails w podstawowej konfiguracji nie przechowuje żadnych plików zapisanych lub utworzonych przez użytkownika, a także żadnych jego ustawień, zainstalowanych programów, modyfikowanej konfiguracji, odwiedzonych witryn (w tym w trybie prywatnym), haseł oraz urządzeń i sieci wi-fi. Jest to możliwe dzięki Nautilus Wipe. Standardowe sposoby kasowania plików w rzeczywistości nie usuwają zawartości danego pliku (nawet po opróżnieniu kosza), jedynie czyszczą tablicę alokacji. Natomiast Nautilus Wipe czyści tę część nośnika, w której dane znajdowały się fizycznie. Własne pliki oraz zainstalowane programy (Tails oferuje aktualnie trzy bezpieczne repozytoria) można oczywiście przechowywać, ale wyłącznie wtedy, gdy przy uruchamianiu systemu (tzw. bootowaniu) wprowadzi się hasło administratora (domyślnie Tails jest pozbawiony użytkownika *root*[55] w celu maksymalizacji bezpieczeństwa) oraz stworzy się zaszyfrowany kontener przeznaczony do takiego dodatkowego oprogramowania. Bezpieczeństwo jest zapewniane również przez mechanizm nadpisywania pamięci o dostępie losowym (RAM) przy każdym wyłączaniu Linux Tails. Zapobiega to m.in. tak zwanym atakom zimnego rozruchu (*cold boot attacks*).

„Incognito" w nazwie oznacza z kolei wdrożenie zaawansowanych mechanizmów strzeżenia tożsamości użytkownika. Anonimizacja jest zapewniana dzięki użyciu systemu Tor. Tails co prawda zdradza na zewnątrz, że doszło do użycia sieci Tor, jednak implementuje funkcje, które uniemożliwiają, a co najmniej utrudniają, odróżnienie użytkowników systemu Tails od innych użytkowników. Tor chroni adres IP użytkownika, dodatkowo i opcjonalnie jest zabezpieczony adres fizyczny urządzenia sieciowego (MAC adres karty wi-fi/Ethernet). Warto jednak wiedzieć, że twórcy systemu nie zadbali o eliminowanie odcisku palca tzw. niebezpiecznej przeglądarki (*unsafe browser*). Zidentyfikowanie użytkownika systemu Tails jest jednak możliwe na podstawie pewnych wskaźników inferencyjnych (takich jak np. niegenerowanie z danej maszyny ruchu innego niż Tor; zwykły użytkownik jest źródłem takiego ruchu) – paradoksalnie zatem mechanizmy anonimizacji stają się źródłem częściowej deanonimizacji. Tails nie implementuje podstawowego mechanizmu sieci Tor, jakim jest mechanizm ochrony węzła wejściowego. Działanie chroniące węzeł wejściowy polega na przypisaniu maszynie, na której uruchomiono Tor, na stałe (okres ok. 45 dni ± 15 dni) puli węzłów wejściowych. Ten mechanizm ma chronić sieć Tor globalnie, czyli uniemożliwić lub utrudnić ataki przez analizę ruchu, to jest wyliczanie adresów IP użytkowników sieci przez obserwowane lub kontrolowane węzły wejściowe przechwytujące ruch. Utrudnienie polega również na zwiększaniu kosztów potencjalnie ponoszonych przez węzły ukryte. Z drugiej strony ten właśnie mechanizm staje się ewentualnym czynnikiem deanonimizacji z perspektywy końcowego użytkownika. Funkcja „incognito" to zatem silne i różnorodne mechanizmy szyfrowania komunikacji oraz samego systemu.

[55] *Root* (pol. korzeń) – tradycyjna nazwa uniksowego konta, które ma pełną kontrolę nad systemem operacyjnym. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

„Live" wskazuje na jeden z elementów systemu bezpieczeństwa (system znajduje się w niezmiennej formie i nawet po jednorazowym naruszeniu integralności zostaje przywrócony do stanu pierwotnego), ale również na wygodę użytkowania (można go uruchomić na dowolnej – z kilkoma wyjątkami – maszynie, do której jest dostęp fizyczny oraz BIOS/UEFI nie są zabezpieczone hasłem). System „live" oznacza możliwość uruchamiania w pełni funkcjonalnego systemu operacyjnego bez konieczności instalowania go na dysku twardym. Linux Tails może być uruchamiany zarówno jako „live USB", jak i „live CD", przy czym ze względów bezpieczeństwa jest zalecana ta druga opcja (istnieje znacznie większa możliwość nadpisania urządzenia pamięci masowej, tj. pendrive'a, niż płyty CD zabezpieczonej przed zapisem). Linux Tails może być uruchamiany również na maszynach wirtualnych, jednak Microsoft Windows i MacOS to oprogramowania zastrzeżone i nie można ich uznać za godne zaufania (pozostaje wykorzystanie wirtualizacji w tych systemach wyłącznie w celach testowych lub edukacyjnych).

Rękojmią prywatności oprogramowania Linux Tails jest transparentne finansowanie – we wsparciu partycypują głównie podmioty pozarządowe, a w mniejszym wymiarze – komercyjne. Są to m.in. Mozilla Open Source Support (w 2017 r. ponad 50 tys. dolarów, w 2019 r. ponad 100 tys. dolarów), Handshake (w 2019 r. ponad 100 tys. dolarów), Open Technology Fund (w 2016 r. ponad 50 tys. dolarów), Hivos People Unlimited. Linux Tails powstaje przy stałym wsparciu Tor Project Foundation (nieprzerwanie od momentu powstania, tj. od 2010 r.). Ponadto cały kod oprogramowania jest publiczny, co umożliwia niezależnym badaczom bezpieczeństwa audyt funkcji Tails w dowolnym momencie.

Przy tworzeniu systemu operacyjnego Whonix skoncentrowano się na zaawansowanych funkcjach bezpieczeństwa i anonimowości – jest on w pełni funkcjonalną, wzmocnioną (*hardening*) wersją systemu Debian. Konstrukcja tego systemu jest wyjątkowa. Whonix jest złożony z dwóch maszyn wirtualnych – Whonix-Gateway oraz Whonix-Workstation przeznaczonych do użytku w postaci zwirtualizowanej[56]. Jest to darmowy i otwarty systemem operacyjny, który został stworzony jako narzędzie przeciwko cenzurze. Jednak nie jest to rozwiązanie zapewniające bezpieczeństwo „jednym kliknięciem" – wymaga więcej kompetencji informatycznych, zarówno podczas instalacji, jak i w użytkowaniu, niż Linux Tails. System Whonix ma wbudowane zaawansowane funkcje bezpieczeństwa. Jako jedyny zapewnia ochronę przed wysoce profesjonalnymi atakami deanonimizacyjnymi, zapobiega profilowaniu i deanonimizacji na podstawie wzorców behawioralnych użytkowania klawiatury (*keystroke dynamics*, szeroko ujęta stylometria, odcisk cyfrowy klawiatury lub myszy), zapewnia szczelność, chroniąc

[56] Wirtualizacja polega na utworzeniu symulowanego (wirtualnego) środowiska komputerowego, które stanowi przeciwieństwo środowiska fizycznego; obejmuje wygenerowane komputerowo wersje sprzętu, systemów operacyjnych, urządzeń magazynujących. Whonix jest uruchamiany w pamięci RAM systemu operacyjnego gospodarza (np. Windows, innego systemu Linux) za pośrednictwem programu nazywanego maszyną wirtualną (może to być np. Oracle Virtualbox, VMware, zaleca się jednak Kernel-based Virtual Machine, KVM, działających wyłącznie w systemach GNU Linux).

przed wyciekami DNS[57] i wyciekami strefy czasowej (Dev/TimeSync). Whonix oferuje AppArmor, czyli system obowiązkowej kontroli dostępu, który ogranicza uprawnienia aplikacji zgodnie z zestawem reguł określających, do których plików dany program może uzyskać dostęp. To proaktywne podejście chroni system operacyjny i aplikacje przed zewnętrznymi lub wewnętrznymi zagrożeniami. Whonix ma wbudowany mechanizm wymuszonej anonimowości – cały ruch sieciowy jest zapośredniczany wyłącznie przez sieć Tor. Ponadto zapewnia ochronę przed profilowaniem na złośliwych węzłach wejściowych Tora, a także obsługuje mechanizm izolacji strumieni. System, o którym mowa, mnoży połączenia Tora i ustala dla każdego połączenia odrębnie marszrutę przez sieć Tor, co utrudnia śledzenie aktywności użytkownika. Klasyczny mechanizm Tora nie ma tego rozwiązania. Ciekawym pomysłem jest SecBrowser – bezpieczna, ale nieanonimowa przeglądarka. Warto nadmienić, że Whonix nie ma jeszcze funkcji nadpisywania pamięci RAM podczas zamykania systemu, którą zapewnia Linux Tails. Średnio zaawansowani użytkownicy mogą jednak wdrożyć inne mechanizmy[58].

Anonimowa wymiana handlowa

Kryptowaluty to zagadnienie wielowymiarowe – zarówno pod względem technicznym, jak i politycznym[59], prawnym[60] i ekonomicznym[61]. Aktualnie istnieje ponad 6 tys. kryptowalut o różnych parametrach informatycznych, ekonomicznych i kryptograficznych[62], a łączna kapitalizacja tego rynku sięga obecnie (sierpień 2020 r.) 347 mld dolarów amerykańskich[63]. Ideologiczno-polityczne korzenie kryptowalut silnie tkwią w środowiskach anarchistycznych, hakerskich i hipisowskich[64], same

[57] Domain Name System (pol. system nazw domen) – hierarchiczny rozproszony system nazw sieciowych, który odpowiada na zapytania o nazwy domen. Dzięki DNS nazwa mnemoniczna, np. pl. wikipedia.org, jest tłumaczona na odpowiadający jej adres IP. Za: Wikipedia [dostęp: 18 I 2021] – przyp. red.

[58] Szerzej na ten temat: *Whonix Documentation*, https://www.whonix.org/wiki/Documentation [dostęp: 1 VIII 2020].

[59] B.B. Barbirato, *Bitcoin: A Political Analysis*, maj 2016 r., https://www.researchgate.net/publication/309411431_Bitcoin_A_Political_Analysis [dostęp: 1 VIII 2020].

[60] S. Jafari i in., C*ryptocurrency: A Challenge to Legal System*, Social Science Research Network, styczeń 2018 r., https://www.researchgate.net/publication/325747817_Cryptocurrency_A_Challenge_to_Legal_System [dostęp: 1 VIII 2020].

[61] D. Stancel, *Economic Consequences of Cryptocurrencies and Associated Decentralized Systems*, https://www.researchgate.net/publication/280794376_Economic_Consequences_of_Cryptocurrencies_and_Associated_Decentralized_Systems [dostęp: 1 VIII 2020].

[62] *6,208 crypto currencies*, https://coinlib.io/coins [dostęp: 1 VIII 2020].

[63] Informacja za: TradingView, https://pl.tradingview.com/ [dostęp: 1 VIII 2020]. Podana wartość była dwukrotnie wyższa (i najwyższa w historii) w 2018 r., osiągnęła niemal 700 mld dolarów amerykańskich.

[64] B. Maurer, T.C. Nelms, L. Swartz, *When Perhaps the Real Problem Is Money Itself! The Practical Materiality of Bitcoin,* „Social Semiotics" 2013, nr 2, s. 261–277.

kryptowaluty zaś są postrzegane jako antypolityczne[65]. Liczni zwolennicy, twórcy i użytkownicy kryptowalut hołdują rozmaitym odmianom ideologii anarchistycznej, w tym libertariańskiej[66]. Raporty wykazują, że kryptowaluty są wykorzystywane przez państwa zbójeckie[67], handlarzy narkotyków[68], handlarzy innymi dobrami zakazanymi[69] (w tym do handlu bronią[70]) oraz służą do legalizacji środków finansowych pozyskanych z działalności przestępczej (pranie brudnych pieniędzy)[71]. Jeśli chodzi o finansowanie terroryzmu z użyciem kryptowalut, to zdania są podzielone. Niektórzy autorzy wskazują, że organizacje terrorystyczne chętnie używają tego typu walut, a w literaturze przedmiotu odnajdujemy studia przypadków oraz opracowania o charakterze syntetycznym na ten temat[72]. Z drugiej strony zeszłoroczny raport RAND podważa część tych ustaleń oraz wskazuje bariery sprawiające, że kryptowaluty nie stanowią optymalnego rozwiązania finansowego w działalności terrorystycznej[73]. Z punktu widzenia działalności terrorystycznej czy przestępczej (w tym cyberprzestępczej) środek płatniczy, jakim jest kryptowaluta, winien mieć następujące cechy: anonimowość, płynność, stabilność i łatwość użytkowania. W im mniejszym stopniu

---

65 R. Herian, *The Politics of Blockchain*, „Law and Critique" 2018, nr 2, s. 129–131.

66 I. Eyal, *Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities*, „Computer" 2017, nr 9, s. 38–49; C. Faife, *Live Free or Mine: How Libertarians Fell in Love With Bitcoin*, CoinDesk, 8 X 2016 r., https://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin [dostęp: 1 VIII 2020]; H. Karlstrøm, *Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin*, „Distinktion: Scandinavian Journal of Social Theory" 2014, nr 1, s. 23–36. Zob. także raport z badań dotyczących sympatii ideologicznych użytkowników kryptowalut: P. Ryan, *Left, Right and Center: Crypto Isn't Just for Libertarians Anymore*, CoinDesk, 27 VII 2018 r., https://www.coindesk.com/no-crypto-isnt-just-for-libertarians-anymore [dostęp: 1 VIII 2020].

67 G. Hurlburt, *Shining Light on the Dark Web*, „IEEE Computer" 2017, nr 4, s. 100–105.

68 M.C. Van Hout, T. Bingham, *Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences*, „International Journal of Drug Policy" 2013, nr 5, s. 385–391.

69 A.T. Zulkarnine i in., *Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content*, IEEE Conference on Intelligence and Security Informatics (ISI), Tucson 2016 r., s. 109–114, https://ieeexplore.ieee.org/xpl/conhome/7739307/proceeding [dostęp: 3 VIII 2020].

70 G. Weimann, *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict and Terrorism" 2016, nr 3, s. 195–206.

71 V. Dostov, P. Shust, *Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?*, „Journal of Financial Crime" 2014, nr 3, s. 249–263.

72 S. Higgins, *ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide*, CoinDesk, 7 VII 2014 r., https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist-movements/ [dostęp: 1 VIII 2020]; T. Keatinge, D. Carlisle, F. Keen, *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, 2018 r., http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)604970_EN.pdf [dostęp: 1 VIII 2020]; Y.J. Fanusie, T. Robinson, *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies, and Elliptic, 12 I 2018 r., http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf, s. 7 [dostęp: 1 VIII 2020].

73 C. Dion-Schwarz, D. Manheim, P.B. Johnson, *Terrorist Use of Cryptocurrencies*…

transakcje mogą być śledzone i w im mniejszym stopniu da się je powiązać z tożsamościami użytkowników, tym bardziej taki środek płatniczy jest użyteczny. Jest to zapewniane za pomocą wielu mechanizmów kryptograficznych. Warto podkreślić, że anonimowość danej kryptowaluty nie jest nigdy dana raz na zawsze – jest to nieustanny wyścig miecza i tarczy[74]. Płynność jest rozumiana jako łatwość wymiany na inne kryptowaluty, w tym waluty fiat. To implikuje takie cechy, jak powszechność, wiedza i świadomość użytkowników, zaufanie do środka płatniczego oraz istnienie niezbędnej infrastruktury technicznej (tzw. górnicy zatwierdzający transakcje i tworzący blockchaina, portfele do przechowywania kryptowalut, oficjalne poradniki itp.). Wiąże się to z łatwością użytkowania pod względem oprogramowania (wygodne w użyciu portfele, dostępne zarówno na komputerach, jak i na tabletach lub smartfonach) oraz nieskomplikowaną obsługą. Istotną cechą, aktualnie niespełnialną w odniesieniu do kryptowalut, jest stabilność, ze względu na silne i raczej nieprzewidywalne wahania ich kursów. Zadowalająca jest względna stabilność finansowa, a więc wystarczająco długi czas istnienia i kapitalizacji.

Warto odnotować, że najpopularniejsza kryptowaluta – bitcoin, jakkolwiek używana w celach przestępczych czy terrorystycznych, nie spełnia wszystkich wymienionych warunków. Po pierwsze, bitcoin nie jest anonimowy, lecz pseudonimowy (eliminacja funkcji śledzących odbywa się przez tzw. miksery bitcoinów[75]), po drugie, nie jest on walutą wygodną w transakcjach (koszt transakcji). Zapewnienie anonimowości podczas wymiany z użyciem bitcoinów jest możliwe, jednak wymaga użycia dodatkowych środków (sposoby nabycia, użycie protokołów anonimizujących, np. Tor, I2P).

Dostępne są liczne kryptowaluty wspierające anonimowość użytkownika (*private coins*). Jest to nazwa zbiorcza i należy podkreślić, że ta prywatność bywa rozmaicie wywodzona, rozumiana i implementowana[76]. Pośród systemów *private coins* liczących się w rankingu wymienia się Monero (XMR) – zajmujące 15. miejsce w globalnym rankingu kryptowalut, Dash – 25. miejsce, Zcash – 26. miejsce, a także inne, mniej znaczące, jak: Verge (XVG) – opierający się na sprawdzonych rozwiązaniach anonimizacji (Tor i I2P), Horizen (ZEN) – mający mechanizmy anonimizacji homologiczne jak w systemie Zcash, a także Komodo (KMD), stanowiący tzw. *fork*, czyli rozwidlenie,

---

[74] A. Greenberg, *The dark web's favorite currency is less untraceable than it seems*, „Wired", 27 III 2018 r., https://www.wired.com/story/monero-privacy/ [dostęp: 1 VIII 2020].

[75] T. de Balthasar, J. Hernandez-Castro, *An Analysis of Bitcoin Laundry Services*, Nordic Conference on Secure IT, Tartu 2017 r., https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services [dostęp: 4 VIII 2020].

[76] Pogłębionej analizy motywów oraz sposobów rozumienia prywatności wybranych kryptowalut na podstawie analizy 333 tzw. *whitepapers* (dokument dostarczany przez twórców danej kryptowaluty, obejmujący techniczne, ekonomiczne i społeczno-polityczne założenia i cele projektu) dokonali: J. Harvey, I. Branco-Illodo, *Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in 'Privacy Coin' Whitepapers*, „Journal of Political Marketing" 2020, nr 1–2, s. 107–136.

projektu Zcash[77]. Wymienione systemy kryptowalut znajdują się w orbicie zainteresowań cyberprzestępców i terrorystów, stanowiąc jednocześnie istotną konkurencję dla Bitcoina i Litecoina (LTC)[78]. Poniżej omówiono trzy najważniejsze ekosystemy kryptowalut: Monero, Zcash i Dash.

Monero (XMR) lokuje się na pierwszym miejscu wśród *private coins* przede wszystkim ze względów technicznych oraz stopnia rozpowszechnienia (większość sklepów w domenie specjalnej .onion – darkmarketów – akceptuje tę kryptowalutę podobnie jak bitcoina). Monero istnieje od 2014 r., podczas gdy pozostałe analizowane waluty – od 2016 r. Kapitalizacja rynkowa na sierpień 2020 r. wyniosła ponad 1,5 mld dolarów amerykańskich (1 653 750 000), co daje najwyższy poziom kapitalizacji pośród *private coins*. Wolumen obrotu przekracza 83 mln dolarów, a kurs oscyluje tuż poniżej 100 dolarów[79]. Warto odnotować trzy udokumentowane przypadki wykorzystania kryptowaluty monero w działalności cyberprzestępczej. Pierwszym z nich jest darkmarket AlphaBay (pwoah7foa6au2pul.onion) należący do nieżyjącego już Alexandre'a Cazesa, działający od września 2014 r. do lipca 2017 r., który wdrożył transakcje z użyciem monero w lipcu 2016 r. Federalne Biuro Śledcze przejęło z serwera sklepu 11 993 monero[80] o wartości ok. 0,5 mln dolarów, jednak nie było możliwości całościowego oszacowania kwoty transakcji. Drugim przykładem jest hakerska grupa Shadow Brokers[81], która w czerwcu 2017 r. ogłosiła, że akceptuje płatności w monero obok dotychczas używanej kryptowaluty zcash (notabene: instrukcja odnosząca się do sposobu płatności zawierała błąd, który mógł ujawnić nabywców, a z płatności w monero szybko zrezygnowano)[82]. Trzeci przypadek to operatorzy *ransomware*[83] WannaCry,

---

[77] Według raportu Recorded Future w 2018 r. na wschodnioeuropejskich giełdach obok bitcoina dominował litecoin (35% wolumenu transakcji w porównaniu z bitcoinem), dash (24%) oraz bitcoin cash (BCH) (15%). Obecne były również ethereum (ETH) i zcash (ZEC), monero (XMR) zaś stanowiło zaledwie 3% transakcji. Z kolei w anglojęzycznych darkmarketach dominował bitcoin, a z użyciem monero dokonywano zaledwie 11% transakcji. Zob. A. Barysevich, A. Sola, *Litecoin Emerges as the Next Dominant Dark Web Currency*, Recorded Future, 8 II 2018 r., https://go.recordedfuture.com/hubfs/reports/cta-2018-0208.pdf, s. 5 [dostęp: 1 VIII 2020].

[78] T. Keatinge, D. Carlisle, F. Keen, *Virtual currencies and terrorist financing*…

[79] Por. *Monero (XMR)*, CoinGecko, https://www.coingecko.com/pl/waluty/monero [dostęp: 1 VIII 2020].

[80] Warto zwrócić uwagę na dwa istotne fakty. Po pierwsze, oprócz monero używano w sklepie bitcoinów, etherów oraz zcashów, a wszystkie z nich przejęto z serwerów AlphaBay. Po drugie, z prywatnych portfeli Cazesa FBI przejęła wszystkie kryptowaluty z wyjątkiem monero. Szerzej na ten temat: *United States of America vs. Alexandre Cazes. Verified complaint for forfeiture In Rem*, 2017 r., https://www.justice.gov/opa/press-release/file/982821/download [dostęp: 1 VIII 2020].

[81] Grupa ujawniała zarówno tajemnice Agencji Bezpieczeństwa Narodowego USA, jak i narzędzia informatyczne służące tej agencji do naruszania prywatności użytkowników komputerów i telefonów.

[82] J. Cox, *Cryptocurrency Transactions May Uncover Sales of Shadow Broker Hacking Tools*, „Vice", 28 VI 2018 r., https://www.vice.com/en_us/article/j5k7zp/zcash-shadow-brokers-uncover-hacking-tool-sales [dostęp: 1 VIII 2020].

[83] *Ransomware* (nazwa jest zbitką angielskich słów: *ransom* – okup i *software* – oprogramowanie) – oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt

którzy usiłowali nieudolnie zalegalizować środki z działalności cyberprzestępczej, wymieniając bitcoiny na monero za pośrednictwem szwajcarskiej usługi giełdowej ShapeShift. Organizacja ta rozpoczęła współpracę z organami ścigania USA i w ten sposób udało się uwierzytelnić zaledwie kilkadziesiąt tysięcy dolarów[84]. Monero jest w pełni anonimową kryptowalutą, wykorzystującą następujące funkcjonalne instancje bezpieczeństwa: RingCT zabezpieczające samą transakcję, podpis pierścieniowy (*ring signature*) chroniący nadawcę, ukryty jednorazowy adres odbiorcy (*stealth address*) oraz mechanizm ukrywający adres IP nadawcy (Dandelion++). RingCT (*confidential transaction*) ukrywa kwotę transakcji, tj. umożliwia nadawcy udowodnienie posiadania wystarczającej kwoty bez ujawniania na zewnątrz informacji o wolumenie transakcji. W przypadku większości kryptowalut kwoty transakcji są przesyłane w postaci zwykłego tekstu, widocznego dla każdego obserwatora. Z kolei sygnatura pierścieniowa jest raczej mechanizmem zaciemniania niż całkowitej anonimizacji nadawcy środków. Polega na grupowym dokonywaniu transakcji – łączone są klucze z wielu wyjść i wpisywane do blockchaina, aby utrudnić rozpoznanie prawdziwego nadawcy środków. Natomiast *stealth address* (*one-time address*, *burn-after-reading*) chroni odbiorcę przez utworzenie losowego adresu jednorazowego, tak aby różne płatności dokonane na rzecz tego samego odbiorcy stały się niemożliwe do połączenia. Mechanizm Dandelion++ jest mechanizmem anonimizacji stosunkowo nowym dla systemu Monero, lecz znanym od dawna (pierwotnie zaprojektowany dla systemu Bitcoin, którego społeczność odmówiła przyjęcia tego rozwiązania)[85]. Do Monero wdrożył go w lipcu 2020 r. deweloper Lee Clagett. W uproszczeniu polega on na skierowaniu transakcji do odległego węzła, aby ukryć adres IP nadawcy, co uniemożliwia deanonimizację nawet w sytuacji ataków na dużą skalę[86]. W przyszłości jest planowane wdrożenie mechanizmu Triptych multiplikującego liczebność sygnatur pierścieniowych, co istotnie zwiększy anonimowość transakcji. Warto podkreślić, że w określonych warunkach deanonimizacja użytkowników systemu Monero jest możliwa[87]. Ograniczone, zgodnie w powyższymi

zapisanych w nim danych (często wykorzystując techniki szyfrujące), a następnie żąda okupu od ofiary za przywrócenie stanu pierwotnego. Za: Wikipedia [dostęp: 18 I 2021 r.] – przyp. red.

[84] T. Fox-Brewster, *Wannacry hackers are using this Swiss company to launder $142,000 Bitcoin ransoms*, „Forbes", lipiec 2017 r., https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacryhackers-use-shapeshift-to-launder-bitcoin [dostęp: 1 VIII 2020].

[85] S.B. Venkatakrishan, G. Fanti, P. Viswanath, *Dandelion: Redesigning the Bitcoin Network for Anonymity*, Sigmetrics'17, 5–9 VI 2017 r., Urbana-Champaign, http://publish.illinois.edu/science-of-security-lablet/files/2016/07/Dandelion-Redesigning-BitCoin-Networking-for-Anonymity.pdf [dostęp: 1 VIII 2020]; G. Fanti i in., *Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonimity Guarantees*, „Proceedings of the ACM on Measurement and Analysis of Computing Systems" 2018, nr 2, https://arxiv.org/pdf/1805.11060.pdf [dostęp: 1 VIII 2020].

[86] L. Clagett, *Dandelion Onions: Protecting Transaction Privacy in Monero*, Monero Konferenco, 22–23 VI 2019 r., https://www.monerooutreach.org/monero-konferenco/lee-clagett.html [dostęp: 1 VIII 2020].

[87] M. Möser i in., *An Empirical Analysis of Traceability in the Monero Blockchain*, „Proceedings on Privacy Enhancing Technologies" 2018, nr 3, s. 143–163, https://arxiv.org/pdf/1704.04299/

rozważaniami, informacje na temat transakcji dokonanych w kryptowalucie monero są dostępne w eksploratorach: monerovision.com, moneroblocks.info, xmr.tokenview.com, blockchair.com.

Zcash (ZEC) powstał w 2016 r. (wcześniej był znany jako Zerocoin). Obecnie jego kapitalizacja rynkowa wyniosła ponad 928 mln dolarów, w obiegu znalazło się blisko 10 mln monet, a aktualny kurs to ok. 100 dolarów amerykańskich. Zcash jest obecny na globalnych giełdach, jak BKEX, Binance, YoBit i OKEx. Nie jest to kryptowaluta używana do dużych transakcji (wymiana powyżej 100 tys. dolarów amerykańskich stanowi mniej niż 7 proc. wszystkich transakcji[88]). System Zcash zapewnia opcjonalną anonimowość, a wszystkie transakcje są odnotowywane w blockchainie; sam jego kod jest *open source*. Analizy transakcji w systemie Zcash dokonuje się z użyciem eksploratorów: explorer.zcha.in, zecblockexplorer.com, zcash.tokenview.com, blockchair.com. Anonimowość ZCash ma charakter opcjonalny i jest realizowana przez wdrożenie dwóch typów adresów: prywatnych (*shielded, z-addr*) – rozpoczynających się literą „z" oraz transparentnych (*transparent, t-addr*) – rozpoczynających się literą „t". Te dwa typy adresów współdziałają ze sobą, co oznacza, że przepływ środków między nimi jest możliwy. W praktyce mniejszość transakcji jest anonimowa – analitycy wskazują, że forma *private* jest wybierana w ok. 6 proc. wszystkich transakcji, a w praktyce niemożliwe do wyśledzenia jest 0,9 proc. z nich[89]. Możliwość wyboru między transakcjami prywatnymi i transparentnymi ma znaczenie nie tylko techniczne i praktyczne, lecz także polityczne – istnieje bowiem mniejsze ryzyko objęcia kryptowaluty negatywnymi regulacjami prawnymi. Anonimowość jest zapewniana przez nowy algorytm zk-SNARK (*Zero-Knowledge Succinct Non-Interactive Argument of Knowledge*). Jest to konstrukcja dowodowa umożliwiająca udowodnienie posiadania pewnych informacji lub zasobów (w tym przypadku środków zcash i pseudonimowej tożsamości), bez bezpośredniego ujawniania tych informacji. Jest to tzw. dowód wiedzy zerowej (*zero-knowledge proof*), pozwalający potwierdzającemu udowodnić drugiej stronie (weryfikującemu), że informacje są prawdziwe, bez ujawniania jakichkolwiek danych wykraczających poza ważność samego oświadczenia. Należy podkreślić, że bezpieczeństwo systemu Zcash jest hipotetyczne, jest to bowiem nowa forma kryptografii, której podatności są jeszcze nieznane. Na technicznych założeniach kryptowaluty zcash oparto kryptowalutę komodo (KMD) – dziedziczy ona wiele funkcji bezpieczeństwa pierwowzoru[90].

[dostęp: 1 VIII 2020]. Warto odnotować inicjatywę United States Internal Revenue Services, który zaoferował nagrodę w wysokości 650 tys. dolarów za pomoc w złamaniu anonimowości Monero, https://beta.sam.gov/opp/3b7875d5236b47f6a77f64c19251af60/ [dostęp: 29 I 2021].

88 Por. *ZCash (ZEC)*, CoinGecko, https://www.coingecko.com/pl/waluty/zcash [dostęp: 1 VIII 2020].

89 Claire Ye i in., *Alt-Coin Traceability*, International Association for Cryptologic Research, 18 V 2020 r., https://eprint.iacr.org/2020/593.pdf, s. 16–21 [dostęp: 1 VIII 2020].

90 *Advanced Blockchain Technology, Focused on Freedom*, Komodo, https://komodoplatform.com/wp-content/uploads/2018/06/Komodo-Whitepaper-June-3.pdf [dostęp: 1 VIII 2020].

Dash (DASH) wprowadzono na rynek w 2014 r. z wykorzystaniem jako podstawy protokołu systemu Bitcoin. Pierwotnie był znany jako XCoin, następnie jako Darkcoin, a po zaakceptowanym przez społeczność rebrandingu jako Dash (co jest skrótowcem utworzonym od *digital cash*). Kapitalizacja wynosi 937 mln dolarów, a w obrocie jest obecnie nieco ponad 9640 tys. monet dash. Dash jest otwartoźródłowy, nieinflacyjny (może powstać nie więcej niż 19 mln dashów) oraz częściowo zdecentralizowany. Instancją umiarkowanie centralizującą są tzw. węzły zarządzające (*masternodes*), a ich sieć tworzy zdecentralizowaną autonomiczną organizację (DAO). Służą one utrzymywaniu funkcjonowania sieci: potwierdzaniu i przesyłaniu transakcji, zapewnianiu anonimowości części z nich (na żądanie), a właściciele tych węzłów mają prawo głosu w sprawach istotnych dla społeczności Dash. Taka struktura zakłada częściowe zaufanie do podmiotów pośredniczących w transakcjach, czyli właścicieli *masternodes*. Dash oferuje dwa typy transakcji o różnym przeznaczeniu: natychmiastowe (InstantSend) i prywatne (PrivateSend). Oba typy transakcji są realizowane przez węzły zarządzające. Transakcje prywatne wykorzystują zmodyfikowaną i ulepszoną wersję protokołu CoinJoin, pierwotnie przeznaczoną do częściowej anonimizacji kryptowaluty bitcoin[91]. Istotą tej metody jest miksowanie polegające na rozmienianiu monet służących do transakcji na mniejsze nominały i wymieszaniu ich z monetami innych użytkowników przed dokonaniem transakcji. Każda runda jest miksowana na innym węźle. W rezultacie oryginalny adres, z którego transakcja została zainicjowana, jest trudny lub niemożliwy do wyśledzenia (mechanizm nieopłacalności nakładów). Maksymalna liczba dashów przesłana z użyciem transakcji prywatnej wynosi 1 tys.[92]

Anonimizacyjne parametry techniczne spowodowały, że od 2019 r. z monero, zcash i dash rezygnują liderzy giełd kryptowalut: Coinbase, OKEx, UpBit, BitBay – argumentując za wytycznymi The Financial Action Task Force (dalej: FATF), że te środki pieniężne mogłyby być wykorzystywane do działań nielegalnych[93].

Bezpieczne przechowywanie informacji

Technologie chroniące prywatność są stosowane nie tylko w komunikacji (tzw. *data-in-motion*, czyli dane w ruchu), lecz także w przechowywaniu informacji (tzw. *data-in-rest*, czyli dane w spoczynku)[94] znajdujących się w bazach danych, systemach plików i magazynowanych za pomocą innych metod (np. systemów pamięci masowej online). W celu zabezpieczenia tego typu danych korzysta się z mechanizmów kryptografii, co przy wystarczającej wprawie i znajomości tych narzędzi może chronić przed każdym,

[91] E. Duffield, D. Diaz, *Dash: A Privacy-Centric Crypto-Currency*, https://www.zioncoins.co.uk/wp-content/uploads/2015/06/Dash-Whitepaper.pdf, s. 7–8 [dostęp: 1 VIII 2020].

[92] Zob. *Dash FAQ*, https://www.dash.org/pl/faq/ [dostęp: 1 VIII 2020].

[93] FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paryż 2019 r., http://www.fatf-gafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html [dostęp: 1 VIII 2020].

[94] Lyong S.L. Liu, R. Kuhn, *Data Loss Prevention*, „IT Professional" 2010, nr 2, s. 10–13.

w tym wysoce profesjonalnym, nieautoryzowanym dostępem. Współcześnie używane mechanizmy kryptograficzne są uznawane za względnie trudne do przełamania, dlatego też władze podejmują równolegle dwa typy działań, których celem jest techniczne oraz prawne umożliwienie pozyskania informacji zabezpieczonych kryptograficznie. W przypadku pierwszego typu działań opinia publiczna nie jest w pełni świadoma możliwości, jakimi dysponują władze[95]. Informatyczno-techniczne aspekty kryptoanalizy mogą być jednak ewaluowane przez pryzmat wdrażanych rozwiązań prawnych. W wielu krajach wprowadzono prawny obowiązek ujawniania kluczy kryptograficznych pod karą grzywny lub pozbawienia wolności[96] (tzw. *key disclosure laws*), w wielu innych forsuje się lub rozważa implementację takich rozwiązań. To zjawisko potrzebuje szerszego omówienia ze względu na jego rangę. Ochronę informacji w kontekście wspomnianego obowiązku zapewnia szyfrowanie danych stanowiących tzw. wiarygodne zaprzeczenie (*plausible deniability*), a wspierają je produkty ochrony prywatności oparte na kryptografii (VeraCrypt, a dawniej TrueCrypt, czy steganografia polegająca na ukrywaniu jednej informacji w innej, np. obrazu w pliku tekstowym). Poszczególne kraje starają się radzić sobie i z takimi rozwiązaniami – wprowadzają rozmaite uregulowania prawne, które w skrajnych przypadkach naruszają prawo do niedostarczania dowodów na swoją niekorzyść i prawo do milczenia (zasada prawna: *nemo se ipsum accusare tenetur*[97]), czy po prostu ujawniają prywatne dane osobowe. Tak twarde prawo obowiązuje np. we Francji, gdzie prokurator lub sędzia może zmusić każdą osobę do przekazania kluczy lub odszyfrowania danych w celu udostępnienia informacji potrzebnych do prowadzenia dochodzenia. Za nieprzestrzeganie tego prawa grożą trzy lata więzienia lub grzywna. Przewidziana kara wzrasta do pięciu lat i grzywny nawet w wysokości 75 tys. euro, jeśli przestrzeganie przepisów zapobiegłoby przestępstwu lub złagodziło jego skutki[98]. Na mniej rygorystyczne przepisy zdecydował się belgijski ustawodawca, który daje sędziemu możliwość nakazania – zarówno operatorom systemów komputerowych, jak i dostawcom usług telekomunikacyjnych – udzielenia pomocy organom ścigania, w tym polegającej na odszyfrowaniu danych, oraz zachowania swojej pomocy w tajemnicy. Takiego działania nie można jednak podjąć wobec podejrzanego lub jego rodziny. Za nieprzestrzeganie grozi kara od sześciu

[95] Typologia i skuteczność ataków są znane wyłącznie w publicznym, naukowym dyskursie. Nie wiadomo, w jakim stopniu kryptoanaliza służb dyspozycyjnych i organów ścigania różni się od tej znanej publicznie. Dostępna jest wiedza na przykład o możliwościach i ograniczeniach ataków typu: *brute force*, *meet in the middle*, statystyczne, przez analizę różnicową, urodzinowe, zimnego rozruchu, algebraiczne i inne. Zob. np.: Ch. Swenson, *Modern Cryptanalysis: Techniques for Advanced Code Breaking,* New Jersey 2008, rozdz. 5.

[96] Dotyczy to obywateli (np. Australia), dostawców usług informatycznych (np. Belgia) oraz innych osób – m.in. ekspertów (np. Holandia).

[97] Z łac. nikt nie jest zobowiązany do oskarżania siebie (przyp. red.).

[98] *Loi relative à la sécurité quotidienne* (ustawa o powszechnym bezpieczeństwie), nr 2001–1062, 15 XI 2001 r., http://www.ejustice.just.fgov.be/eli/loi/2000/11/28/2001009048/justel [dostęp: 26 VIII 2020].

miesięcy do roku więzienia lub grzywna w wysokości od 130 do 100 tys. euro[99]. Natomiast Polska jest jednym z krajów, w których nie ma podobnych regulacji w tej kwestii. *Kodeks postępowania karnego*[100] (dalej: kpk) w art. 74 § 1 stanowi, że oskarżony nie ma obowiązku dowodzenia swojej niewinności ani obowiązku dostarczania dowodów na swoją niekorzyść. Ponadto art. 182 kpk statuuje prawo odmowy zeznań: § *1. Osoba najbliższa dla oskarżonego może odmówić zeznań; § 2. Prawo odmowy zeznań trwa mimo ustania małżeństwa lub przysposobienia; § 3. Prawo odmowy zeznań przysługuje także świadkowi, który w innej toczącej się sprawie jest oskarżony o współudział w przestępstwie objętym postępowaniem*. Porównywalne gwarancje, znane polskiemu prawu, zawiera art. 14 ust. 3 *Międzynarodowego Paktu Praw Obywatelskich i Politycznych* oraz art. 6 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*.

Wskazane uregulowania prawne stały się silnym impulsem do opracowania i wdrożenia mechanizmów samoobrony przed sankcjonowanym wymogiem ujawnienia kluczy kryptograficznych. Określa się je powszechnie mianem wiarygodnego zaprzeczenia. Wiarygodne zaprzeczenie jest to pewna informatyczna właściwość programu kryptograficznego umożliwiająca odszyfrowanie zaszyfrowanej informacji do dwóch różnych, wiarygodnie wyglądających tekstów w zależności od dostarczonego klucza kryptograficznego. To oznacza, że jeśli do dekryptażu zastosuje się klucz kryptograficzny A, to otrzyma się informację B, a przy użyciu klucza B po odszyfrowaniu odczyta się informację C. Nie ma przy tym możliwości stwierdzenia, czy zaszyfrowany obszar mieści jedną czy dwie informacje[101]. Frazy „wiarygodna zaprzeczalność" jako pierwszy użył w literaturze przedmiotu Michael Roe w swojej dysertacji[102], a omawiana koncepcja szybko doczekała się rozszerzenia i dookreślenia[103]. Jej istotę doskonale oddaje następujące zdanie: *Przedstawienie wiarygodnego dowodu jest nieodmiennie bardziej wiarygodne niż oświadczenie 'wymazałem' lub 'zapomniałem'*[104]. Pierwsze praktyczne wdrożenie mechanizmu wiarygodnej zaprzeczalności odbyło się w 1999 r., gdy przedstawiono prototyp zaprzeczalnego systemu plików o nazwie StegFS[105]. W 2004 r. powstał program TrueCrypt (wersja 1.0), który stał się niekwestionowanym

---

[99] *Loi du 28 novembre 2000 relative à la criminalité informatique* (ustawa o przestępstwach komputerowych), nr 2001009035, 28 XI 2000 r., https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2000112834&table_name=loi [dostęp: 26 VIII 2020].

[100] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: DzU z 2021 r. poz. 534).

[101] M. Kędziora, Yang-Wai Chow, W. Susilo, *Threat Models for Analyzing Plausible Deniability of Deniable File Systems*, „Journal of Software Networking" 2017, nr 1, s. 241–242.

[102] M. Roe i in., *Cryptography and Evidence*, Cambridge 1997 r., University of Cambridge, https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-780.pdf, s. 11 [dostęp: 26 VIII 2020].

[103] R. Canetti i in., *Deniable Encryption*, w: *Advances in Cryptology – CRYPTO'97*, B.S. Kaliski (red. nauk.), Berlin 1997, s. 90–104.

[104] Tamże, s. 91.

[105] M. Smith, *Mission Implausible: Defeating Plausible Deniability with Digital Forensics*, SANS Institute, 2 IV 2020 r., https://www.sans.org/reading-room/whitepapers/forensics/mission-implausible-defeating-plausible-deniability-digital-forensics-39500 [dostęp: 1 VIII 2020].

liderem programów oferujących wiarygodną zaprzeczalność. W 2014 r. organizacja The TrueCrypt Foundation zarzuciła projekt w jak dotąd niewyjaśnionych okolicznościach – oświadczenie jego twórców jest niezgodne z wynikami późniejszych audytów. Program został wycofany z oficjalnej strony oraz repozytoriów, a wspomniane oświadczenie nigdy nie było wyjaśniane, komentowane ani rozszerzane przez autorów aplikacji[106].

Następcą TrueCrypt stał się VeraCrypt – aktualnie najbardziej uniwersalny program służący do szyfrowania danych. Powstał on w 2013 r. za sprawą francuskiej firmy IDRIX. Wywodzi się (jest tzw. *forkiem*) od TrueCrypt[107]. VeraCrypt bywa wymieniany w materiałach szkoleniowych dla islamskich terrorystów[108]. Pojawiają się doniesienia, że próby pozyskania dowodów z nośników zaszyfrowanych VeraCrypt podejmowane przez służby specjalne kończą się porażką[109]. Dostarczono też wielu przykładów skutecznego stawienia oporu organom ścigania przez użytkowników[110]. VeraCrypt jest programem uniwersalnym w sensie wieloplatformowości – jest dostępny dla systemów Windows, MacOS, Linux, FreeBSD. Kodów źródłowych można użyć również samodzielnie do własnej kompilacji na różne platformy sprzętowe lub systemy. Jest popularny w społeczności informatycznej, ze względu zarówno na jakość, jak i brak alternatyw szerzej rozpowszechnionych i co najmniej równie funkcjonalnych (ograniczoną popularność oraz funkcjonalność mają np. dm-crypt, TCNext, LUKS, LiberCrypt). Warto dodać, że obsługuje on zbiory zaszyfrowane z użyciem programu TrueCrypt oraz że naprawiono w nim znane podatności. VeraCrypt jest odporny m.in. na „atak złej pokojówki" (*evil maid attack*), polegający na fizycznym przejęciu zaszyfrowanego nośnika, częściowo jest uodporniony również na tzw. atak zimnego rozruchu. Program VeraCrypt jest uznawany za względnie bezpieczny, a spośród aktualnie istniejącego oprogramowania –

---

[106] A. Junestam, N. Guigo, *Open Crypto Audit Project TrueCrypt Security Assessment,* iSec Partners, 2014 r., https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [dostęp: 1 VIII 2020]; A. Balducci, S. Devlin, T. Ritter, *TrueCrypt. Cryptographic Review*, Open Crypto Audit Project, NCC Group, 2015 r., https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf, s. 1–21 [dostęp: 1 VIII 2020].

[107] A. Haertle, *Audyt Truecrypta zakończony, dwa istotne błędy w jego implementacji*, Zaufana Trzecia Strona, 2 IV 2015 r., https://zaufanatrzeciastrona.pl/post/audyt-truecrypta-zakonczony-znaleziono-dwa-istotne-bledy-w-implementacji/ [dostęp: 1 VIII 2020].

[108] *Cyber-Terrorism Activities Report No. 18*, lipiec–wrzesień 2016 r., International Institute for Counter-Terrorism, https://www.ict.org.il/UserFiles/ICT-Cyber-Review-18.pdf, s. 24 [dostęp: 1 VIII 2020].

[109] A. Ścibor, *Służbom ze sojuszu Five Eyes nie udało się złamać szyfrowania VeraCrypt*, 29 V 2019 r., Fundacja AVLab dla Cyberbezpieczeństwa, https://avlab.pl/sluzbom-ze-sojuszu-five-eyes-nie-udalo-sie-zlamac-szyfrowania-veracrypt [dostęp: 1 VIII 2020].

[110] A. Balogun, Shao Ying Zhu, *Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology*, „International Journal of Advanced Computer Science and Applications" 2013, nr 5, s. 36–40; A. Czeskis i in., *Defeating encrypted and deniable file systems: TrueCrypt v5.1a and the case of the tattling OS and applications*, w: *Proceedings of 3rd USENIX Workshop on Hot Topics in Security*, 2008 r., https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf [dostęp: 1 VIII 2020].

za najbezpieczniejszy[111]. W 2015 r. VeraCrypt przeszedł kompleksowy audyt, który wypadł pomyślnie. Stwierdzono brak jakichkolwiek „tylnych drzwi" w jego kodzie[112]. Uczestniczy w programie Bug Bounty (2020 r.) gwarantującym nagrody pieniężne za odnajdywanie luk bezpieczeństwa w oprogramowaniu. Luk poszukują członkowie informatycznej społeczności, co znacznie usprawnia prace nad bezpieczeństwem programu[113]. VeraCrypt jest krytykowany głównie za algorytm doboru liczb losowych (mechanizm entropii jest oparty na /dev/random zamiast innych, bardziej losowych mechanizmach)[114]. Czasami podaje się w wątpliwość kwestię instytucjonalną tworzenia programu: oczywisty i udokumentowany związek przedsiębiorstwa rozwijającego VeraCrypt z francuskim rządem. Niektórzy użytkownicy zgłaszają również uwagi, że Windows 10 nie współpracuje z VeraCrypt, jeśli dojdzie do aktualizacji systemu operacyjnego znajdującego się na ukrytym nośniku. Warto jednak podkreślić, że VeraCrypt jest programem zaawansowanym kryptograficznie – implementuje liczne, dodatkowe zabezpieczenia w postaci PIM (*Personal Iterations Multiplier*), plików-kluczy oraz tokenów. Zaopatrzono go w klasyczne (*Advanced Encryption Standard, Serpent, Twofish, Camelia*), jak i najnowsze (*Kuznyechik*) algorytmy kryptograficzne i haszujące, o zróżnicowanej wydajności i poziomie gwarantowanego bezpieczeństwa. Co najistotniejsze, jest on nadzwyczaj prosty i przystępny w obsłudze (*stupid-proof*). Najważniejszą cechą programu VeraCrypt jest jego wielozadaniowość. Umożliwia on utworzenie zaszyfrowanego:

- **woluminu w zwykłym pliku**. Plik poza objętością i tym, że nie da się z niego skorzystać, jest nieodróżnialny od analogicznego pliku;
- **sekretnego woluminu w zaszyfrowanym woluminie umieszczonym w zwykłym pliku (matrioszka)**. Tworzenie tzw. matrioszek ma szczególne znaczenie dla zachowania prywatności. Powstają wówczas dwa zaszyfrowane obszary i są ustalane dwa różne hasła – każde z nich odszyfrowuje inny wolumin. Jest to praktyczna realizacja koncepcji wiarygodnej zaprzeczalności, a zatem nie ma możliwości stwierdzenia, czy zaszyfrowany obszar zawiera jeden, dwa czy więcej takich woluminów;

---

[111] Interesująca dyskusja wywiązała się na forum SourceForge w 2019 r. Ze względu na anegdotyczność tego przykładu zamieszczono go w przypisie. Otóż 24 maja opublikowano na forum post, drobiazgowo opisujący historię konfiskaty sprzętu elektronicznego, w tym dysków twardych zaszyfrowanych VeraCrypt w wersji 1.13, przez służby dyspozycyjne jednego z państw. Po upływie dwóch i pół roku urządzenia zwrócono właścicielowi, który nie poniósł żadnych konsekwencji. Ponadto autor wiadomości uwiarygodnił się, wpłacając w ramach podziękowania równowartość 10 tys. dolarów w bitcoinach na rozwój VeraCrypt, a ten fakt odnotowano w łańcuchu blockchain BTC. Zob. https://sourceforge.net/p/veracrypt/discussion/general/thread/720575f74e/ [dostęp: 1 VIII 2020].

[112] Pełny raport z audytu: A. Balducci, S. Devlin, T. Ritter, *TrueCrypt*…

[113] *Public Bug Bounty List,* Bugcrowd, 2020 r., https://www.bugcrowd.com/bug-bounty-list/ [dostęp: 1 VIII 2020].

[114] Por. dyskusja: Hacker News, https://news.ycombinator.com/item?id=21185594 [dostęp: 1 VIII 2020].

- **całego nośnika pamięci** (np. nośnika USB) **lub ukrytej partycji niesystemowej** (jednej lub wielu);
- **ukrytej partycji systemowej**. Jest ona tworzona na takiej zasadzie jak w matrioszkach. W istocie powstają dwa systemy operacyjne – zaszyfrowany, ale przeznaczony do ujawnienia, oraz zaszyfrowany i mający pozostać tajnym systemem operacyjnym. Jest to również praktyczne wdrożenie mechanizmu wiarygodnego zaprzeczenia.

Podsumowanie – modelowe atrybuty technologii wspierających prywatność

George Danezis, konstruując model zagrożeń technologii wspierających prywatność, celnie wskazał ich główne źródła. Są to: koszt (*cost*), zmowa (*collusion*), przymus (*compulsion*), korupcja (*corruption*) i nieostrożność (*carelessness*)[115]. Tą koncepcją, jako szczególnie wartościową heurystycznie, posłużono się do usystematyzowania wniosków, podając wyczerpujący zestaw modelowych cech technologii wspierających prywatność.

Warunkiem umasowienia rozwiązania chroniącego prywatność jest jego niski **koszt**. Narzędzie jest tym szerzej używane, im niższy jest próg kompetencyjny jego skutecznego zastosowania – kwalifikacje wymagane od użytkownika są niewielkie, a względnie krótkie przeszkolenie wystarcza, aby mógł on wykorzystać potencjał produktu. Czynnikiem zmniejszającym koszt jest ponadto dobrze opracowana dokumentacja, a także społeczność wspierająca produkt informatyczny i jego użytkowników. Zadaniem takiej społeczności jest świadczenie wzajemnej, zbiorowej pomocy, a także wykrywanie, zgłaszanie i trwałe usuwanie usterek w funkcjonowaniu narzędzia. Analizowane programy, systemy i usługi mają wszystkie wskazane cechy. Wspomniany koszt może być również rozumiany dosłownie – jako nieodpłatna dostępność narzędzi. Tak jest w przypadku wyżej opisanych rozwiązań. Wniesienie za nie opłat ma charakter dobrowolny i nie jest wymagane, aby program, system lub usługę użytkować. Na koszt można spojrzeć także z perspektywy barier chroniących przed naruszeniem bezpieczeństwa oferowanego przez dane narzędzie wspierające prywatność. A zatem im nakłady techniczne, finansowe i organizacyjne muszą być większe, aby te bariery przełamać, tym bardziej dane narzędzie można uznać za bezpieczne. Zasada działania technologii wspierających prywatność opiera się na takim właśnie rozwiązaniu – bariery prywatności nie są całkowite ani niemożliwe do przełamania, ale ich naruszanie jest nieopłacalne (na ogół masowe, ale czasem nawet jednostkowe i jednorazowe). Nieopłacalność naruszenia anonimowości użytkowników jest wzmacniana przez mechanizmy: podobieństwa użytkowników oraz masowości. Jeśli system lub usługa każdego

[115] G. Danezis, *A Gentle Introduction to Privacy Enhancing Technologies & 2 Case Studies*, Interdisciplinary Summerschool on Privacy, 11 VII 2016 r., https://isp.cs.ru.nl/2016/danezis.pdf [dostęp: 1 VIII 2020].

z użytkowników dla zewnętrznego obserwatora wygląda tak samo (w mechanizmie zbierania elektronicznych odcisków palców), to trudne, a nawet niemożliwie jest śledzenie poszczególnych użytkowników. W przypadku takich rozwiązań, jak VeraCrypt mechanizm maksymalizacji kosztów dla przełamującego zabezpieczenia opiera się na zasadach matematycznych – zgodnie z nimi przełamanie mechanizmów kryptograficznych w akceptowalnym czasie jest niemożliwe.

Edward Snowden, doprowadzając do największego w historii Stanów Zjednoczonych wycieku tajnych informacji, unaocznił opinii publicznej rolę, jaką odgrywa mechanizm **zmowy**, w tym konkretnym przypadku tajnego (i wymuszonego) porozumienia Agencji Bezpieczeństwa Narodowego i głównych przedsiębiorstw będących dostawcami usług, systemów i urządzeń informatycznych. Uniknięcie takiej intrygi jest możliwe przez instytucjonalne rozwiązanie przyjętego modelu biznesowego, polegające na transparentności wytwarzania, a następnie zarządzania produktem lub usługą. Środkiem najłatwiejszym do wdrożenia jest udostępnienie kodu źródłowego oraz bieżący monitoring tego kodu przez oddolnie tworzoną, opartą na samorekrutacji, zdecentralizowaną społeczność. Najważniejsze znaczenie ma tu decentralizacja, a więc brak instancji zarządzających narzędziem i brak własności intelektualnej dotyczącej tego narzędzia. Jeśli całkowite spłaszczenie struktur nie jest możliwe (sieć Tor), wówczas zadowalającym rozwiązaniem jest federalizacja. Ten typ struktury zakłada wielość, na ogół równorzędnych, ośrodków zarządczych, w związku z czym kontrolowanie ich wszystkich lub ich wystarczającej liczby jest nieopłacalne. W takiej sytuacji zmowa nie jest możliwa, a taki model (decentralizacji – Freenet, federalizacji – Tor) jest dominujący w krajobrazie PET.

Analogiczny schemat może być realizowany w celu zapobiegania mechanizmom **korupcji**. Są one również przezwyciężane przez uczynienie właścicielem produktu lub usługi całej społeczności oraz – na etapie jej funkcjonowania – przez częściową lub całkowitą jej decentralizację, a więc eliminację instytucji zaufanej trzeciej strony. Taka strategia antykorupcyjna jest w oczywisty sposób skuteczna. Rozwiązanie wykorzystane w sieci Tor zakłada liczebną i rozproszoną „zaufaną trzecią stronę" w postaci licznych i zmiennych węzłów. W przypadku sieci Freenet taki mechanizm nie występuje, sieć tworzą bowiem sami użytkownicy. Podobne zasady są stosowane w społecznościach blockchainowych, będących zbiorowymi właścicielami i zarządcami określonej kryptowaluty (np. węzły zarządzające w Dash). Z kolei twórcy takich systemów, jak Linux Tails czy Whonix zapobiegają mechanizmom korupcji inferencyjnie – przez ujawnienie kodu źródłowego i animowanie społeczności mogącej dokonywać audytu, a także pozostają otwarci na współpracę z programistami, którzy chcą uczestniczyć w projekcie.

Twórcy narzędzi wspierających prywatność coraz częściej biorą pod uwagę problem **przymusu**, rozumianego jako uregulowania prawne utrudniające lub uniemożliwiające korzystanie z tych narzędzi do celów przestępczych lub innych. Z reguły te rozstrzygnięcia przyjmują formę norm prawnych, które narzucają określonej stronie (użytkownikowi, dostawcy usług lub wytwórcy oprogramowania) ściśle określone wymogi (i w jakimś stopniu penalizujące używanie tych narzędzi). W odpowiedzi na to

wdrożono wiele innowacji informatycznych (w przypadku sieci Tor stosuje się mechanizm „zaciemniający" – obfs4, a dla VeraCrypt – mechanizm wiarygodnego zaprzeczenia). Rozwiązaniem uzupełniającym, które służy do zminimalizowania przymusu prawnego, jest stosowanie przemyślanych, systemowych wybiegów paraprawnych[116].

Przezwyciężanie mechanizmów zmowy, korupcji oraz przymusu jest wzmacniane przez postawy ideologiczno-polityczne środowiska tworzącego i wykorzystującego technologie wspierające prywatność. Jak wskazano, są one nastawione co najmniej krytycznie, jeśli nie negatywnie, do instytucji państwa, z reguły traktują je jako główne zagrożenie prywatności. Ich sympatie oscylują wokół szeroko pojętego anarchizmu czy libertarianizmu.

W technologiach wspierających prywatność najważniejszą rolę odgrywa **nieostrożność**. Brak luk bezpieczeństwa lub znane mechanizmy pozbawiające anonimowości sprawiają, że często jedyną możliwością deanonimizacji użytkownika przez służby dyspozycyjne jest błąd przez niego popełniony. Można przytoczyć wiele przykładów zaniedbania bezpieczeństwa operacyjnego przez użytkowników, co doprowadziło do aresztowań. Błędy wynikające z niewiedzy lub nieostrożności użytkowników technologii wspierających prywatność przyczyniły sie do licznych sukcesów służb dyspozycyjnych[117].

Model technologii wspierających prywatność obejmuje przemyślaną mozaikę rozwiązań informatycznych, których podstawą są kryptografia oraz rozwiązania prawne.

---

[116] *Warrant canary* to potoczne określenie odnoszące się do regularnie upublicznianego (dowolną drogą) oświadczenia, zgodnie z którym usługodawca nie otrzymał nakazu służb dyspozycyjnych dotyczącego współpracy ze służbami lub uzyskania przez nie dostępu do nośników informacji usługodawcy. Zgodnie z rozstrzygnięciami prawnymi w niektórych krajach (np. w USA) ujawnienie współpracy jest penalizowane. Działanie, które nie narusza istniejącego prawa, a jednocześnie ostrzega usługobiorców, polega na nieaktualizowaniu oświadczenia lub usunięciu go, a więc opiera się na zasadzie logicznego mechanizmu kontrapozycji. W latach 2016–2019 istniała organizacja Canary Watch (https://canarywatch.org/), koncentrująca wysiłki na zbadaniu cech *warrant canary* oraz informowaniu społeczności o inicjatywach poszczególnych usługodawców w tym zakresie. Więcej na ten temat: K. Opsahl, *Warrant Canary Frequently Asked Questions*, Electronic Frontier Foundation, 10 IV 2014 r., https://www.eff.org/deeplinks/2014/04/warrant-canary-faq [dostęp: 1 VIII 2020]. W kontekście zagrożeń bezpieczeństwa narodowego zob. R. Wexler, *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, „The Yale Law Journal" 2014, nr 158, http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design, strony nienumerowane [dostęp: 1 VIII 2020].

[117] Długą listę otwierają twórcy sklepów ze środkami psychoaktywnymi w sieci Tor, począwszy od Rossa Ulbrichta (znanego jako Dread Pirate Roberts), przez twórcę Alpha Bay Alexandre'a Cazesa, właściciela Sheep Marketplace Tomáša Jiříkovský'ego, a na administratorach Dream Market skończywszy. Analogiczną nieświadomością i lekkomyślnością w stosowaniu zasad bezpieczeństwa operacyjnego wykazali się Eric Eoin Marques, twórca i administrator największego hostingu w sieci Tor – Freedom Hosting, oraz liczni użytkownicy oferowanej przez niego usługi. Warto zasygnalizować również niedawny przypadek Bustera Hernandeza – tu również przyczyną zatrzymania była lekkomyślność cyberprzestępcy. Zob. *United States of America v. Buster Hernandez*, United States District Court, https://casetext.com/pdf-email?slug=united-states-v-hernandez-1195, s. 1–28 [dostęp: 1 VIII 2020].

Ponadto do cech konstytutywnych należy zdecentralizowany lub co najmniej sfederalizowany (rozproszony, wieloośrodkowy) model narzędzia. Najważniejszym warunkiem powodzenia tych technologii jest łatwość instalacji i obsługi, wsparta czytelnymi mechanizmami stosowania zabezpieczeń zapobiegających sprzeniewierzeniu się zasadom bezpieczeństwa operacyjnego. Własność intelektualna winna spoczywać w rękach społeczności, a kod źródłowy oprogramowania powinien być wolny. Cechy dodatkowe to masowość użytkowania oraz podobieństwo użytkowników dla obserwatora zewnętrznego.

Technologie wspierające prywatność intensywnie rozwijają się w trzech głównych obszarach funkcjonowania Internetu: komunikacji, przechowywania danych oraz wymiany handlowej. Z technicznego punktu widzenia omawiane technologie wykorzystują dwa rozwiązania – szyfrowanie oraz anonimizację lub pseudonimizację. Dodatkowe narzędzie stanowi prawo, które jest wykorzystywane instrumentalnie w celu wzmocnienia ochrony informatycznej (popatrz: *warrant canary*). Należy podkreślić, że kilkadziesiąt lat lobbingu legislacyjnego na rzecz ochrony prywatności nie powstrzymało erozji wartości prywatności (przynajmniej w oczach niektórych obserwatorów), a technologie wspierające prywatność pojawiły się jako odpowiedź na braki legislacyjne[118].

Technologie wspierające prywatność to narzędzia podwójnego zastosowania. Mogą posłużyć i są faktycznie wykorzystywane zarówno do oddolnej samoobrony jednostek przed działaniami ujawniającymi dane wrażliwe, jak i do działań cyberprzestępczych (zwłaszcza przestępczości o charakterze ekonomicznym, politycznym i obyczajowym). Pierwotne przeznaczenie technologii wspierających prywatność do ochrony jednostki w kontekście działań cyberprzestępczych oraz agresywnego marketingu jest niepodważalne i nie budzi wątpliwości ani etycznych, ani prawnych[119]. Mogą się one pojawić, jeśli spojrzy się na to zagadnienie z technicznego punktu widzenia: stopień zaawansowania i jakość rozwiązań wydają się nadmierne do ochrony dóbr zagrożonych w tym sensie, że można te dobra z powodzeniem chronić przy użyciu prostszych narzędzi i rozwiązań. Dualizm tych zastosowań jest nierozerwalny, a przez to dylemat penalizacji środków wspierających prywatność wydaje się nierozwiązywalny z użyciem działań legislacyjnych lub technicznych. Jako jedyne rozwiązanie problemu wskazuje się czasochłonną i kosztochłonną społeczną redefinicję pojęcia p r y w a t n o ś ć[120].

---

[118] P.E. Agre, M. Rotenberg, *Technology and Privacy: The New Landscape*, Cambridge 1997; C.J. Bennet, *Regulating Privacy: Data Protection and Public Policy in Europe and the United States*, Ithaca 1992; D. Lyon, *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination*, New York–London 2003.

[119] R.V. Clarke, *Technology, criminology and crime science,* „Crime and Deviance in Cyberspace" 2004, nr 1, s. 441–450; A.S. Wilner, *Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation,* „International Journal: Canada's Journal of Global Policy Analysis" 2018, nr 2, s. 308–316.

[120] F. Stalder, *The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy*, „Sociological Research Online" 2002, nr 2, s. 25–39.

Bibliografia

Acar K.V., *Child abuse materials as digital goods: Why we should fear new commercial forms*, „Economics Discussion Papers" 2017, nr 15, bez paginacji.

Assange J. i in., *Cypherpunks. Freedom and the Future of the Internet*, New York–London 2012, OR Books.

Balogun A., Zhu Shao Ying, *Privacy Impacts of Data Encryption on the Efficiency of Digital Forensics Technology*, „International Journal of Advanced Computer Science and Applications" 2013, nr 5, s. 36–40.

Canetti R. i in., *Deniable Encryption*, w: *Advances in Cryptology – CRYPTO'97*, B.S. Kaliski (red. nauk.), Berlin 1997, Springer, s. 90–104.

Chaum D., *Security without Identification. Transaction Systems to Make Big Brother Obsolete*, „Communications of the ACM" 1985, nr 10, s. 1030–1044.

Clarke R.V., *Technology, criminology and crime science*, „Crime and Deviance in Cyberspace" 2004, nr 1, s. 441–450.

Clifford B., Powell H., *Encrypted Extremism. Inside the English-Speaking Islamic State Ecosystem on Telegram, Program on Extremism*, Washington 2019, The George Washington University.

Crypto Anarchy, Cyberstates, and Pirate Utopias, P. Ludlow (red.), Cambridge 2001, Bradford Books.

Denning D.E., Baugh W.E, *Encryption and evolving technologies: Tools of organized crime and terrorism, Working group on organized crime*, Washington 1997, National Strategy Information Center, s. 1–64.

Diffie W., Hellman M.E., *New Directions in Cryptography*, „IEEE Transactions on Information Theory" 1976, nr 6, s. 644–654.

Dion-Schwarz C., Manheim D., Johnson P.B., *Terrorist Use of Cryptocurrencies. Technical and Organizational Barriers and Future Threats*, Santa Monica 2019, RAND Corporation.

Dostov V., Shust P., *Cryptocurrencies: An Unconventional Challenge to the AML/CFT Regulators?*, „Journal of Financial Crime" 2014, nr 3, s. 249–263.

Eyal I., *Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities*, „Computer" 2017, nr 9, s. 38–49.

Fanti G. i in., *Dandelion ++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees*, „Proceedings of the ACM on Measurement and Analysis of Computing Systems" 2018, nr 2, https://arxiv.org/pdf/1805.11060.pdf [dostęp: 1 VIII 2020].

Hammill Ch., *Od kuszy do kryptografii, czyli psucie państwu szyków przy pomocy techniki*, tłum. J. Sierpiński, „Kultura i Historia" 2007, nr 11, http://www.kulturaihistoria.umcs.lublin.pl/archives/701 [dostęp: 20 XI 2018].

Handbook of Privacy and Privacy-Enhancing Technologies. The case of Intelligent Software Agents, G.W. van Blarkom, J.J. Borking, J.G.E. Olk (red. nauk.), Haga 2003, PISA Consortium.

Harvey J., Branco-Illodo I., *Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in 'Privacy Coin' Whitepapers*, „Journal of Political Marketing" 2020, nr 1–2, s. 107–136.

Herian R., *The Politics of Blockchain*, „Law and Critique" 2018, nr 2, s. 129–131.

Heurix J. i in., *A taxonomy for privacy enhancing technologies*, „Computers & Security" 2015, t. 53, s. 1–17.

Hurlburt G., *Shining Light on the Dark Web*, „IEEE Computer" 2017, nr 4, s. 100–105.

Karlstrøm H., *Do Libertarians Dream of Electric Coins? The Material Embeddedness of Bitcoin*, „Distinktion: Scandinavian Journal of Social Theory" 2014, nr 1, s. 23–36.

Kędziora M., Chow Yang-Wai, Susilo W., *Threat Models for Analyzing Plausible Deniability of Deniable File Systems*, „Journal of Software Networking" 2017, nr 1, s. 241–264.

Lewis J.A., Zheng D.E., Carter W.A, *The Effect of Encryption on Lawfull Access to Communications and Data, Rowman & Littlefield*, Lanham–Boulder–New York–London 2017, Rowman&Littlefield.

Liu Lyong S.L., Kuhn R., *Data Loss Prevention*, „IT Professional" 2010, nr 2, s. 10–13.

Malik N., *Terror in the Dark. How terrorists use encryption, the darknet, and cryptocurrencies*, Millbank 2018, The Henry Jackson Society.

Maurer B., Nelms T.C., Swartz L., *When Perhaps the Real Problem Is Money Itself! The Practical Materiality of Bitcoin*, „Social Semiotics" 2013, nr 2, s. 261–277.

Mider D., *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, „Przegląd Bezpieczeństwa Wewnętrznego" 2019, nr 21, s. 154–190.

Möser M. i in., *An Empirical Analysis of Traceability in the Monero Blockchain*, „Proceedings on Privacy Enhancing Technologies" 2018, nr 3, s. 143–163, https://arxiv.org/pdf/1704.04299/ [dostęp: 1 VIII 2020].

Privacy-enhancing technologies. The path to anonimity, R. Hes, J.J. Borking (red. nauk.), Haga 2000, Registratiekamer.

Pryciak M., *Prawo do prywatności*, „Wrocławskie Studia Erazmiańskie" 2010, nr 4, s. 211–229.

Quayle E., Taylor M., *Paedophiles, Pornography and the Internet: Assessment Issues*, „British Journal of Social Work" 2002, nr 7, s. 863–875.

Shapiro A.L., *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know*, New York 1999, Perseus Books.

Stalder F., *The Failure of Privacy Enhancing Technologies (PETs) and the Voiding of Privacy*, „Sociological Research Online" 2002, nr 2, s. 25–39.

Swenson Ch., *Modern Cryptanalysis: Techniques for Advanced Code Breaking*, rozdz. 5, New Jersey 2008, John Wiley&Sons.

United Nations Office on Drugs and Crime, *The use of the Internet for terrorist purposes*, New York 2012.

Van Hout M.C., Bingham T., *Silk Road, the Virtual Drug Marketplace: A Single Case Study of User Experiences*, „International Journal of Drug Policy" 2013, nr 5, s. 385–391.

Wang Yang, Kobsa A., *Privacy-Enhancing Technologies*, w: *Handbook of Research on Social and Organizational Liabilities in Information Security*, M. Gupta, R. Sharman (red. nauk.), New York 2009, IGI Global.

Warren S.D., Brandeis L.D., *The Right to Privacy*, „Harvard Law Review" 1890, nr 4, s. 193–220.

Weimann G., *Going Dark: Terrorism on the Dark Web*, „Studies in Conflict & Terrorism" 2016, nr 3, s. 195–206.

Weimann G., *Terror on the Internet: The New Arena, The New Challenges*, Washington 2006, United States Institute of Peace.

Weimann G., *Terrorism in Cyberspace: The Next Generation*, New York 2015, Columbia University Press.

Weimann G., *Terrorist Migration to the Dark Web*, „Perspectives on Terrorism" 2016, nr 3, s. 40–44.

Wexler R., *Warrant Canaries and Disclosure by Design: The Real Threat to National Security Letter Gag Orders*, „The Yale Law Journal" 2014, nr 158, http://www.yalelawjournal.org/forum/warrant-canaries-and-disclosure-by-design, bez paginacji [dostęp: 1 VIII 2020].

Wilner A.S., *Cybersecurity and its discontents: Artificial intelligence, the Internet of Things, and digital misinformation*, „International Journal: Canada's Journal of Global Policy Analysis" 2018, nr 2, s. 308–316.

Źródła internetowe

Advanced Blockchain Technology, *Focused on Freedom*, Komodo, https://komodoplatform.com/wp-content/uploads/2018/06/Komodo-Whitepaper-June-3.pdf [dostęp: 3 VIII 2020].

Arora H., *NSA classifies Linux Journal readers, Tor and Tails Linux users as "extremists"*, 4 VII 2014 r., https://static.techspot.com/community/topics/nsa-classifies-linux-journal readers-torand-tails-linux-users-as-extremists.203649/page-3 [dostęp: 1 VIII 2020].

Austin J., *'Traitor' Edward Snowden 'taught ISIS Paris terrorists how to avoid detection'*, „Express", 18 XI 2015 r., https://www.express.co.uk/news/world/620270/Traitor Edward-Snowden-taught-ISIS-Paris-terrorists-avoid-detection-NSA-CIA-John-Brennan [dostęp: 2 VIII 2020].

Barbirato B.B., *Bitcoin: A Political Analysis*, maj 2016 r., https://www.researchgate.net/publication/309411431_Bitcoin_A_Political_Analysis [dostęp: 1 VIII 2020].

Barysevich A., Sola A., *Litecoin Emerges as the Next Dominant Dark Web Currency*, Recorded Future, 8 II 2018 r., https://go.recordedfuture.com/hubfs/reports/cta-2018 0208.pdf [dostęp: 1 VIII 2020].

Berton B, *The dark side of the web: ISIL's one-stop shop*?, raport European Union Institute for Security Studies, czerwiec 2015 r., https://www.iss.europa.eu/sites/default/files/EUISSFiles/Alert_30_The_Dark_Web.pdf [dostęp: 1 VIII 2020].

Balducci A., Devlin S., Ritter T., *TrueCrypt. Cryptographic Review*, Open Crypto Audit Project, NCC Group, 2015 r., https://opencryptoaudit.org/reports/TrueCrypt_Phase_II_NCC_OCAP_final.pdf, s. 1–21 [dostęp: 2 VIII 2020].

Clagett L., *Dandelion Onions: Protecting Transaction Privacy in Monero*, Monero Konferenco, 22–23 VI 2019 r., https://www.monerooutreach.org/monero-konferenco/lee-clagett.html [dostęp: 1 VIII 2020].

Cox J., *Cryptocurrency Transactions May Uncover Sales of Shadow Broker Hacking Tools*, „Vice", 28 VI 2018 r., https://www.vice.com/en_us/article/j5k7zp/zcash-shadow-brokers-uncoverhacking-tool-sales [dostęp: 1 VIII 2020].

Cyber-Terrorism Activities Report No. 18, lipiec–wrzesień 2016 r., International Institute for Counter-Terrorism, https://www.ict.org.il/UserFiles/ICT-Cyber-Review-18.pdf, s. 24 [dostęp: 1 VIII 2020].

Czeskis A. i in., *Defeating encrypted and deniable file systems: TrueCrypt v5.1a and the case of the tattling OS and applications*, w: *Proceedings of 3rd USENIX Workshop on Hot Topics in Security*, 2008 r., https://www.usenix.org/legacy/event/hotsec08/tech/full_papers/czeskis/czeskis.pdf [dostęp: 1 VIII 2020].

Danezis G., *A Gentle Introduction to Privacy Enhancing Technologies & 2 Case Studies*, 11 VII 2016 r., https://isp.cs.ru.nl/2016/danezis.pdf [dostęp: 1 VIII 2020].

Danezis G., Gürses S., *A critical review of 10 years of Privacy Technology*, Proceedings of Surveillance Cultures: A Global Surveillance Society, kwiecień 2010 r., https://homes.esat.kuleuven.be/~sguerses/papers/DanezisGuersesSurveillancePets2010.pdf [dostęp: 1 VIII 2020].

De Balthasar T., Hernandez-Castro J., *An Analysis of Bitcoin Laundry Services*, Nordic Conference on Secure IT, Tartu 2017 r., https://www.researchgate.net/publication/319944399_An_Analysis_of_Bitcoin_Laundry_Services [dostęp: 4 VIII 2020].

Duffield E., Diaz D., *Dash: A Privacy-Centric Crypto-Currency*, https://www.zioncoins.co.uk/wp-content/uploads/2015/06/Dash-Whitepaper.pdf, s. 7–8 [dostęp: 1 VIII 2020].

Faife C., *Live Free or Mine: How Libertarians Fell in Love With Bitcoin*, CoinDesk, 8 X 2016 r., https://www.coindesk.com/live-free-or-mine-how-libertarians-fell-in-love-with-bitcoin [dostęp: 1 VIII 2020].

Fanusie Y.J., Robinson T., *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*, Foundation for Defense of Democracies and Elliptic, 12 I 2018 r., http://www.defenddemocracy.org/content/uploads/documents/MEMO_Bitcoin_Laundering.pdf, s. 7 [dostęp: 1 VIII 2020].

FATF, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, Paryż 2019 r., http://www.fatfgafi.org/publications/fatfrecommendations/documents/Guidance-RBA-virtual-assets.html [dostęp: 1 VIII 2020].

Fox-Brewster T., *Wannacry hackers are using this Swiss company to launder $142,000 Bitcoin ransoms*, „Forbes", lipiec 2017 r., https://www.forbes.com/sites/thomasbrewster/2017/08/03/wannacryhackers-use-shapeshift-to launder-bitcoin [dostęp: 1 VIII 2020].

Gogłoza W., *Cypherpunks, WikiLeaks i widmo kryptograficznej anarchii*, https://wgogloza.com/umcs/informatyka-prawnicza/cypherpunks/ [dostęp: 20 XII 2018].

Goodwin B., *Islamic State supporters shun Tails and Tor encryption for Telegram,* „Computer Weekly", 8 I 2017 r., https://www.computerweekly.com/news/450419581/Islamic-State-supporters-shun-Tails-and-Tor-encryption-for-Telegram [dostęp: 1 VIII 2020].

Greenberg A., *The dark web's favorite currency is less untraceable than it seems*, „Wired", 27 III 2018 r., https://www.wired.com/story/monero-privacy/ [dostęp: 1 VIII 2020].

Greene D., *NSA Mass Surveillance Programs. Unnecessary and Disproportionate*, Electronic Frontier Foundation, 2014 r., https://www.eff.org/files/2014/05/29/unnecessary_and_disproportionate.pdf [dostęp: 1 VIII 2020].

Haertle A., *Audyt Truecrypta zakończony, dwa istotne błędy w jego implementacji*, Zaufana Trzecia Strona, 2 IV 2015 r., https://zaufanatrzeciastrona.pl/post/audyt-truecryptazakonczony-znaleziono-dwa-istotne-bledy-w-implementacji/ [dostęp: VIII 2020].

Harris S., *CIA's Ex-No. 2 Says ISIS 'Learned From Snowden'*, „Daily Beast", 12 VII 2017 r., https://www.thedailybeast.com/cias-ex-no-2-says-isis-learned-from-snowden [dostęp: 1 VIII 2020].

Higgins S., *ISIS-Linked Blog: Bitcoin Can Fund Terrorist Movements Worldwide*, CoinDesk, 7 VII 2014 r., https://www.coindesk.com/isis-bitcoin-donations-fund-jihadist movements/ [dostęp: 1 VIII 2020].

Jafari S. i in., *Cryptocurrency: A Challenge to Legal System*, Social Science Research Network, styczeń 2018 r., https://www.researchgate.net/publication/325747817_Cryptocurrency_A_Challenge_to_Legal_System [dostęp: 1 VIII 2020].

Junestam A., Guigo N., *Open Crypto Audit Project TrueCrypt Security Assessment*, iSec Partners, 2014 r., https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf [dostęp: 1 VIII 2020].

Keatinge T., Carlisle D., Keen F., *Virtual currencies and terrorist financing: assessing the risks and evaluating responses*, European Parliament, Policy Department for Citizen's Rights and Constitutional Affairs, 2018 r., http://www.europarl.europa.eu/RegData/etudes/STUD/2018/604970/IPOL_STU(2018)60497 _EN.pdf [dostęp: 1 VIII 2020].

Makdad Ch., *"God Rewards Fools" – Whitfield Diffie and Martin Hellman's Stand to Revolutionize Cryptography*, The Eagle Eye News, https://tyroneeagleeyenews.com/wp content/uploads/2017/05/Makdad_Senior_TyroneAreaHighSchool_PA.pdf [dostęp: 1 VIII 2020].

Malik N., *Terror in the Dark*, London 2015 r., raport Henry Jackson Society, http://henryjacksonsociety.org/wp-content/uploads/2018/04/Terror-in-the-Dark.pdf [dostęp: 4 VIII 2020].

May T.C., *Cyphernomicon. Cypherpunks FAQ and More, Version 0.666,* 10.09.1994, http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html [dostęp: 20 XII 2018].

May T.C., *The Crypto Anarchist Manifesto*, Activism.net, 22 XI 1992 r., https://www.activism.net/cypherpunk/crypto-anarchy.html [dostęp: 20 XII 2018].

May T.C., *True Nyms and Crypto Anarchy*, 2001, http://www.isfdb.org/cgi-bin/title.cgi?195636 [dostęp: 20 XII 2018].

Opsahl K., *Warrant Canary Frequently Asked Questions*, Electronic Frontier Foundation, 10 IV 2014 r., https://www.eff.org/deeplinks/2014/04/warrant-canary-faq [dostęp: 1 VIII 2020].

Protecting privacy in practice. The current use, development and limits of Privacy Enhancing Technologies in data analysis, A. Noble (red. nauk.), The Royal Society, marzec 2019 r., https://royalsociety.org/-/media/policy/projects/privacy-enhancing-technologies/privacy enhancing-technologies-report.pdf [dostęp: 5 VIII 2020].

Public Bug Bounty List, Bugcrowd, 2020 r., https://www.bugcrowd.com/bug-bounty-list/ [dostęp: VIII 2020].

Roe M. i in., *Cryptography and Evidence*, Cambridge 1997 r., University of Cambridge, https://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-780.pdf, s. 11 [dostęp: 26 VIII 2020].

Ryan P., *Left, Right and Center: Crypto Isn't Just for Libertarians Anymore*, CoinDesk, 27 VII 2018 r., https://www.coindesk.com/no-crypto-isnt-just-for-libertarians-anymore [dostęp: 1 VIII 2020].

Shen Y., Pearson S., *Privacy Enhancing Technologies: A Review*, HP Laboratories, sierpień 2011 r., https://www.hpl.hp.com/techreports/2011/HPL-2011-113.pdf [dostęp: 5 VIII 2020].

Smith M., *Mission Implausible: Defeating Plausible Deniability with Digital Forensics*, SANS Institute, 2 IV 2020 r., https://www.sans.org/reading-room/whitepapers/forensics/mission-implausible-defeating-plausible-deniability-digital-forensics-39500 [dostęp: 1 VIII 2020].

Stancel D., *Economic Consequences of Cryptocurrencies and Associated Decentralized Systems*, https://www.researchgate.net/publication/280794376_Economic_Consequences_of_Cryptocu rencies_and_Associated_Decentralized_Systems [dostęp: 1 VIII 2020].

Ścibor A., *Służbom ze sojuszu Five Eyes nie udało się złamać szyfrowania VeraCrypt*, Fundacja AVLab dla Cyberbezpieczeństwa, 29 V 2019 r., https://avlab.pl/sluzbom-ze-sojuszu-five-eyes-nie-udalo-sie-zlamac-szyfrowaniaveracrypt [dostęp: 3 VIII 2020].

United States of America v. Buster Hernandez, United States District Court, https://casetext.com/pdf-email?slug=united-states-v hernandez-1195, s. 1–28 [dostęp: 1 VIII 2020].

Titcomb J., *Did Paris terrorists really use PlayStation 4 to plan attacks?,* „The Telegraph", 16 XI 2015 r., https://www.telegraph.co.uk/technology/videogames/playstation/11997952/paris-attacks-playstation-4.html [dostęp: VIII 2020].

Venkatakrishan S.B, Fanti G., Viswanath P., *Dandelion: Redesigning the Bitcoin Network for Anonymity*, Sigmetrics'17, 5–9 VI 2017 r., Urbana-Champaign, https://dl.acm.org/doi/10.1145/3078505.3078528 [dostęp: 1 VIII 2020].

Ye Claire i in., *Alt-Coin Traceability*, International Association for Cryptologic Research, 18 V 2020 r., https://eprint.iacr.org/2020/593.pdf, s. 16–21 [dostęp: 1 VIII 2020].

Zulkarnine A.T. i in., *Surfacing Collaborated Networks in Dark Web to Find Illicit and Criminal Content*, IEEE Conference on Intelligence and Security Informatics (ISI), Tucson 2016 r., s. 109–114, https://ieeexplore.ieee.org/xpl/conhome/7739307/proceeding [dostęp: 3 VIII 2020].

Akty prawne

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. uchwalona przez Zgromadzenie Narodowe w dniu 2 kwietnia 1997 r., przyjęta przez Naród w referendum konstytucyjnym w dniu 25 maja 1997 r., podpisana przez Prezydenta Rzeczypospolitej Polskiej w dniu 16 lipca 1997 r. (DzU z 1997 r. nr 78 poz. 483, ze zm.).

Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności sporządzona w Rzymie dnia 4 listopada 1950 r., zmieniona następnie Protokołami nr 3, 5 i 8 oraz uzupełniona Protokołem nr 2 (DzU z 1993 r. nr 61 poz. 284).

Międzynarodowy Pakt Praw Obywatelskich i Politycznych otwarty do podpisu w Nowym Jorku dnia 19 grudnia 1966 r. (DzU z 1977 r. nr 38 poz. 167).

Powszechna Deklaracja Praw Człowieka (*Rezolucja Zgromadzenia Ogólnego ONZ 217 A (III) przyjęta i proklamowana 10 grudnia 1948 r.).*

Karta Praw Podstawowych Unii Europejskiej z 7 grudnia 2000 r. (Dz. Urz. UE C 83 z 30 III 2010 r., s. 389.)

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – (Dz. Urz. UE L 119 z 4 V 2016 r., s. 1).

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j.: DzU z 2019 r. poz. 1781).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2020 r. poz. 1444, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego (t.j.: DzU z 2021 r. poz. 534).

Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (tj.: Dz.U. z 2019 r. poz. 1231).

Ustawa z dnia 23 kwietnia 1964 r. – Kodeks cywilny (t.j.: Dz.U. z 2019 r. poz. 1145, ze zm.).

Abstrakt

Technologie wspierające prywatność (*Privacy Enhancing Technologies*, PET) stwarzają zagrożenie ładu społecznego. Wskazuje na to analiza ich ideologiczno-politycznych fundamentów oraz uregulowań prawnych wprowadzających ograniczenia w zakresie ich używania, a także analiza ich faktycznych zastosowań w działalności cyberprzestępczej. Opracowanie ma charakter przeglądowy i praktyczny, dokonano w nim autorskiego stypologizowania technologii wspierających prywatność. Ocenie poddano wybrane instrumenty informatyczne, które są najpowszechniej używane oraz stanowią potencjalne i rzeczywiste zagrożenie. Są to: oprogramowania zapewniające anonimową komunikację (Tor, Freenet, Linux Tails, Whonix), ekosystemy kryptowalut umożliwiające anonimową wymianę handlową (Monero, Zcash, Dash) oraz aplikacja, która pozwala na szyfrowanie danych (VeraCrypt). Podsumowanie jest próbą wskazania modelowych atrybutów technologii wspierających prywatność na podstawie wcześniej przeprowadzonych analiz.

Słowa kluczowe: technologie wspierające prywatność, anonimowość, cyberprzestępczość, terroryzm, kryptoanarchizm.

Privacy Enhancing Technologies – ideology, law and implementations

Abstract

Privacy Enhancing Technologies (PET) create a threat to the social order which is shown in the analysis of their ideological as well as political foundations and legal regulations that introduce restrictions on their use. Study into their actual applications in cybercriminal activity proves it too. This paper is a review with practical purpose and includes an original typology of PET. The most commonly used IT instruments that create a potential and actual threat were selected and analysed: software ensuring anonymous communication (Tor, Freenet, Linux Tails, Whonix), cryptocurrency systems enabling anonymous trade (Monero, Zcash, Dash) and an application enabling data encryption (VeraCrypt). The summary includes an attempt to extract the model attributes of privacy-enhancing technologies on the basis of previous analyses.

Keywords: privacy enhancing technologies, anonymity, cybercrime, terrorism, crypto anarchy.