CZŁOWIEK W CYBERŚWIECIE: CIEMNE I JASNE STRONY TECHNOLOGII

Maciej Miłostan

Politechnika Poznańska

Postęp technologiczny powoduje zwykle poprawę warunków życia człowieka, zwiększa komfort funkcjonowania zarówno indywidualnych jednostek, jak i całych społeczeństw. Jednak patrząc z perspektywy historycznej, łatwo zauważyć, że dzieła nauki i techniki niejednokrotnie znajdują zastosowanie do mniej szczytnych celów, a niekiedy wręcz są tworzone z myślą o tym, by szkodzić człowiekowi. Dobrym punktem odniesienia są w tym przypadku technologie militarne, które z założenia tworzy się tak, aby były możliwie destrukcyjne dla potencjalnego wroga.

Przy czym postęp uzyskany w technologiach wojskowych niejednokrotne przekłada się na postęp w technologiach cywilnych, dobrym przykładem jest tu energetyka jądrowa – najpierw do użycia weszła bomba atomowa[1], a następnie skonstruowano stosunkowo bezpieczne reaktory wykorzystywane do wytwarzania energii elektrycznej[2].

Niektóre technologie mogą mieć jednocześnie zastosowanie w sektorze cywilnym oraz militarnym, co świetnie obrazuje wynalazek Nobla – dynamit[3].

[1] „Trinity Test – 1945", Atomic Heritage Foundation, http://www.atomicheritage.org/history/trinity-test-1945 (dostęp 15.11.2019).

[2] „First nuclear power", Oak Ridge National Laboratory, https://www.ornl.gov/blog/ornl-reporter/first-nuclear-power (dostęp 15.11.2019).

[3] Marc Lallanilla, „The Dark Side of the Noble Prizes", https://www.livescience.com/40188-dark-history-alfred-nobel-prizes.html (dostęp 14.01.2020).

Dobrym przykładem różnorodnego sposobu wykorzystania tej samej technologii jest również broń palna[4], której używa się zarówno do polowań, obrony własnej, jak i do siania terroru przez zorganizowane grupy przestępcze lub organizacje paramilitarne.

Przytaczając te przykłady, zmierzamy do tego, że technologia – niezależnie od tego, w jakim celu pierwotnie została stworzona – sama w sobie zwykle nie jest ani zła, ani dobra, dopiero sposób jej wykorzystania sprawia, że odbieramy ją pozytywnie lub negatywnie. Technologia pierwotnie stworzona dla dobrych celów może zostać wykorzystana w złych intencjach i *vice versa*.

Przyjrzyjmy się teraz temu, jakie technologie stanowią podstawy współczesnego cyberświata, świata, w którym komunikujące się urządzenia cyfrowe grają pierwsze skrzypce i stanowią podstawę do tworzenia nowych usług. Nie można zaprzeczyć, że weszliśmy w erę powszechnej cyfryzacji[5] rozmaitych aspektów życia i aktualnie świat cyfrowy, wirtualny, coraz bardziej splata się ze światem fizycznym. Technologie, z których na co dzień korzystamy, są dla nas z jednej strony wybawieniem, a z drugiej zagrożeniem. Mogą one być stosowane z korzyścią dla nas, w uczciwym celu, jak również w celach przestępczych lub w celu ograniczania swobód obywatelskich. Właściwie stosowane stanowią element systemu bezpieczeństwa chroniącego indywidualne osoby lub systemy, a nadużywane są środkiem umożliwiającym osiąganie wymiernych korzyści przez grupy przestępcze, lobbystów lub rządzących (zwłaszcza w państwach niedemokratycznych). Przeanalizujmy kilka przykładów technologii i związanych z nimi zagrożeń.

Za pierwszy przykład niech posłużą nam tzw. zapory sieciowe (ang. *firewall*[6]). Blokują one, selektywnie, połączenia wychodzące i przychodzące, w pewnych podsieciach lub na pojedynczych komputerach, i są powszechnie wykorzystywane do ochrony infrastruktury sieciowej przed atakami oraz przejmowaniem zasobów komputerowych przez hakerów, w tym przed wykorzystywaniem łącz do rozsyłania niechcianej korespondencji. Dla przykładu, blokada protokołu SMTP i komunikacji na porcie 25 u większości dostawców Internetu ogranicza propagację tzw. spamu. Zapory wymyślono po to, by chronić sieci korporacyjne

[4] „Firearms", History.com, https://www.history.com/topics/inventions/firearms (dostęp 14.01.2020).

[5] „Od papierowej do cyfrowej Polski", Ministerstwo Cyfryzacji RP, https://www.gov.pl/web/cyfryzacja/od-papierowej-do-cyfrowej-polski (dostęp 14.01.2020).

[6] „Firewall", Wikipedia, https://en.wikipedia.org/wiki/Firewall_(computing) (dostęp 14.01.2020).

i indywidualnych użytkowników Internetu poprzez ograniczenie ich ekspozycji na zagrożenia. Jednakże Iran i Chiny wykorzystują tę samą technologię do skutecznego ograniczania kontaktów własnych obywateli z resztą świata[7], głównie ze światem zachodnim. Tak zwany Wielki Chiński Firewall[8] utrudnia dostęp do stron uznanych przez cenzurę za zakazane, np. popularnych usług firmy Google. Podobnie sprawy mają się w Iranie, tam również obywatele nie mają swobodnego dostępu do światowego Internetu. Rosja natomiast głośno mówi o tworzeniu własnego „Internetu" z możliwością odseparowania od sieci międzynarodowej[9], tu oficjalnym celem jest lepsza „ochrona" własnych obywateli, a w praktyce lepsza kontrola nad obywatelami i treściami, do których mają oni dostęp.

W odpowiedzi na próby inwigilacji i ograniczania dostępu do zasobów zaproponowano wiele rozwiązań mających na celu ochronę prywatności i danych, a także umożliwiających obejście zapór sieciowych. Do portfolio powszechnie stosowanych rozwiązań możemy zaliczyć szyfrowanie kanałów komunikacyjnych (i dysków)[10], enkapsulację czy tunelowanie ze szczególnym uwzględnieniem wirtualnych sieci prywatnych (VPN)[11], jak również sieci węzłów pośredniczących ze specjalnie skonstruowanymi mechanizmami routingu (wyboru tras pakietów), opartymi na algorytmach kryptograficznych – przykładem takiego rozwiązania jest Tor[12].

Innymi słowy, wraz ze wzrostem świadomości zagrożeń zarówno wśród użytkowników Internetu, jak i decydentów, zaczęto projektować i wdrażać systemy lepiej chroniące dane na różnych etapach przetwarzania. Podstawowym mechanizmem zabezpieczania danych przesyłanych kanałami komunikacyjnymi i przechowywanych w systemach komputerowych są algorytmy kryptograficzne umożliwiające szyfrowanie danych. W chwili obecnej stosuje się dwie główne klasy tych algorytmów: symetryczne i asymetryczne. Te drugie, zwane również

[7] „Cenzura w Internecie", Wikipedia, https://pl.wikipedia.org/wiki/Cenzura_w_Internecie (dostęp 14.01.2020).
[8] „The Great Firewall of China", Bloomberg News, https://www.bloomberg.com/quicktake/great-firewall-of-china (dostęp 14.01.2020).
[9] M. Domańska, „Twierdza Runet: walka Kremla z „wrogim" Internetem", Ośrodek Studiów Wschodnich, https://www.osw.waw.pl/pl/publikacje/analizy/2019-04-19/twierdza-runet-walka-kremla-z-wrogim-internetem (dostęp 14.01.2020).
[10] „OpenSSL", OpenSSL Software Foundation, https://www.openssl.org/ (dostęp 14.01.2020).
[11] „VPN Gate Overview", University of Tsukuba, Japan, https://www.vpngate.net/en/about_overview.aspx (dostęp 14.01.2020).
[12] Tor Project, https://www.torproject.org/ (dostęp 14.01.2020).

algorytmami z kluczem jawnym, tworzą podstawy tzw. infrastruktury klucza publicznego[13] (PKI – *Public Key Infrastucture*). W przypadku tej grupy algorytmów mamy do czynienia z parą kluczy – jeden klucz (zwany publicznym) jest powszechnie znany i wykorzystywany do szyfrowania wiadomości, a drugi jest tajny i służy do deszyfrowania wiadomości. Konstrukcja algorytmu zwykle dopuszcza możliwość zamiany kluczy i wykorzystanie klucza prywatnego do szyfrowania, a publicznego do deszyfrowania, co stanowi podstawę podpisów elektronicznych. Gwarantem bezpieczeństwa takiego systemu kryptograficznego jest złożoność obliczeniowa operacji, w której można z klucza publicznego wygenerować klucz prywatny. Innymi słowy, wyliczenie klucza prywatnego z publicznego zajmuje bardzo dużo czasu, w praktyce powinno trwać dłużej niż wynosi „okres przydatności" zaszyfrowanej wiadomości.

PKI jest powszechnie wykorzystywana w podpisach cyfrowych i to ona umożliwia m.in. dostarczanie certyfikatów SSL używanych do zabezpieczania stron WWW. Dzięki certyfikatom przeglądarka jest w stanie potwierdzić tożsamość witryny na podstawie łańcucha zaufania i poinformować użytkownika, że łączy się ze zweryfikowaną witryną – świadczy o tym symbol kłódki wyświetlany przy pasku adresu. Weryfikacja tożsamości jest możliwa, gdyż przeglądarka jest dystrybuowana z certyfikatami zaufanych centrów certyfikacji (CA), które to centra wystawiają certyfikaty SSL dla konkretnej witryny. Certyfikaty CA zainstalowane w przeglądarce dają możliwość stwierdzenia, czy certyfikat, którym przedstawia się witryna, został podpisany przez zaufaną stronę trzecią.

Łatwo zauważyć, że kluczowe jest tutaj zaufanie do dostawców oprogramowania (przeglądarek) oraz centrów certyfikacji. Niestety rzeczywiste przypadki pokazują, że nie zawsze możemy w pełni ufać stronom trzecim. W roku 2018 firma DigiCert (będąca CA) anulowała ponad 20 tys. certyfikatów SSL[14], po tym jak wyciekły klucze prywatne z nimi powiązane. Podobny przypadek odnotowano w roku 2011[15], lecz wówczas wyciekł klucz wykorzystywany do podpisywania certyfikatów

[13] „Infastruktura Klucza Publicznego", Wikipedia, https://pl.wikipedia.org/wiki/Infrastruktura_klucza_publicznego (dostęp 14.01.2020).

[14] Adam Haertle „Jaka piękna katastrofa...", Zaufana Trzecia Strona, https://zaufanatrzeciastrona.pl/post/jaka-piekna-katastrofa-czyli-czego-nie-robic-z-certyfikatami-ssl/ (dostęp 14.01.2020).

[15] Dennis Fisher „Final Report on DigiNotar Hack Shows Total Compromise of CA Servers", Threatpost.com https://threatpost.com/final-report-diginotar-hack-shows-total-compromise-ca-servers-103112/77170/ (dostęp 14.01.2020).

przez DigiNotar, co umożliwiło wygenerowanie sfałszowanych certyfikatów. W oparciu o te certyfikaty przeprowadzono szereg ataków typu *man-in-the-middle*[16] na użytkowników serwisów internetowych. W tym przypadku ślad prowadził w stronę wywiadu irańskiego, a także NSA. Nikogo nie skazano, a dostawcy przeglądarek wprowadzili certyfikaty DigiNotar na czarną listę. DigiNotar ogłosiło bankructwo w niedługim czasie po ujawnieniu incydentów.

Podsumowując, mechanizmy szyfrowania asymetrycznego są wykorzystywane do weryfikacji tożsamości, natomiast szyfrowanie symetryczne, w powiązaniu z algorytmami uzgadniania czy wymiany klucza (takim jak np. algorytm Diffiego-Hellmana), są wykorzystywane do szyfrowania kanałów komunikacyjnych – algorytmy asymetryczne są do tego celu za wolne (wymagają znacznych nakładów obliczeniowych). W przypadku algorytmów uzgadniania klucza dwie strony mogą ustalić wspólny klucz poprzez niezabezpieczony kanał komunikacyjny bez ryzyka ujawnienia go stronom trzecim, mającym możliwość podsłuchiwania wszystkich komunikatów. Wykorzystuje się do tego odpowiednią sekwencję ustalonych operacji matematycznych.

Jednakże i w przypadku stosowania algorytmów wymiany klucza nie możemy czuć się w pełni bezpieczni lub pewni, że nikt nas nie podsłuchuje – otóż w 2015 roku pokazano, że fakt, iż wiele implementacji algorytmu Diffiego-Hellmana używa tych samych liczb pierwszych, daje, w znacznej liczbie przypadków, agencjom dysponującym dużą mocą obliczeniową możliwość przeprowadzania ataku polegającego na wyliczeniu wartości klucza. Dodatkowo słabość w implementacji tego protokołu, wymuszona restrykcjami eksportowymi wprowadzonymi w latach 90. XX wieku przez USA, umożliwiała obniżenie długości liczb pierwszych używanych w tym protokole do 512 bitów. W ataku typu MITM (*man-in-the-middle*), czyli z udziałem „osoby" pośredniczącej, która może zmodyfikować początkowe komunikaty w trakcie negocjacji połączenia, podatność tę nazwano LOGJAM[17].

Stosowanie technik kryptograficznych ma za zadanie zapewnić poufność przesyłanych danych, natomiast to, jakie dane są przesyłane, zależy tylko i wyłącznie od użytkowników technologii. Mogą to być treści związane z finansami (np. dostęp do systemów bankowych), dane medyczne, dane stanowiące tajemnicę danej firmy, ale mogą to być również treści związane z działalnością przestępczą, terroryzmem.

[16] Atak typu *man-in-the-middle*, to atak, w którym osoba trzecia może przechwytywać i modyfikować dane przesyłane pomiędzy dwoma komunikującymi się stronami.
[17] „Weak Diffie-Hellman and the Logjam Attack", https://weakdh.org/ (dostęp 14.01.2020).

Innymi słowy, technologia ta służy zarówno zwykłym obywatelom, jak i przestępcom. Treści zaszyfrowanych zwykle nie można w prosty sposób filtrować czy przeglądać ich zawartości bez uprzedniego odszyfrowania, co komplikuje ochronę sieci korporacyjnych i infrastruktury sieciowej, a także może utrudniać działania policji i innym służbom śledczym. Notabene niektóre rządy (np. USA) nakładają w związku z tym embarga na transfery technologii wykorzystujących silne mechanizmy kryptograficzne – tak, aby służby mogły złamać szyfry w akceptowalnym czasie. W niektórych przypadkach w środowiskach korporacyjnych dokonuje się odszyfrowywania ruchu na firewallu i przeprowadza się klasyczną inspekcję zawartości pakietów, ale wymaga to odpowiedniej konfiguracji komputerów klienckich i całej infrastruktury sieciowej.

Stosowanie szyfrowanych kanałów komunikacyjnych ogranicza możliwość infiltracji różnych środowisk, ale nie wyeliminowuje tej możliwości w 100% – nadal można ustalić np. między jakimi adresami IP zestawione zostało połączenie lub kto do kogo i kiedy dzwonił, a co za tym idzie, zawęzić grono podejrzanych, jeśli transmisja lub rozmowa miała związek z działalnością przestępczą lub działalnością stanowiącą zagrożenie w oczach rządzących. W oparciu o logi połączeń czy dane billingowe nadal można próbować szukać powiązań pomiędzy komunikującymi się osobami. Oliwy do ognia dodaje fakt, że również biblioteki kryptograficzne mogą zawierać błędy umożliwiające ataki na komputery z nich korzystające i ich użytkowników. Wykryta w 2014 roku w bibliotece OpenSSL (jednej z najpowszechniej stosowanych bibliotek kryptograficznych na świecie) luka HeartBleed[18] umożliwiała zdalne pozyskanie fragmentów pamięci serwerów używających podatnej na ataki biblioteki. W pamięci można było znaleźć klucze prywatne i ciasteczka sesyjne użytkowników, co umożliwiało dalsze ataki. Błąd wykryto dopiero po dwóch latach od jego wprowadzenia do kodu źródłowego biblioteki. Kolejny błąd (POODLE[19]) w konstrukcji protokołu SSLv3 doprowadził do gwałtownego zaprzestania korzystania z niego. Atak w skrócie umożliwiał przejęcie sesji użytkowników.

Wracając do inwigilacji użytkowników, to nawet przy założeniu, że korzystamy z bezpiecznych bibliotek, możliwe jest analizowanie danych o połączeniach – adresy źródłowe i docelowe w protokole TCP/IP nie są szyfrowane. Dlatego, w celu zwiększenia stopnia prywatności (anonimizacji

[18] The Heartbleed Bug, http://heartbleed.com/ (dostęp 14.01.2020).

[19] „SSLv3 umarł. Zjadł go pudel.", Niebezpiecznik.pl, https://niebezpiecznik.pl/post/sslv3-umarl-zjadl-go-pudel/ (dostęp 14.01.2020).

informacji o połączeniach) i ograniczenia możliwości inwigilacji, wprowadzono szereg kolejnych, dodatkowych mechanizmów, do których zalicza się technologię wirtualnych sieci prywatnych (VPN). Została ona zaprojektowana głównie po to, by dać możliwość podłączania się do sieci korporacyjnych przez pracowników pracujących w terenie lub z domu, lecz szybko została zaadaptowana do celów związanych z ukrywaniem własnej tożsamości. W VPN cały ruch do określonych sieci jest przesyłany (tunelowany) przez pojedynczy host pośredniczący, do którego to hosta ruch odbywa się kanałem szyfrowanym. VPN jest dość często wykorzystywany do obchodzenia cenzury lub ukrywania źródeł ataku. W tych przypadkach zwykle wykorzystuje się serwery VPN umieszczone w sieciach, których operatorzy nie są skorzy do współpracy z organami ścigania i/lub znajdują się w innym kraju niż osoba prowadząca zabronioną działalność. Organy ścigania mają mocno ograniczone pole działania, jeśli atak pochodzi z kraju, z którym nie mają ustalonych procedur współpracy lub brak jest możliwości prawnych na podjęcie interwencji. W niektórych przypadkach wykorzystanie pojedynczego hosta pośredniczącego to za mało do skutecznego ukrycia prawdziwej tożsamości – znaczenie tu ma, gdzie znajdują się cele i źródła ataku i kto ma dostęp do danych o połączeniach. Poprzez korelację wolumenów ruchu, czasu i informacji o adresach źródłowych i docelowych operator może dokonać deanonimizacji połączeń.

W latach 90. XX wieku rozpoczęto pracę nad rozwiązaniami, które umożliwiłyby skuteczne ukrywanie tożsamości komunikujących się stron nawet przed operatorami mającymi możliwość monitorowania aktywności poszczególnych użytkowników sieci. W efekcie powstał Tor – system, który wykorzystuje szereg węzłów pośredniczących i mechanizmy szyfrowania asymetrycznego w protokole routingu, tak aby każdy węzeł znał tylko bezpośredniego poprzednika i następcę w łańcuchu połączeń. Informacje o wszystkich hostach pośredniczących są szyfrowane z użyciem algorytmów asymetrycznych, aby możliwe było przesłanie komunikatów zwrotnych. System jest wyposażony w dedykowaną przeglądarkę internetową (Tor Browser), która daje możliwość wyboru punktów wejścia i wyjścia z sieci Tor (np. wskazanie kraju), pozwalając na zachowanie anonimowości przy dostępie do zasobów internetowych lub omijanie ograniczeń terytorialnych. Ograniczenia terytorialne są często stosowane np. przez dostawców multimediów (wideo na żądanie (VOD), telewizja on-line). Dedykowana przeglądarka ma ograniczoną liczbę wtyczek, aby zminimalizować ryzyko ujawnienia oryginalnego adresu IP klienta, w szczególności

standardowo blokowany jest Flash i odtwarzacze multimediów, takie jak RealPlayer oraz Quicktime.

Teoretycznie Tor zapewnia dość dużą anonimowość, ale w niektórych scenariuszach istnieje możliwość zidentyfikowania osoby, która z niego korzysta. Dla przykładu na Harvardzie jeden ze studentów, łącząc się przez Tora, wszczął fałszywy alarm bombowy, wysyłając e-maila z jednorazowej skrzynki[20]. Pech chciał, że student, który to zrobił, był jedynym użytkownikiem, który łączył się z Torem z uniwersyteckiej sieci wi-fi w momencie wysłania zgłoszenia i stosunkowo łatwo udało się go namierzyć na podstawie logów uniwersyteckich systemów komputerowych. Student przyznał się do zarzucanych mu czynów[21].

Sieć Tor umożliwia również udostępnianie w sposób anonimowy stron internetowych[22]. Do tego celu przewidziano specjalny protokół (Onion Service Protocol), który umożliwia rejestrację usług w sieci Tor bez ujawniania własnej tożsamości. Udostępniana usługa otrzymuje identyfikator w specjalnej domenie .onion. W sieci Tor nie ma klasycznych wyszukiwarek internetowych, takich jak np. Google. Wymiana informacji o udostępnianych stronach odbywa się w taki sam sposób jak w początkowym okresie funkcjonowania Internetu, aczkolwiek pojawiają się katalogi stron tworzone mniej lub bardziej automatycznie. Anonimowość zapewniana przez sieć Tor powoduje, że ukryte zasoby, strony i usługi w niej udostępniane są często wykorzystywane przez przestępców i z tego względu noszą miano „ciemnej sieci" – Dark Web. W Dark Web można znaleźć zarówno treści, które są w pełni legalne, np. kluby książki czy portale informacyjne umożliwiające swobodną wymianę opinii w poczuciu pełnej wolności słowa, jak również cały szereg portali służących działalności przestępczej. Dla przykładu na portalach w Dark Web można uzyskać dostęp do skradzionych danych, takich jak hasła do przejętych kont na portalach, numery identyfikacyjne (np. Social Security Number), numery kart kredytowych. Istnieją tam również platformy, na których można nabyć nielegalne substancje, np. narkotyki, leki bez posiadania stosownej recepty oraz środki toksyczne. Ponadto dystrybuowane są tam również

[20] R. Brandom, „FBI agents tracked Harvard bomb threats despite Tor", https://www.theverge.com/2013/12/18/5224130/fbi-agents-tracked-harvard-bomb-threats-across-tor (dostęp 14.01.2020).

[21] P. Vogt, „That Bomb-Hoaxing Harvard Student Was Using Tor, But They Caught Him Anyway", https://www.wnyc.org/story/harvard-bomb-threat/ (dostęp 14.01.2020).

[22] K. Rankin„Tor Hidden Services", https://www.linuxjournal.com/content/tor-hidden-services (dostęp 14.01.2020).

treści zabronione, takie jak pornografia dziecięca czy mniej kontrowersyjne materiały chronione prawami autorskimi. Można zamówić ataki cybernetyczne, np. tzw. DDoS – ataki wykorzystujące sieci botnetów (zainfekowanych komputerów) w celu zalania dużym wolumenem ruchu serwisów będących celem ataku i przez to uniemożliwienie ich normalnego funkcjonowania. Z bardziej drastycznych zastosowań należy wymienić handel ludźmi czy handel organami do przeszczepów bądź świadczenie usług kryminalnych (płatne morderstwa, pobicia).

Rozkwit przestępczej działalności ułatwiają kryptowaluty[23] – wirtualne waluty bazujące na mechanizmach kryptograficznych i rejestrach rozproszonych, które miały dać społeczeństwom możliwość swobodnej wymiany kapitału i realizowanie płatności w sposób niezależny od jakichkolwiek rządów, instytucji regulujących przepływy finansowe czy operatorów kart płatniczych. Miały dać jednostkom swobodę handlu na arenie międzynarodowej bez konieczności uiszczania drakońskich opłat transakcyjnych, opłat za przelewy międzynarodowe czy uwzględniania różnic kursowych pomiędzy cenami kupna i sprzedaży (tzw. *spread*). Pierwszą i jednocześnie najszerzej rozpoznawalną kryptowalutą jest Bitcoin[24]. Intencje wprowadzenia tego rodzaju środkach płatniczego były dobre, ale kryptowaluty szybko zostały docenione przez przestępców i umożliwiły rozkwit nielegalnego handlu, stając się znakomitym uzupełnieniem sieci Dark Web. Zostały one również docenione przez twórców wirusów szyfrujących dyski i żądających okupu[25] (tzw. *ransomware*) – okup za odszyfrowanie dysku płaci się kryptowalutami. Początkowo entuzjastyczny stosunek do kryptowalut z czasem nieco osłabł – kryptowaluty zamiast szeroko trafić pod strzechy, stały się narzędziem w rękach spekulantów. Wprawdzie nadal się dużo o nich mówi i próbuje je wdrażać w sposób bardziej kontrolowany, ale ich adopcję znacznie utrudnia niejasny status legislacyjny. Co ciekawe, nad własną, globalnie stabilną kryptowalutą pracuje Facebook, ale w ostatnich miesiącach stracił wsparcie ze strony wiodących instytucji finansowych z grupy G20 oraz Visy i MasterCard[26].

[23] „Kryptowaluta", Wikipedia, https://pl.wikipedia.org/wiki/Kryptowaluta (dostęp 14.01.2020).

[24] Bitcoin, Bitcoin.org, https://bitcoin.org/pl/jak-to-dziala (dostęp 14.01.2020).

[25] Michael Baker, „How Cryptocurrencies Are Fueling Ransomware Attacks And Other Cybercrimes", Forbes, https://www.forbes.com/sites/forbestechcouncil/2017/08/03/how-cryptocurrencies-are-fueling-ransomware-attacks-and-other-cybercrimes/ (dostęp 14.01.2020).

[26] Leo Jakobson, „With stablecoin ban, G20 deals Facebook's Libra ambitions another blow", https://modernconsensus.com/regulation/with-stablecoin-ban-g20-deals-facebooks-libra-ambitions-another-blow/ (dostęp 14.01.2020).

Mniej kontrowersji wzbudza technologia wywodząca się z kryptowalut, a mianowicie technologia *blockchain* (łańcuch bloków). Technologia *blockchain* umożliwia tworzenie rozproszonych, redundantnych rejestrów i odnotowywanie wszelkich zmian wprowadzanych do składowanych w nich danych. Rejestry tworzone z użyciem technologii *blockchain* powinny być niemutowalne – raz dodany blok powinien pozostawać niezmieniony, dlatego próbuje się je stosować do implementacji rejestrów, które z założenia przechowują dane permanentnie (np. księgi katastralne). Problem jednak w tym, że w przypadku przejęcia lub wprowadzenia do systemu wystarczająco dużej liczby węzłów (w przypadku Bitcoina jest >50% mocy obliczeniowej) można zmodyfikować bloki, które już się w łańcuchu bloków znajdują. Kolejnym problemem jest permanentne przechowywanie wszystkich bloków, co może w niektórych zastosowaniach rodzić problemy z ochroną danych osobowych i praw jednostek. Dość poważnym zarzutem kierowanym w kierunku tej technologii jest także jej ślad energetyczny i rozmiar wolumenów dyskowych (te same dane są zduplikowane na wielu węzłach). Warto jednak zaznaczyć, że mimo swoich ograniczeń *blockchain* pozostaje obiecującą technologią o dużym potencjale.

Przejdźmy teraz do innego rodzaju zagrożenia, a mianowicie wycieków danych czy przejmowania systemów na skutek błędów w aplikacjach, usługach czy systemach operacyjnych. Popełnianie błędów jest rzeczą ludzką i programiści, projektanci oraz administratorzy systemów informatycznych nie są tutaj wyjątkiem. W efekcie dochodzi do znajdywania w systemach luk, które czynią je podatnymi na ataki, umożliwiając dla przykładu przejęcie kont użytkowników lub kradzież danych składowanych w systemie (w tym np. skrótów haseł bądź wręcz całych haseł). M.in. z tego względu zaleca się stosowanie różnych haseł do różnych portali. Błędy występują również w oprogramowaniu klienckim, np. w przeglądarkach internetowych czy ich wtyczkach (np. Flash czy Java), i umożliwiają infekcję komputera w przypadku wejścia na specjalnie spreparowaną stronę. Podatności w oprogramowaniu biurowym mogą również zostać wykorzystane do przejęcia komputera – wystarczy, że użytkownik otworzy specjalnie spreparowany załącznik do e-maila. Współczesne edytory tekstów, jak np. Microsoft Word, umożliwiają stosowanie automatyzacji w postaci makr lub osadzanie bardziej złożonych obiektów, co rozszerza spektrum potencjalnych scenariuszy ataków. Podatności w przeglądarkach internetowych umożliwiały wykorzystanie do infekcji komputerów nawet plików graficznych, takich jak np. jpg. Co ciekawe, podatności w systemach zarządzania treścią na serwerach i oprogramowaniu klienckim niekiedy

bywają wykorzystywane przez cyberpolicję – dobrym przykładem jest tu akcja wymierzona przeciwko pedofilom, przeprowadzona przez policję holenderską. Policjanci przejęli forum w Dark Web i zainfekowali je własnym trojanem, który automatycznie instalował się na komputerach przestępców je odwiedzających. Operacje nosiła kryptonim „torpedo"[27]. Warto wspomnieć, że dla zwykłych użytkowników Internetu zagrożenie stanowią również firmy świadczące usługi tak zwanego „kuloodpornego" hostingu („bulletproof" hosting), który daje możliwość hostowania serwerów z praktycznie dowolną nielegalną zawartością (choć tu niektóre firmy wprowadzają pewne ograniczenia przynajmniej w oficjalnych regulaminach) i podejmowania z nich działań przestępczych. Firmy świadczące tego typu usługi starają się skutecznie utrudniać pracę policji, ale i w walce z nimi służby odnoszą sukcesy, co pokazuje akcja niemieckiej policji z września 2019 roku[28].

Wśród użytkowników Internetu wzrasta świadomość zagrożeń wynikających z używania niewłaściwie zabezpieczonego sprzętu lub oprogramowania podatnego na ataki. Warto zauważyć, że możliwość wystąpienia błędu czyniącego oprogramowanie podatnym na atak jest trudna do uniknięcia, można co najwyżej ograniczać ryzyko wystąpienia takich błędów. Oprogramowanie jest tworzone przez zespoły programistyczne o różnych kwalifikacjach, często w sposób modularny i naturalną (typowo ludzką) rzeczą jest, że w implementacjach pojawiają się błędy, które wykrywane są już po powszechnym wdrożeniu produktu i integracji niezależnych modułów. Zatem to, co można robić, to dostarczać mechanizmy pozwalające na właściwe adresowanie problemów bezpieczeństwa w krótkim czasie. Do tego służą systemy automatycznych aktualizacji. Dzięki tym systemom ograniczamy możliwość ataku na nasze zasoby, ale jednocześnie dajemy dostawcom możliwość oprogramowania dystrybucji dowolnych kodów, które mogą w pewnym momencie (np. konflikt militarny) zostać wykorzystane przeciwko nam. Zdarza się również, że nowe aktualizacje jednego producenta nie są w pełni kompatybilne z użytkowanym przez nas oprogramowaniem innego lub nawet tego samego producenta. Idea zatem jest jak najbardziej właściwa, ale w niektórych zastosowaniach należy zachować ostrożność. Warto tu przywołać rok 2016 i skandal z oprogramowaniem do zdalnej aktualizacji firmware-u (z ang. FOTA – *Firmware Over The Air*) na telefonach

[27] Operacja torpedo, https://www.wired.com/2014/08/operation-torpedo/ (dostęp 14.01.2020).
[28] Brian Krebs „German Cops Raid „Cyberbunker 2.0," Arrest 7 in Child Porn, Dark Web Market Sting" https://krebsonsecurity.com/2019/09/german-cops-raid-cyberbunker-2-0-arrest-7-in-child-porn-dark-web-market-sting/ (dostęp 14.01.2020).

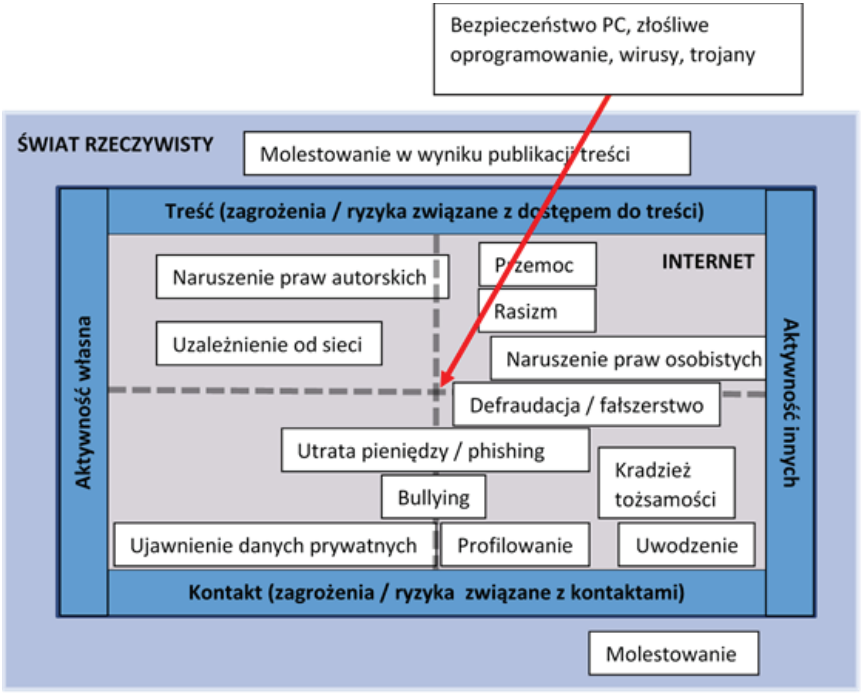
komórkowych, który pokazał, że niekiedy systemy automatycznej aktualizacji mogą ujawniać więcej danych, niż byśmy sobie tego życzyli. W tym przypadku dostawca oprogramowania do aktualizacji, tj. chińska firma ADUPS, zbierała m.in. dane o identyfikatorach stacji bazowych, do których telefon się łączył, połączeniach, a także zawartości wiadomości SMS. Oprogramowanie było wykorzystywane na ponad 150 modelach telefonów sprzedawanych na całym świecie, aczkolwiek początkowo mówiono tylko o urządzeniach firmy BLU (dystrybuowanych m.in. przez Amazona). Do czego firma wykorzystywała te dane w praktyce nie wiadomo, przy czym w oficjalnym komunikacie, opublikowanym po ujawnieniu problemu, zastrzega, że nie dzieliła się tymi danymi z firmami trzecimi ani agencjami rządowymi. W przypadku systemów automatycznej aktualizacji, podobnie jak w przypadku systemów chmurowych czy platform usługowych i społecznościowych, pojawia się kwestia zaufania – komu ufamy i jakie dane mu powierzamy.

Inwencja cyberprzestępców w tworzeniu nowych ataków i kreatywne wykorzystywanie wszystkich dostępnych, często z pozoru niegroźnych, zasobów bywa zaskakująca, co pokazują wolumenowe ataki wielkoskalowe (typu DRDoS) poważnie zakłócające pracę operatorów sieci i serwisów internetowych. Dla przykładu do przeprowadzenia dużego ataku na portal KrebsOnSecurity wykorzystano botnet (zwany Mirai), stworzony z niezabezpieczonych kamer podłączonych do sieci Internet[29]. Do ataków na sieć Sony PlayStation i Microsoft (serwisy związane z Xbox-em) wykorzystano routery domowe, które miały „dziurawe" oprogramowanie układowe (*firmware*)[30]. W amplifikacji ataków powszechnie wykorzystuje się również popularne serwery usług, np. serwery nazw, serwery czasu (NTP) czy serwery usług katalogowych (LDAP). Najłatwiej do tego wykorzystać serwery, które operują w oparciu o protokół UDP, gdyż w ich przypadku istnieje możliwość sfałszowania adresu nadawcy, który odpowiada adresowi serwera ofiary. Ofiara (serwer) zostaje zalana odpowiedziami, których się nie spodziewa i w krytycznym przypadku dochodzi do wysycenia łącza lub zasobów, co prowadzi do niedostępności usługi.

[29] B. Kerbs, „Study: Attack on KrebsOnSecurity Cost IoT Device Owners $323K", https://krebsonsecurity.com/2018/05/study-attack-on-krebsonsecurity-cost-iot-device-owners-323k/ (dostęp 14.01.2020).

[30] Ch. Brook, „Lizard Squad's DDoS-For-Hire Service Built on Hacked Home Routers" https://threatpost.com/lizard-squads-ddos-for-hire-service-built-on-hacked-home-routers/110341/ (dostęp 14.01.2020).

Łatwo zauważyć, że większość niebezpieczeństw i zagrożeń nie wynika z samej technologii, a z niewłaściwego jej wykorzystywania przez osoby o złych intencjach oraz w mniejszym stopniu od czynników losowych (np. awarie, katastrofy naturalne, wypadki). Biorąc ten aspekt pod uwagę, możemy zdefiniować katalog zagrożeń przez pryzmat kilku podstawowych czynników, to jest: treści, które publikujemy, konsumujemy lub przesyłamy; kontaktów, które nawiązujemy przy pomocy Internetu; oraz aktywności naszej i cudzej. Klasyfikację zagrożeń opartych na tych trzech czynnikach nazywa się modelem 3Cs (ang. *content* (treść), *contact* (kontakt), *condact* (postępowanie)). Model ten pozwala podejść metodycznie do charakterystyki zagrożeń (por. rys. 1), na które są narażeni użytkownicy Internetu i stosuje się go zwłaszcza w kontekście korzystania z sieci przez osoby małoletnie.



Rys. 1. Model klasyfikacji zagrożeń 3Cs

(źródło: I.R. Berson, M.J. Berso, „High-tech Tots: Childhood in a Digital World", Information Age Publishing, 2010.)

Katalog zagrożeń obejmuje takie aspekty, jak: *bullying*, czyli znęcanie się czy zastraszanie najczęściej przez grupę rówieśniczą; uwodzenie i molestowanie, w tym wykorzystanie nieletnich; naruszanie praw osobistych, oszczerstwa, mowa nienawiści; rasizm; nawoływanie do przemocy; narażenie na oglądanie treści niedostosowanych do wieku; malwersacje, oszustwa, w tym *phishing* i kradzieże tożsamości, podszywanie się; utrata prywatności; kradzieże praw majątkowych, np. praw autorskich.

W tym kontekście niestety należy ze smutkiem stwierdzić, że największym zagrożeniem w cyberświecie nie jest technologia, a drugi człowiek. Cyberświat jest lustrzanym odbiciem świata rzeczywistego, przy czym w tym odbiciu zarówno aspekty pozytywne, jak i negatywne ulegają wyjaskrawieniu. Na szczęście części zagrożeń możemy unikać, podobnie jak w świecie rzeczywistym, nie szukając miejsc, w których nie chcielibyśmy się znaleźć, zachowując swoistą higienę (nie dotykamy i nie ściągamy wszystkiego „jak leci") i traktując innych internautów tak jak sami chcielibyśmy być traktowani. Internet stanowi medium, w którym znajdziemy wiele pozytywów. Internet pozwala nam na szybsze załatwienie rozmaitych codziennych spraw, jak np. płatności za rachunki, rozliczenia, zakupy, rezerwacje wakacyjnych wojaży i noclegów. Listę można by ciągnąć niemal w nieskończoność, ale dodam jeszcze tylko jeden istotny aspekt – a mianowicie technologie ułatwiają nam pozostawanie w kontakcie z ważnymi dla nas, najczęściej bliskimi nam, osobami. A dzięki kryptografii możemy to robić niemal pewni, że treści, które wymieniamy, mogą pozostać między nami (no i może niektórymi służbami lub operatorami naszych skrzynek pocztowych, jeśli godzimy się na utratę części prywatności, korzystając z ich usług).

Korzystajmy z technologii w dobrych celach i przeciwstawiajmy się agresji oraz próbom zawłaszczania naszego wirtualnego i rzeczywistego świata przez przestępców czy innych agresorów.