VOL. 54 STUDIA POLITOLOGICZNE
DOI: 10.33896/SPolit.2019.54.10

Paweł Tomczyk
ORCID: 0000-0002-4983-5864
Daniel Mider
ORCID: 0000-0003-2223-5997
Józef Grzegorczyk
ORCID: 0000-0001-5348-3737

Inwigilacja elektroniczna jako metoda pozyskiwania informacji – ewaluacja i prognozy

Słowa kluczowe:
społeczeństwo nadzoru, informatyka społeczna, inwigilacja elektroniczna, infobrokering

STUDIA I ANALIZY

Wprowadzenie

W dyskursie filozoficznym wiedza bywa utożsamiana z władzą. Dla Michela Foucaulta te dwa pojęcia są kluczowe dla rozumienia rzeczywistości i nierozdzielne do tego stopnia, że ukuł pojęcie „wiedzy-władzy". Pojmował te kategorie jako nierozłączne: „Ani władza nie może być praktykowana bez wiedzy, ani wiedza nie może nie płodzić władzy"[1].

Pomimo że koncepcja ta została wyłożona na początku lat 70. ubiegłego wieku[2], to intensywny rozwój technologii informacyjnych, a w szczególności środków komunikowania elektronicznego sprawił, że refleksje M. Foucaulta pozostają w niekwestionowany sposób aktualne. Współczesny status informacji jest nie do przecenienia – jest to szczególne

[1] M. Foucault, *Gry władzy*, przekł. T. Komendant, „Literatura na Świecie" 1988, nr 6, s. 319.

[2] Tenże, *Historia seksualności*, przekł. B. Banasiak, T. Komendant, K. Matuszewski, Gdańsk 2010; tenże, *Nadzorować i karać*, przekł. T. Komendant, Warszawa 1998.

dobro niematerialne równoważne lub cenniejsze od dóbr materialnych, w myśl reguł wyłożonych w *Zmianie władzy* Alvina Tofflera[3]. Intensywny rozwój technologii informacyjnych doprowadził do ujawnienia się lub zintensyfikowania licznych negatywnych zjawisk, których induktorem jest łatwość pozyskiwania i dystrybucji informacji z użyciem urządzeń elektronicznych. Technologie informacyjne zamknęły współczesne społeczeństwa w swoistym więzieniu opisywanym wprost w koncepcji społeczeństwa nadzorowanego (*surveillance society*) lub alegorycznie w koncepcji Panoptykonu[4]. Taki status informacji we współczesnych społeczeństwach sprawia, że staje się ona centralną kategorią analityczną, bez której niemożliwe jest zrozumienie relacji społecznych, w tym relacji władzy.

Inwigilacja ma obecnie charakter powszechny, stała się nieodłącznym elementem krajobrazu współczesnych społeczeństw, co skłoniło do charakteryzowania ich jako *„eavesdropping societies"* („społeczeństwa podsłuchu")[5]. Niniejszy artykuł ogniskuje się na jednym z elementów przynależnych społeczeństwu nadzorowanemu – inwigilacji z użyciem narzędzi elektronicznych. Autorzy podejmują w nim próbę odpowiedzi na szereg następujących pytań. Po pierwsze, jakie typy negatywnych zjawisk są wytwarzane i intensyfikowane przez technologie inwigilacji elektronicznej? Po wtóre, jak głęboki jest stan „bezbronności inwigilacyjnej" współczesnych społeczeństw, to jest jakie są możliwości urządzeń służących inwigilacji? Po trzecie, czy istnieje możliwość praktycznego przeciwstawienia się im, a jeśli tak – w jaki sposób i jakie są tego granice? Po czwarte, jaka jest geneza tych zjawisk i jakie spodziewane scenariusze przyszłości można szkicować na podstawie antycypacji zaobserwowanych trendów? Tak zdefiniowany zbiór pytań badawczych wymaga oglądu zarazem z dwóch perspektyw: socjologicznej i technicznej.

---

[3] A. Toffler, *Zmiana władzy. Wiedza, bogactwo i przemoc u progu XXI stulecia*, przekł. P. Kwiatkowski, Poznań 2003.

[4] O. Gandy, *Data Mining and Surveillance In the Post – 9/11 Environment*, [w:] K. Ball, F. Webster (red.), *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Era*, Londyn 2003; D. Lyon, *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis 1994; G.T. Marx, *The Surveillance Society: the Threat of 1984-style Techniques*, „The Futurist" 1985, nr 6; B. Simon, *The Return of Panopticism: Supervision, Subjection and the New Surveillance*, „Surveillance & Society" 2005, nr 3(1).

[5] K. Reis, *The Eavesdropping Society. Electronic Surveillance and Information Brokering*, „Patents, Copyrights, Trademarks, and Literary Property", June 2001.

Rozważania definicyjne

Łaciński źródłosłów tytułowego pojęcia „inwigilacja" – *invigilare* – dosłownie oznacza „czuwanie nad czymś", lecz takie rozumienie wydaje się zbyt oględne, ogólnikowe i przez to nietrafne. Pojęcie inwigilacji wykazuje pokrewieństwo z pojęciem podsłuchu, przy czym jest odeń szersze. Podsłuch stanowi szczególną formę inwigilacji: akustyczną z użyciem urządzeń elektronicznych i ukrytą, to jest bez wiedzy i autoryzacji poddanych podsłuchowi. Z technicznego punktu widzenia używa się do tego celu specjalistycznych elektronicznych urządzeń, jak na przykład miniaturowych mikrofonów, mikrofonów kierunkowych, zazwyczaj połączonych z cyfrowymi rejestratorami, wzmacniaczami lub z nadajnikami radiowymi[6]. Uprawnienia do stosowania inwigilacji (tzw. kontroli operacyjnej) mają w Polsce służby dyspozycyjne cywilne i wojskowe[7], a jak pokazuje praktyka detektywistyczna, podsłuchy stosują powszechnie podmioty drugiego sektora, a także osoby prywatne. Rodzime prawodawstwo konstytuuje trzy kategorie podsłuchu: procesowy, operacyjny i prywatny[8]. Pierwszy z wymienionych – podsłuch procesowy regulowany jest przez kodeks postępowania karnego (roz. 26, art. 237–242, dalej kpk)[9], w którym określone zostały warunki kontroli i utrwalania rozmów – telefonicznych i innych – lub przekazów informacji, w tym przesyłanych drogą elektroniczną. Kontrolę taką ordynuje prokurator za zgodą sądu albo uprzednią, albo w przypadkach niecierpiących zwłoki – następczą (co oznacza konieczność wystąpienia do sądu o zatwierdzenie samodzielnej decyzji w ściśle określonym terminie trzech dni). Może być ona prowadzona do trzech miesięcy, z możliwością jej przedłużenia na kolejne trzy miesiące.

Prawodawstwo precyzyjnie definiuje przypadki, gdy taki środek pozyskiwania dowodów jest legalny. Kontroli rozmów podlega wyłącznie

---

6 M. Pečenka i in., *Encyklopedia szpiegostwa*, przekł. K. Wojciechowski, Warszawa 1995, s. 202.

7 Są to: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, Centralne Biuro Antykorupcyjne, Krajowa Administracja Skarbowa, Policja, Służba Kontrwywiadu Wojskowego, Służba Ochrony Rządu, Służba Wywiadu Wojskowego, Straż Graniczna, Żandarmeria Wojskowa.

8 Por. M. Rogalski, *Kontrola i utrwalanie rozmów w procesie karnym*, „Prokuratura i Prawo" 2017, nr 6; K. Marszał, *Podsłuch w polskim procesie karnym* de lege lata *i* de lege ferenda, [w:] *Problemy nauk penalnych. Prace ofiarowane Pani Profesor Oktawii Górniok*, Katowice 1996, s. 343.

9 Ustawa z 6 czerwca 1996 r. – Kodeks postępowania karnego (t.j. Dz.U. z 2018 r., poz. 1987, ze zm.).

podejrzany, oskarżony lub pokrzywdzony, gdy istnieje domniemanie, iż mogą kontaktować się z nim dwie pierwsze kategorie wymienionych. Podsłuchowi może również podlegać osoba mogąca mieć związek ze sprawcą lub z grożącym przestępstwem. Kontrola jest możliwa wyłącznie wówczas, gdy toczące się postępowanie bądź uzasadniona obawa popełnienia nowego przestępstwa dotyczy między innymi zabójstwa, narażenia na niebezpieczeństwo powszechne lub sprowadzenia katastrofy, zamachu stanu, handlu ludźmi, stręczycielstwa, kuplerstwa i sutenerstwa, płatnej protekcji, łapownictwa, wymuszenia rozbójniczego lub rozboju, szpiegostwa lub odnosi się do mienia znacznej wartości (art. 237 § 3 kpk). Warto podkreślić, iż choćby zebrano dowody dotyczące innych przestępstw lub osób niż wymienione, to w świetle prawa procesowego takie dowody są bezużyteczne. Analogicznie skonstruowane są procedury podjęcia podsłuchu operacyjnego, z tym że reguluje go inny akt prawny – ustawa o policji (art. 19)[10]. Zarządzić takie działania jest władny sąd okręgowy na wniosek Komendanta Głównego Policji / komendanta wojewódzkiego, który uprzednio uzyskał w tej sprawie zgodę Prokuratora Generalnego lub odpowiednio prokuratora okręgowego. Czynności operacyjno-rozpoznawcze można stosować w celach zapobiegawczych, wykrywania, ustalania sprawców oraz uzyskania i utrwalenia dowodów ściganych z oskarżenia publicznego. Trzecia z kategorii to podsłuch prywatny. Jest on legalny, jeśli rejestracji podlega rozmowa, w której uczestniczy prowadzący rejestrację rozmowy. Nielegalność orzeka się, gdy posługując się urządzeniem podsłuchowym stosuje się je dla pozyskania informacji, do której uzyskania nie jest się uprawnionym (art. 267 § 3 kodeksu karnego)[11]. Wykorzystanie dowodów pochodzących z podsłuchu prywatnego nie jest w polskim prawodawstwie wprost zakazane, a więc nie obowiązuje doktryna „owoców zatrutego drzewa"[12]. Niektóre jednak orzeczenia odnoszą się do tej zasady krytycznie. Wskazuje się, że użyty podstęp godzi w konstytucyjną zasadę swobody i ochrony komunikowania się, a dowody tak zebrane nie powinny być dopuszczane w postępowaniu cywilnym[13]. Warto też podkreślić stosowanie działań wywiadowczych bez dbania o wyżej wymienione reguły przez wywiady obcych państw oraz kategorię wywiadu gospodarczego.

---

[10] Ustawa z 6 kwietnia 1990 r. o policji (t.. Dz.U. z 2019 r. poz. 161, ze zm.).

[11] Ustawa z 6 czerwca 1997 r. – Kodeks karny (t.j. Dz.U. z 2018 r. poz. 1600, ze zm.).

[12] Zasada ta po raz pierwszy pojawiła się w orzecznictwie Sądu Najwyższego USA (sprawa Nardone v. USA z 1939 r.).

[13] Takie stanowisko zajął np. Sąd Apelacyjny w Poznaniu (wyrok z 10.01.2008 r., I ACa 1057/07) oraz Sąd Apelacyjny w Warszawie (orzeczenie z 6.07.1999 r., I ACa 380/99).

Takie rozumienie pojęcie, choć specjalistyczne, wydaje się nazbyt wąskie na potrzeby niniejszego tekstu, jednocześnie nie uwzględniając aktualnego stanu rozwoju techniki – w szczególności urządzeń rejestrujących obraz czy przechwytujących komunikację elektroniczną (*via* Internet). Zatem na potrzeby niniejszego tekstu pojęcie inwigilacji będzie rozumiane jako przechwytywanie i utrwalanie obrazu, dźwięku lub treści dokumentów elektronicznych w sposób ukryty, to jest bez wiedzy i/lub zgody podmiotu kontrolowanego. Drugi człon związku frazeologicznego – „elektroniczna" odnosi się do technik rejestracji za pomocą zarówno specjalistycznych, jak i amatorskich urządzeń elektronicznych.

Technologiczny potencjał inwigilacji elektronicznej – przegląd autorski

Analiza technicznych aspektów inwigilacji elektronicznej oraz zasad i sposobów realizacji podsłuchów ma kluczowe znaczenie: uświadamia jej współczesne możliwości oraz łatwość naruszania prywatności. Potencjał środków inwigilacji trafnie określają ich rozmaite typologie. Elementarną kategoryzację urządzeń służących inwigilacji można utworzyć na podstawie schematu typowego systemu podsłuchowego, składającego się z trzech głównych elementów: punktu nadawczego / rejestratora, linii przesyłowej oraz punktu odbiorczego.

PUNKT NADAWCZY / REJESTRATOR

Punkt nadawczy można scharakteryzować z użyciem następujących parametrów: typ rejestrowanego przekazu, rodzaj zastosowanego kamuflażu, sposób i miejsce umieszczenia urządzenia w miejscu poddawanym inwigilacji, czas działania oraz sposób aktywacji urządzenia.

- Typ rejestrowanego przekazu – wydaje się najistotniejszym parametrem charakteryzującym punkt nadawczy. Wyróżnić można: urządzenia rejestrujące dźwięk otoczenia (podsłuchy klasyczne – i jako takie – najliczniejsze); urządzenia przechwytujące obraz bądź w formie statycznej (fotografie – nazywamy je fotopułapkami), bądź jako obraz dynamiczny (nagranie filmowe); urządzenia (lub programy) przechwytujące aktywność na urządzeniach komputerowych (uderzenia klawiszy, obraz, w tym metadane, jak na przykład przebieg aktywności użytkownika lub ruch w sieci); urządzenia (lub programy) przechwytujące komunikację telefoniczną (zarówno telefonii stacjonarnej i mobilnej). Rejestrowane są także inne typy

przekazu. Na przykład wszystkie oferowane na rynku fotopułapki i wiele kamer służących do dyskretnej inwigilacji mają wbudowany czujnik ruchu (PIR – *Passive Infra Red*) o zasięgu do parudziesięciu metrów. Z kolei większość nowszych kamer służących inwigilacji zaopatrzona jest w oświetlacz/reflektor podczerwieni pozwalający na prowadzenie rejestracji w nocy lub w innych oświetleniowo niesprzyjających warunkach (oświetlacze IR wbudowane w kamery zazwyczaj umożliwiają obserwację w odległości do kilku–kilkunastu metrów, a zewnętrzne, profesjonalne reflektory IR pozwalają na zwiększenie tego dystansu nawet do jednego kilometra). Dodatkowym kryterium podziału w ramach analizowanego aspektu jest wydzielenie dwóch grup urządzeń: profesjonalnych i pozostałych (amatorskich), przy czym różnice te mają istotne znaczenie dla jakości rejestrowanego przekazu.

- Rodzaj kamuflażu – może być rozumiany jako wizualna charakterystyka urządzenia nadawczego uniemożliwiająca lub utrudniająca odkrycie jego przeznaczenia. Urządzenia mogą wymagać – lub nie – dokonania samodzielnych zabiegów ich ukrywania. W pierwszym przypadku konieczne jest umieszczanie ich w takiej lokalizacji, która umożliwia skuteczną inwigilację, a jednocześnie stanowi zabezpieczenie urządzenia przed wykryciem. Parametrem wspomagającym, to jest utrudniającym wykrycie, jest miniaturyzacja urządzenia. Rozwiązania i możliwości wyboru zakamuflowanych urządzeń są nader bogate. Przykładowo na cywilnym rynku dostępne są liczne modele urządzeń podsłuchowych ukrytych przykładowo w: pendrivie, długopisie, zapalniczce, żarówce, czujniku dymu, listwie przepięciowej (przedłużacz i rozgałęźnik), sieciowej ładowarce samochodowej, karcie płatniczej, płycie CD wraz z opakowaniem. Takie urządzenia bardzo łatwo pozostawić w inwigilowanym pomieszczeniu, nie wzbudzając niczyich podejrzeń – na przykład podmieniając oryginalne przedmioty, darowując je lub pozostawiając, rzekomo z roztargnienia. Ceny takich urządzeń wahają się od kilkuset do kilku tysięcy złotych. Tworzone są również bardziej profesjonalne rozwiązania – podsłuchy umiejscawiane w odpowiednich statuetkach lub innych przedmiotach pamiątkowych wręczanych osobie przewidzianej do inwigilowania. Z kolei kamery wraz z mikrofonami w gotowych produktach inwigilacyjnych przykładowo kamuflowane są jako: piloty TV, latarki, zasilacze sieciowe, czujniki ruchu czy przeciwpożarowe, okulary i inne części garderoby (guziki, krawaty). Stosunkowo dobrze rozwinięty jest pod tym względem rynek urządzeń komputero-

wych[14] – dostępne są keyloggery (to jest urządzenia zapisujące znaki wybierane na klawiaturze przez osobę inwigilowaną) w postaci gotowych klawiatur lub adapterów (przejściówek USB/PS2), a także urządzeń sczytujących obraz z ekranu monitora montowanych pomiędzy nim a jednostką centralną jako adapter DVI/HDMI/VGA (urządzenia takie określa się mianem *frame-grabber*, jednym z przykładów jest kosztujący kilkaset złotych VideoGhost). Typ kamuflażu może być również rozpatrywany jako charakterystyka techniczna urządzenia rozumiana jako ekranowanie elektromagnetyczne urządzenia. Zasadniczo w istotny sposób potencjał ulotu informacji w wyniku elektromagnetycznej emisji ujawniającej redukuje fakt umieszczenia urządzenia w innym urządzeniu elektronicznym.

- Sposób ulokowania – to kolejny parametr urządzenia inwigilującego, a determinowany jest przez liczne zmienne: posiadanie kamuflażu lub jego brak, sposób zasilania, sposób przesyłania informacji do punktu odbiorczego, zasięg jego działania, konieczność jego zabrania po wykonaniu zadania, możliwość celowego lub przypadkowego wykrycia bądź zniszczenia. Pierwszą z przesłanek stanowi konieczność zapewnienia odpowiednio wysokiej jakości zbieranej informacji, co wymusza umieszczenie urządzenia w bezpośrednim sąsiedztwie obiektu inwigilowanego (na przykład urządzenie podsłuchowe powinno znajdować się w jak najbliższej odległości od miejsca rozmów, a urządzenie rejestrujące obraz nigdy bezpośrednio naprzeciwko okna). Po wtóre, urządzenia należy lokować z dala od źródeł zakłóceń dźwiękowych i/lub wizualnych. Po trzecie, nie należy umieszczać urządzeń przekazujących informację drogą radiową w miejscach ekranowanych (na przykład aluminiowych obudowach lub stalowych szafkach).
- Czas działania urządzenia – jest zależny przede wszystkim od możliwości zapewnionego zasilania, wtórnie zaś od zapotrzebowania energetycznego wyznaczanego przez typ rejestrowanego przekazu oraz sposobu komunikacji urządzenia nadawczego z urządzeniem odbiorczym. Zasadniczo wyróżniamy urządzenia z zasilaniem własnym oraz zasilaniem zewnętrznym. Pierwszy typ ma ograniczony czas działania, drugi zaś – potencjalnie nieograniczony. Zasilanie własne wykorzystuje baterie lub akumulatory umożliwiające nieprzerwane

[14] Istnieją liczne możliwości inwigilacji komputerów bez użycia sprzętu wymagającego dostarczenia i instalacji w miejscu znajdowania się komputera. Zagadnienie to jest jednak zbyt obszerne jak na wymagania objętościowe niniejszego tekstu.

działanie od około kilku do nawet kilkudziesięciu godzin (dla podsłuchów). Z kolei niektóre nowe fotopułapki mogą działać w stanie uśpienia bezobsługowo nawet kilka miesięcy (na przykład model LTL Acorn 6511WMG). Za bezpieczną w kontrinwigilacyjnej praktyce przyjmuje się powszechnie półroczną cezurę – po upływie tego czasu uznaje się baterię w potencjalnym podsłuchu za rozładowaną. Stąd wynika reguła biznesowego bezpieczeństwa umieszczania wszelkich nowych przedmiotów w przestrzeni neutralnej (najlepiej w pomieszczeniu, gdzie nie prowadzi się poufnych rozmów, jak gablota znajdująca się w korytarzu) na wskazany półroczny okres. Urządzenia mające zewnętrzne źródło zasilania można podzielić na takie, do których zasilanie zostało doprowadzone za pomocą kabla (rzadziej stosowane, wymagające bezpośredniego dostępu do miejsca w celu przeprowadzenia montażu), wbudowane w urządzenie mające zasilanie (na przykład keylogger montowany w obudowie klawiatury) lub takie, które same stanowią źródła zasilania (podsłuchy montowane w gniazdach elektrycznych – w elektroinstalacyjnych puszkach) oraz dołączane do źródła zasilania (jak pendrive USB z podsłuchem, rozgałęźnik z gniazdami elektrycznymi, żarówka zawierająca podsłuch, odświeżacz powietrza wpinany do gniazda elektrycznego).

- Sposób działania urządzenia – podstawowe rodzaje to urządzenia działające w sposób ciągły oraz te wzbudzane impulsami: dźwiękowymi (rozmowa), świetlnymi (włączenie światła) lub innymi (na ogół jest to ruch, jak na przykład w rejestratorze PV-TM10FHD zawierającym czujnik ruchu – całość ukryta została w wielofunkcyjnym zegarku).

LINIA PRZESYŁOWA

Przegląd wariantów przesyłania informacji z urządzenia nadawczego do urządzenia odbiorczego ukazuje różnorodność i możliwości współczesnych urządzeń inwigilujących dostępnych na cywilnym rynku. Aktualnie stosowane są następujące sposoby transmisji sygnału z urządzenia inwigilującego: radiowe (w tym GSM, Wi-Fi, Bluetooth), elektromagnetyczne (w tym podczerwień bliska i średnia), przewodowe (w podziale na medium własne, medium obce), zdalne (laserowe, sejsmiczne/kontaktowe, mikrofony kierunkowe), sieć Internet.

Transmisja radiowa ma największy zasięg, jednak jest stosunkowo łatwa do wykrycia, ponadto wymaga ustawienia punktu odbiorczego w promieniu zasięgu nadajnika. Obecnie najpopularniejsza jest transmisja zgodna ze standardem telefonii komórkowej (GSM oraz trans-

misji danych)[15]. Urządzenie zaopatrzone jest w moduł GSM, działając analogicznie jak telefon komórkowy, wymagając karty SIM i korzystając z infrastruktury operatorów sieci telefonii komórkowej. Transmisja oparta na GSM ma największy zasięg. W innym wypadku wymaga ustawienia punktu odbiorczego w zasięgu działania urządzenia, przeważnie do kilkuset metrów. Pierwotnie urządzenia służące inwigilacji wykorzystywały zakres UKF (VHF, *Very High Frequency*, fale ultrakrótkie), jest to zakres dedykowany między innymi radiofonii oraz rozmaitym systemom łączności lokalnej (policja, radiotaxi). Do transmisji używane mogą być również standardy sieci bezprzewodowej Wi-Fi (2,4 GHz, 5 GHz) oraz Bluetooth (2,4 GHz), jednak na niewielkie odległości – bez zastosowania repeaterów (urządzeń wzmacniających sygnał). W przypadku urządzeń o standardowych parametrach jest to kilkanaście–kilkadziesiąt metrów dla sieci Wi-Fi i maksymalnie kilkanaście metrów dla sieci Bluetooth.

Nadajniki podsłuchowych urządzeń inwigilujących pracują w różnych zakresach, co łączy się z licznymi wadami i zaletami. Najniższy zakres – od około 30 do 50 MHz – ma bardzo dobrą siłę przenikania w środowisku miejskim, jednak zarówno odbiornik, jak i nadajnik wymagają instalacji stosunkowo długich anten. Sygnał nadajnika może odbijać się od jonosfery na długich odległościach w porze nocnej i docierać do odległych miejsc. Zaletą nadajników pracujących w zakresie od 88 do 130 MHz jest fakt ich stosunkowo niewielkich kosztów, są one jednak słabo zabezpieczone przed wyciekiem danych, ich pasmo bowiem pokrywa się z komercyjnym pasmem UKF[16], mogą być zatem odbierane za pomocą zwykłego odbiornika radiowego, a także zagłuszane przez stacje radiowe. Z kolei zakres pracy urządzenia od 130 do 180 MHz sugeruje profesjonalne urządzenie, mniejsza jest szansa przypadkowego wykrycia, anteny są krótkie, a urządzenia charakteryzują się wystarczającą czułością. Są to jednak urządzenia stosunkowo drogie, ponadto częstotliwości te są wykorzystywane do komunikacji przez polskie służby dyspozycyjne. Zakres pracy od 330 do 360 MHz zapewnia bardzo duży stopień bezpieczeństwa, gdyż niewielkie jest wykorzystywanie tej długości fal. Anteny mogą być krótkie, brak jest zakłóceń przez inne nadajniki i naturalne źródła. Są to najdroższe urządzenia.

[15] M. Pavithran, *Eavesdropping on GSM*, „International Journal of Engineering Research in Computer Science and Engineering" 2016, nr 3(9).

[16] Od 88 do 107 MHz – zwykle urządzenia podsłuchowe dostrojone są właśnie do takiej częstotliwości.

Istnieje utajniona do lat 80. ubiegłego wieku metoda rozpraszania widma w systemach szerokopasmowych – FHSS, *frequency-hopping spread spectrum*, co oznacza dosłownie w języku polskim skakanie sygnału po częstotliwościach w kolejnych odstępach czasu, w dostępnym widmie (paśmie). Metoda ta utrudnia wykrycie transmisji inwigilującego urządzenia nadawczego.

Eksperymentalne prace nad transmisją radiową w urządzeniach inwigilujących nie ustają. Na przykład uczeni z izraelskiego Uniwersytetu Ben Guriona stworzyli oprogramowanie komputerowe (robaka, wektor ataku – port USB), które zamienia kartę graficzną zainfekowanego komputera w radio. Technika ta, nazwana AirHopper, pozwala wykradać dane z komputerów znajdujących się w izolowanych sieciach (albo w ogóle niepodpiętych do sieci komputerowych). Do jej użycia wystarczy telefon komórkowy zaopatrzony w odbiornik radiowy FM. Po zainfekowaniu docelowej maszyny AirHopper wpływa na działanie kart graficznych tak, aby generowały swoją pracą odpowiednio silne fale radiowe, które będą mogły zostać podjęte przez odbiornik[17]. Transmisja danych następuje poprzez modulację fal radiowych generowanych przez wpływanie na pracę karty graficznej[18]. Z kolei tajemnicza Equation Group odkryła w 2015 roku, w jaki sposób za pomocą sprzętu o wartości nieco ponad tysiąca złotych można wydobyć między innymi klucze kryptograficzne z zainfekowanego uprzednio komputera, wykorzystując monitoring emisji fal radiowych z procesora[19].

Transmisja przewodowa to w podstawowym rozumieniu fizyczne połączenie mikrofonu lub obiektywu kamery z urządzeniem. Oprócz

---

[17] Możliwości generowania fal radiowych przez karty graficzne komputerów rozważano w literaturze przedmiotu od początku XXI w., zob. M.G. Kuhn, *Compromising Emanations: Eavesdropping Risks of Computer Displays*, „Computer Laboratory" 2003, nr 577; B. Kania, *VGASIG. FM Radio Transmitter Using VGA Graphics Card*, 2009, https://bk.gnarf.org/creativity/vgasig/vgasig.pdf (dostęp: 8.01.2019).

[18] Więcej na ten temat: igH, *AirHopper – narzędzie do wykradania danych z odizolowanych, odciętych od sieci komputerów*, Niebezpiecznik, 3.11.2014, http://niebezpiecznik.pl/post/airhopper-narzedzie-do-wykradania-danych-z-odizolowanych-odcietych-od-sieci-komputerow/ (dostęp: 20.12.2018); M. Guri, G. Kedma, A. Kachlon, Y. Elovici, *AirHopper. Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies*, 2014, https://www.wired.com/wp-content/uploads/2014/11/air-hopper-malware-final-e-141029143252-conversion-gate01.pdf (dostęp: 8.01.2019).

[19] M. Błoński, *Najbardziej zaawansowana operacja hakerska w historii*, 17.02.2015, http://kopalniawiedzy.pl/Equation-Group-haker-szpiegostwo-NSA,21930 (dostęp: 20.12.2018); także portal Ars Technica, https://arstechnica.com/tag/equation-group/ (dostęp: 20.12.2018).

standardowych przewodów dostępne są również rozwiązania wykorzystujące rozmaite substancje przewodzące, jak na przykład farby. W tej kategorii mieszczą się także urządzenia korzystające z kabli energetycznych traktowanych jako medium transmisji sygnałów. Działają one podobnie do adapterów PowerLine służących do przesyłania sygnału internetowego w sieci energetycznej. Nadajnik może być podłączony do linii zasilającej w interesującym podsłuchującego pomieszczeniu, sygnał jest przesyłany „po kablu" do odbiornika podłączonego gdzieś w budynku, na tej samej fazie. Takie rozwiązanie ma przede wszystkim tę zaletę, że jest bardzo trudne do wykrycia. Nie występuje tu żadna transmisja w paśmie podczerwieni ani ultradźwięków. Jednym z nowszych rozwiązań tego typu jest podsłuch klawiatury przez gniazdko sieci elektrycznej. Uderzenia w klawisze wywołują zróżnicowanie szumu w linii naziemnej. Rejestrator działa na około 15 metrów, a jego koszt to około dwa tysiące złotych[20].

Transmisja bezkontaktowa niewymagająca bezpośredniego dostępu do inwigilowanego pomieszczenia obejmuje kilka technik: odczyt transmisji elektromagnetycznej, podsłuch laserowy oraz zastosowanie mikrofonów sejsmicznych i kierunkowych.

- Transmisja elektromagnetyczna – paradoksalnie nie jest tu konieczne urządzenie nadawcze – jest nim samo inwigilowane urządzenie, gdyż wszystkie urządzenia elektroniczne podczas przetwarzania sygnału elektrycznego generują promieniowanie elektromagnetyczne niezależnie od tego, czy przetwarzanie sygnału ma charakter cyfrowy czy analogowy. Urządzenia cyfrowe emitują promieniowanie elektromagnetyczne związane z dwustanowym charakterem tego sygnału zwykle w wysokim zakresie częstotliwości. Na przykład w komputerach stacjonarnych, laptopach, a w mniejszym stopniu w tabletach najsilniejszymi źródłami promieniowania elektromagnetycznego są: monitory LED/LCD/CRT, klawiatury, magistrale PCI, kontrolery SCSI/IDE, łącza RS-232 oraz łącza USB[21]. Ponadto nośnikami takich

[20] M. Vuagnoux, S. Pasini, *Compromising Electromagnetic Emanations of Wired Keyboards, 2007–2009 Security and Cryptography Laboratory – LASEC/EPFL*, 2009, https://lasec.epfl.ch/keyboard/ (dostęp: 20.12.2018).

[21] Na przykład możliwości zastosowań ulotu elektromagnetycznego monitorów analizuje M.G. Kuhn, *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*, 2004, http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf (dostęp: 20.12.2018). Z kolei pracownicy Security and Cryptography Lab at Switzerland's EPFL w 2008 r. opracowali procedurę odczytu nieszyfrowanych danych z łącz USB z wykorzystaniem ulotu elektromagnetycznego: P. Miller, *Keyboard „Eavesdropping" Just Got Way Easier, Thanks to Electromagnetic Emanations*, Engadget, 20.10.2008, http://www.engadget.com/2008/10/20/

sygnałów elektromagnetycznych umożliwiającymi propagowanie ich na większe odległości są sieci energetyczne. Tematyka ulotu elektromagnetycznego jest przedmiotem licznych dociekań oraz publikacji[22]. Jako pierwszy na cywilnym rynku[23] możliwości odczytu ulotu elektromagnetycznego w celu inwigilacji odkrył holenderski uczony Wim van Eck w latach 80. ubiegłego wieku[24]. Demonstrował on w praktyce i publicznie możliwość podsłuchu widma elektromagnetycznego monitorów CRT komputerów znajdujących się w londyńskiej dzielnicy biurowej. Urządzenia te powszechnie nazywane są „receptorami van Ecka". W 1985 roku we współpracy z British Broadcasting Corporation (BBC) stworzył dokument filmowy (zaprezentowany w programie *Tommorow's World*), w którym z użyciem furgonetki wyposażonej w 10-metrowy maszt z anteną UKF z powodzeniem odczytywano treści pojawiające się na monitorach komputerów znajdujących się „w dużej odległości". Skuteczny zasięg receptorów to według W. van Ecka od dziesięciu do kilkudziesięciu metrów, a koszt wykonania urządzenia podsłuchowego przekraczał zaledwie o parędziesiąt dolarów cenę telewizora i anteny UKF. Użycie tej metody nie pozostawia śladów, zatem brak jest wiarygodnych danych dotyczących skali tego typu wycieków. Współczesne monitory LCD są co najmniej tak samo narażone na wyciek danych drogą emisji elektromagnetycznej

keyboard-eavesdropping-just-got-way-easier-thanks-to-electrom/?guccounter=1 (dostęp: 20.12.2018); H.-J. Choi i in., *Reconstruction of Leaked Signal From USB Keyboards*, 2016, http://www.researchgate.net/publication/309327769_Reconstruction_of_leaked_signal_from_USB_keyboards (dostęp: 20.12.2018)..2018]. Przegląd współczesnej aparatury oraz metodyka dokonywania ataków tego typu została wyłożona w: F. Elibol, U. Sarac, I. Erer, *Realistic Eavesdropping Attacks on Computer Displays with Low-Cost and Mobile Receiver System* [w:] *Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, 2012, http://www.eurasip.org/Proceedings/Eusipco/Eusipco2012/Conference/papers/1569583239.pdf (dostęp: 20.12.2018).

[22] Por. R. Frankland, *Side Channels, Compromising Emanations and Surveillance. Current and Future Technologies*, Londyn 2011, http://pdfs.semanticscholar.org/87a4/182d66ab649a35eff0267c5e3a73bb2a5087.pdf (dostęp: 20.12.2018).

[23] Stany Zjednoczone od lat 60. XX w. prowadzą program „TEMPEST" badający potencjał ulotu i podsłuchu urządzeń elektronicznych (komputerów i innych urządzeń komunikacyjnych), opracowując standardy urządzeń ekranowanych. Więcej na ten temat: *The Complete, Unofficial TEMPEST Information Page*, http://cryptome.org/tip/tempestintro.html (dostęp: 20.12.2018).

[24] W. van Eck, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, „North-Holland Computers & Security" 1985, nr 4 (artykuł dostępny obecnie na stronach organizacji Cryptome: http://cryptome.org/emr.pdf (dostęp: 20.12.2018)).

(w tym przez nieekranowane kable VGA)[25]. Opracowano profesjonalne urządzenia służące monitorowaniu wycieku elektromagnetycznego, między innymi do rejestrowania uderzeń klawiszy (dotyczy zarówno klawiatur przewodowych, jak i bezprzewodowych, USB/PS2, w komputerach stacjonarnych i laptopach). Taki analizator widma elektromagnetycznego przechwytujący sygnał działa na odległość do 20 metrów, a jego koszt to około 20 tys. złotych[26].

- Jeśli chodzi o urządzenia laserowe umożliwiające prowadzenie inwigilacji z dużej odległości, to zasada ich działania polega na odbieraniu odbitej wiązki promieniowania laserowego. Promień lasera pada na powierzchnię, na przykład okna, ulegając częściowemu odbiciu. Precyzja działania urządzenia jest bardzo wysoka i możliwe jest wychwycenie wibracji okien, które wywoływane są przez dźwięki wewnątrz pomieszczenia. Odbity promień jest zmodulowany tymi wibracjami i urządzenie jest zdolne na tej podstawie odtworzyć treść rozmowy prowadzonej w podsłuchiwanym pomieszczeniu. Do zalet takiego urządzenia należy duży zasięg pracy nawet do 400 metrów, niska wykrywalność, rozdzielenie modułów nadajnika i odbiornika pozwalające na prowadzenie posłuchu, gdy nie jest możliwe prostopadłe ustawienie (wiązka lasera może być kierowana na inne niż szyby powierzchnie – na przykład zastawę szklaną, butelki z wodą itd.), zintegrowany cyfrowy rejestrator pozwalający na automatyczne archiwizowanie pozyskanych informacji. Wadą jest niewątpliwie cena i choć są one coraz tańsze, to profesjonalny można obecnie kupić za około 200 tys. złotych. Za pomocą urządzeń laserowych można podsłuchiwać nie tylko rozmowy, lecz również pracę klawiatury odległych komputerów, możliwa jest bowiem rejestracja wibracji obudowy laptopa / klawiatury komputera. Każdy klawisz generuje unikatowy wzór wibracji, który można odczytać, jeśli skieruje się wiązkę laserową na miejsce urządzenia, które dobrze odbija światło (na przykład logotyp producenta w laptopie).
- Mikrofony sejsmiczne/kontaktowe – są to urządzenia pozwalające na prowadzenie inwigilacji osób znajdujących się w pomieszczeniu obok, przez ścianę o grubości nawet do 50 centymetrów. Umożliwiają one wzmocnienie dźwięku nawet do 20 tys. razy, pozwalając na swobodny podsłuch przez ściany betonowe, drewniane, metalowe, ceglane czy szklane. Podsłuch może być prowadzony zarówno przez

[25] M.G. Kuhn, *Electromagnetic Eavesdropping Risks…*

[26] M. Vuagnoux, S. Pasini, *Compromising Electromagnetic…*

ściany boczne, jak również sufity i podłogi. Bardzo czuły mikrofon wyłapuje każdy wstrząs przeszkody wywołany przez falę akustyczną. Urządzenie ma algorytm korekcji błędów: zastosowanie zaawansowanej filtracji pasmowej powoduje wzmocnienie sygnałów w paśmie ludzkiej mowy i niweluje niepożądane dźwięki. Mikrofony takie są urządzeniami pasywnymi – nie emitują żadnych fal radiowych, co utrudnia ich zdemaskowanie. Mogą być zasilane z akumulatora lub z sieci i wyposażone w rejestrator. Instalacja urządzenia może przebiegać również w inny sposób, jeśli możliwy jest dostęp do pomieszczenia sąsiadującego z tym, które pragniemy poddać inwigilacji, i jeśli wyposażeni jesteśmy w specjalistyczny mikrofon. W ścianie wierci się otwór, wprowadza weń szklaną rurkę jak najbliżej pomieszczenia inwigilowanego. W rurce instalowany jest mikrofon podłączony do rejestratora. Dzięki temu, że jest on oddalony od podsłuchiwanego pomieszczenia, jest praktycznie nie do wykrycia, nawet przy zastosowaniu wykrywacza złącz nieliniowych.

- Mikrofony kierunkowe umożliwiają podsłuch z dużej odległości w otwartym terenie. Dystans, na jakim urządzenia są efektywnie wykorzystane, dochodzi do 500 metrów w warunkach testowych. Realnie, w warunkach miejskich, jest to około 200 metrów.

Nieprzerwanie odbywa się poszukiwanie nowych dróg emisji dla linii przesyłowych. Jako egzemplifikacje wymienić można podsłuch cieplny/podczerwieni, pierwsze próby z transmisją ultradźwiękową, a także emisją dźwiękową.

Transmisja cieplna stanowi swoistą egzotykę urządzeń inwigilacyjnych i prawdopodobnie znajduje się w fazie eksperymentalnej. Po raz pierwszy w ogólnodostępnej literaturze naukowej została opisana w 2015 roku[27]. Urządzenie zostało nazwane BitWhisper. Wymaga ono uprzedniego zainfekowania inwigilowanego komputera, a także umieszczenia obok komputera inwigilującego[28]. Bezwładność cieplna uniemożliwia wysyłanie dużej liczby danych w krótkim czasie i jest to zaledwie osiem bitów w ciągu godziny. Zmiany temperatury maszyny są trudne do zauważenia, a urządzenie jest wyposażone w korekcję błędów spowodowanych czynnikami obocznymi (jest odporne na zakłócenia w postaci zmian temperatury w otoczeniu). Transmisja w podczerwieni jest trudna do wykrycia, jednak

[27] M. Guri, M. Monitz, Y. Mirski, Y. Elovici, *BitWhisper. Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations*, „Cryptography & Security" 2015.

[28] Eksperyment prowadzony był z maszynami ulokowanymi w odległości 40 centymetrów, jednak należy przyjąć, że urządzenia mogą się znajdować w większej odległości, lecz pomiędzy nimi nie może być żadnych nieprzejrzystych przeszkód.

nadajnik i odbiornik muszą pozostawać nieoddzielone żadnymi przeszkodami, które ograniczałyby widoczność. Tą drogą może być prowadzony również klasyczny podsłuch.

Zastosowanie dla transmisji ultradźwiękowej w urządzeniach inwigilujących znalazł Tristan Lawry. Dostrzegł on, iż ultradźwięki (powyżej 20 kHz) mają tę właściwość, że przenikają przez bariery skutecznie blokujące promieniowanie elektromagnetyczne (ekrany stalowe, klatka Faradaya), a także przez ściany. Jego konstrukt składa się z dwóch urządzeń o następujących funkcjach. Urządzenie nadawcze ma charakter pasywny – nie ma zasilania, musi jednak zostać dostarczone do inwigilowanego pomieszczenia. Z kolei urządzenie odbiorcze zasila urządzenie nadawcze wykorzystując ultradźwięki i zapewniając jednocześnie względnie szybki przesył informacji tą drogą (rzędu około 12 MB/s)[29]. Rejestrowanie uderzeń klawiszy dokonywane jest przez akcelerometr znajdującego się obok smartfona[30] (obecnie technologia ta umożliwia rozpoznawanie spójnego tekstu, lecz nie jest w pełni skuteczna przy odczytywaniu haseł, ma około 80-procentową skuteczność rozpoznawania znaków). W 2017 roku izraelscy badacze zaprezentowali koncepcję złośliwego oprogramowania nazwanego Fansmitter, które używa wentylatorów chłodzących komputery lub napędy dysków twardych do przesyłania skradzionych danych – w postaci fal dźwiękowych wytwarzanych przez te wentylatory[31].

URZĄDZENIA ODBIORCZE

Typologia urządzeń odbiorczych zamyka się w następujących dwóch klasach: urządzenia dedykowane odrębne od urządzeń nadawczych oraz scalone z nimi (jak w opisywanych wyżej przypadkach podsłuchu laserowego). Mają one znaczenie wtórne dla jakości zastosowanych urządzeń inwigilujących. Wśród urządzeń odrębnych możemy wyróżnić urządzenia dedykowane (stworzone wyłącznie na potrzeby odbierania transmisji z określonego urządzenia nadawczego) i uniwersalne (laptopy, tablety, smartfony), wymagające jedynie zainstalowania specjalnego oprogra-

[29] Autorzy podchodzą sceptycznie do podanego wolumenu przesyłu informacji. T. Lawry, *An Acoustic-Electric Bridge: Traversing Metal Barriers Using Ultrasound*, 2011, http://www.ttivanguard.com/ttivanguard_cfmfiles/pdf/miami11/miami11session7014.pdf (dostęp: 20.12.2018).

[30] [b.a.], *Hakerzy praw fizyki. Siły i fale w rękach włamywaczy*, http://mlodytechnik.pl/technika/29132-hakerzy-praw-fizyki (dostęp: 20.12.2018).

[31] M. Guri, Y. Solewicz, A. Daidakulov, Y. Elovici, *Fansmitter. Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers*, 2016, http://www.wired.com/wp-content/uploads/2016/06/Fansmitter-1.pdf (dostęp: 20.12.2018).

mowania. Producenci urządzeń oferują oprogramowanie dodatkowe, na przykład filtrujące i korygujące pozyskane zapisy.

Wybrane aspekty kontrinwigilacji

Rozwój metod wykrywania podsłuchów przypomina walkę pocisku z pancerzem. Urządzenia podsłuchowe wykorzystują różne sposoby przekazu zdobytych informacji: wysyłając sygnał w pasmie radiowym na częstotliwościach około 200–400 MHz do wykorzystujących pasmo GSM, Wi-Fi, przewody elektryczne, podczerwień, ultradźwięki czy nadawanie z przeskokiem częstotliwości. Istnieją również urządzenia pasywne – rejestratory.

Zasadniczo istnieją dwa sposoby zabezpieczenia się przed podsłuchem, stosowane jednocześnie. Po pierwsze, jest to właściwe zabezpieczenie osób (obejmujące wdrażanie do przestrzegania określonych procedur bezpieczeństwa, konfigurację oraz zabezpieczenie urządzeń osobistych, takich jak telefony i komputery osobiste) i pomieszczeń (ingerencja architektoniczna – ekranowanie, wdrożenie procedur bezpieczeństwa związanych z dostępem do pomieszczeń oraz instalacja urządzeń i oprogramowania zabezpieczającego pomieszczenia). Drugi filar kontrinwigilacji stanowi sprawdzanie pomieszczeń (cykliczne, regularne i/lub następcze dokonywane zazwyczaj po faktycznym lub domniemanym wystąpieniu incydentu bezpieczeństwa).

Wykrywanie podsłuchów w toku sprawdzania pomieszczeń wymaga z jednej strony przestrzegania przedstawionej niżej ścisłej procedury, a z drugiej strony – kreatywności i analitycznego myślenia. Procedura sprawdzenia obejmuje dwa następujące typy czynności: bezprzyrządowe oraz z użyciem specjalistycznej aparatury wykrywającej. Wymienione elementy są tylko pozornie odrębne, gdyż powinny one łączyć się wzajemnie i przenikać.

TECHNIKI BEZPRZYRZĄDOWE – WYWIAD ŹRÓDŁOWY I SPRAWDZENIE FIZYCZNE

Istotą technik bezprzyrządowych jest zogniskowanie się na czynniku ludzkim. Procedurę kontrinwigilacyjną nieodmiennie rozpoczyna wywiad źródłowy ze zleceniodawcą, a jeśli to możliwe, także z innymi osobami użytkującymi pomieszczenie. W toku wywiadu należy:

- ustalić, jakimi przesłankami kieruje się zleceniodawca, decydując o prowadzeniu działań kontrinwigilacyjnych (jakie wystąpiły incy-

denty naruszeń bezpieczeństwa informacyjnego: jakie informacje, kiedy, w jakich okolicznościach zostały ujawnione);
- przeanalizować luki bezpieczeństwa systemu zleceniodawcy (czynnik ludzki, czynnik proceduralny, czynnik techniczny);
- odtworzyć *status quo* – kto, na jakich warunkach i kiedy ma/miał dostęp do badanego pomieszczenia oraz jego otoczenia;
- zapoznać się z podejrzeniami zleceniodawcy odnośnie do osób lub organizacji zlecającej inwigilację.

Powyższe informacje w dużej mierze wyznaczają wektory poszukiwań, pozwalając między innymi na ewaluację potencjalnych środków przeznaczonych na inwigilację, a co za tym idzie – typ i sposób umieszczenia urządzeń inwigilacyjnych. Czynność wywiadu źródłowego nigdy, z przyczyn oczywistych, nie powinna odbywać się w miejscu poddawanym procedurze sprawdzenia. Warto podkreślić, że nie należy nigdy ograniczać się wyłącznie do wektorów poszukiwań wynikających z wywiadu.

Następnym elementem procedury jest wizualne i fizyczne sprawdzenie pomieszczenia. Jest ono, jak w klasycznym przeszukaniu, dzielone na sektory, które są następnie systematycznie rewidowane. Przesłanką podziału jest topografia pomieszczenia, ale także wiedza o typowych miejscach umieszczania urządzeń inwigilacyjnych. Inspekcji należy również poddać tzw. tunele akustyczne – umożliwiające ulot dźwięku, to jest sufity podwieszane, wspólne kanały centralnego ogrzewania itd. Inspekcja powinna obejmować umeblowanie pomieszczenia, wbudowane (architektoniczne) elementy wyposażenia, wszystkie urządzenia, okablowanie. Należy zwracać uwagę na potencjalne wskaźniki podejmowanej inwigilacji: naruszone gniazda śrub, plomby i inne elementy montażowe z widocznymi śladami ingerencji, starty kurz lub zabrudzone powierzchnie, świeże ślady farby lub szpachlówki, kawałki przewodów czy taśm, otwory itd. Tego typu sprawdzenia dokonuje się z użyciem latarki stanowiącej silne źródło światła, mającej możliwość przełączania w tryb ultrafioletu (UV)[32]. W toku sprawdzenia należy również poczynić ustalenia dotyczące pomieszczeń przylegających do badanego: typ, sposób użytkowania i zasady dostępu, a także ocenić możliwości prowadzenia inwigilacji z zewnątrz (podsłuch laserowy) oraz ustalić ze zleceniodawcą,

[32] Światło o wysokich częstotliwościach (nadfiolet) pozwala na ujawnienie śladów ingerencji w postaci świeżych farb, kitów, szpachlówek, a także rozmaitych zmian w strukturze, ukrytych przewodów oraz innych wskaźników ingerencji niewidocznych w świetle widzialnym.

czy i jakie w sprawdzanym pomieszczeniu pojawiły się nowe/nierozpoznawane przezeń elementy wyposażenia.

TECHNIKI Z UŻYCIEM SPECJALISTYCZNEJ APARATURY WYKRYWAJĄCEJ

Choć do wykrycia wszystkich rodzajów urządzeń inwigilacyjnych służy cała gama różnorakich przyrządów pomiarowych, to można wyróżnić dwie zasadnicze grupy aparatur: wykrywające transmisję linii przesyłowych oraz wykrywające obecność punktów nadawczych.

Wykrywanie transmisji linii przesyłowych obejmuje sprawdzenie pasma radiowego, propagacji w zakresie podczerwieni IR oraz sprawdzenie linii zasilających i innych przewodów. Do wykrycia transmisji mogą służyć wielofunkcyjne analizatory. Jednym z nich jest na przykład Piranha ST-031M. Koszt takiego urządzenia to około 30 tys. złotych. Umożliwia analizę emisji radiowej w zakresie częstotliwości od 140 MHz do 12 GHz, pozwalając na dynamiczne wyszukiwanie anomalii. Urządzenie wykrywa i identyfikuje sygnały GSM, UMTS, LTE i Wi-Fi. Zadaniem tego typu analizatorów jest ustalenie najsilniejszych sygnałów radiowych w pomieszczeniu. Zasięg ich działania wynosi od dziesięciu centymetrów do około jednego metra od źródła sygnału, co oznacza, że wyszukiwanie związane jest z systematycznym obchodem pomieszczenia, a w szczególności z oceną najbardziej podejrzanych miejsc. Urządzenie Piranha ST-031M umożliwia również detekcję w pasmie podczerwieni, ultrafioletu oraz ultradźwięków. Dodatkowo urządzenie umożliwia sprawdzenie linii zasilających oraz wszelkiego rodzaju innych przewodów (choć urządzeniem dedykowanym do sprawdzania przewodów jest analizator ST-300 SPIDER).

Z kolei wykrywanie obecności punktów nadawczych odbywa się z użyciem wykrywacza złącz nieliniowych, anteny elektromagnetycznej oraz wykrywaczy kamer.

Do wykrywania urządzeń pasywnych, w tym nieaktywnych (bez zasilania) w momencie sprawdzania, na przykład dyktafonów, służą wykrywacze złącz nieliniowych, czyli układów półprzewodnikowych. Najlepiej sprawdzają się one przy przeszukiwaniu miejsc, w których brak jest elektroniki i być jej nie powinno: drewnianych mebli, rzeźb, ścianek działowych. Zasada działania tych urządzeń jest homologiczna do zasady działania radaru. Urządzenie wysyła fale o określonej długości, następnie analizuje sygnał odbity, a dokładniej – składowe harmoniczne sygnału wejściowego (harmoniczna jest definiowana jako składowa przebiegu o częstotliwości będącej całkowitą krotnością częstotliwości podstawo-

wej). Pierwsza harmoniczna jest sygnałem o częstotliwości równej częstotliwości analizowanego sygnału okresowego (i z reguły pochodzi od złącz liniowych), a częstotliwości kolejnych składowych harmonicznych są wielokrotnościami tej częstotliwości[33]. Pojawienie się na wyjściu układu wyższych, parzystych harmonicznych przy pobudzaniu składową podstawową świadczy o nieliniowości tego układu (zniekształcenia nieliniowe), co sugeruje obecność układów półprzewodnikowych (diody, tranzystory, układy scalone). Największym problemem podczas używania tych urządzeń jest fakt, że tak zwane złącze m-o-m (*metal-oxide-metal*), czyli zwykła korozja, daje sygnał pseudoidentyczny jak urządzenie elektroniczne[34]. Może więc dojść do sytuacji, w której znajdujący się pod tynkiem kawałek zardzewiałego gwoździa zostanie zidentyfikowany jako urządzenie elektroniczne. Dlatego najlepszym rozwiązaniem jest stosowanie wykrywacza złącz nieliniowych, który potrafi odróżnić złącze m-o-m od rzeczywistego złącza nieliniowego. Do takich urządzeń należą między innymi wykrywacze z serii Cayman (ST-400, ST-401, ST-402, ST-403). Według analogicznej zasady działają anteny elektromagnetyczne – zaopatrzony w taki dodatek jest wykrywacz Piranha ST-031M.

Wykrywanie kamer może odbywać się między innymi z zastosowaniem urządzeń, których zasadą działania jest emitowanie światła lasera i obserwowanie przez specjalny okular światła odbitego od obiektywu. Urządzenie takie generuje promieniowanie podczerwone (na przykład z zastosowaniem systemu diod LED IR), okular urządzenia zaopatrzony jest w filtry przepuszczające tylko spolaryzowane światło, a takie właśnie jest odbijane od matrycy kamery. Przykładem takiego urządzenia jest Optic-2. Znacznie prostszy sposób stanowi wykorzystanie światła widzialnego – zwykłej latarki. Odpowiednio nakierowana wiązka światła sprawi, że odbije się ono od soczewki i matrycy kamery, ujawniając ją.

Przeprowadzona analiza potencjału urządzeń inwigilujących i kontrinwigilujących uwidacznia przewagę tych pierwszych – są one tańsze, a także liczne, co utrudnia, a niekiedy uniemożliwia przewidywanie wektorów ataku. Urządzenia kontrinwigilujące są kosztowne, wymagają wykwalifikowanego personelu i nie zawsze są całkowicie skuteczne (prawdopodobieństwo wykrycia podsłuchu wzrasta, jeśli zwiększymy czas wyszukiwania).

---

[33] Złącze nieliniowe daje parzyste harmoniczne, to jest drugą, czwartą i szóstą, liniowe zaś – harmoniczne nieparzyste – pierwszą, trzecią, piątą.

[34] Jest to sygnał podobny, jednak niejednorodny i niestabilny w czasie, szczególnie przy zakłóceniach mechanicznych.

Próba diagnozy

Dynamiczny rozwój technologiczny oraz liczne lokalne i globalne wydarzenia związane z inwigilacją (tzw. afery podsłuchowe) umożliwiają sformułowanie wniosków diagnostycznych oraz prognoz w zakresie antycypowanych kierunków rozwoju zjawiska. Argumentacja prezentowana jest na zasadzie kontrapunktu, przesłanką takiego zabiegu jest niemożność przeprowadzenia systematycznych badań. Diagnostyczno-prognostyczne refleksje formułowane są zatem na podstawie zestawienia historycznego i współczesnego oglądu danego aspektu. Dla uporządkowania wywodu opatrzono je następującymi etykietami: eskalacja, profesjonalizacja, instytucjonalizacja i normalizacja.

Najwyraźniej dostrzegalne zjawisko stanowi eskalacja zjawiska inwigilacji, polegająca na coraz łatwiejszym dostępie do urządzeń inwigilacyjnych oraz na stałym poszerzaniu się zakresu i treści informacji, jakie można pozyskiwać z ich użyciem. Rozwój technologii zwiększa zakres możliwej do pozyskania informacji co do jej ilości, a przede wszystkim jej rodzajów; aktualnie możliwy jest podsłuch rozmów, podgląd obrazu, ale także bieżący odsłuch i rejestracja rozmów telefonicznych, konwersacji poprzez komunikatory i czaty, poczty elektronicznej, innej prywatnej korespondencji w mediach społecznościowych, rejestracja miejsca pobytu oraz trasy przemieszczania się. Wejście w posiadanie informacji takich jak wymienione nie nastręcza obecnie trudności i nie wymaga istotnych nakładów finansowych. Tytułem przykładu – odczytywanie cudzej korespondencji prowadzonej z użyciem poczty elektronicznej jest możliwe z użyciem darmowego oprogramowania Social Engineering Toolkit dostępnego w nieodpłatnym systemie operacyjnym Kali Linux[35]. Przeszkolenie w użyciu tych narzędzi zajmuje około dwóch godzin, by przełamać typowe zabezpieczenia komputera potencjalnej osoby inwigilowanej.

Warto na zasadzie kontrapunktu wskazać, jak znaczne nakłady finansowe, czasowe i organizacyjne były niezbędne, by uzyskać informacje w przeszłości. Sun Tzu, autor *Sztuki wojny*, apoteozował w tym kontekście rolę wywiadowcy: „Spośród ludzi armii nikt nie jest tak bliski dowódcy jak poufny agent, ani też w nagrodach generał nie jest tak hojny wobec nikogo, jak wobec zaufanego informatora. Z wojskowych tajemnic żadne nie są tak dobrze strzeżone, jak te dotyczące tajnych planów”[36].

---

[35] https://www.kali.org (dostęp: 20.12.2018).

[36] Sun Tzu, *Sztuka wojny*, s. 81, https://www.lazarski.pl/fileadmin/user_upload/dokumenty/student/Sun_Tzu_sztuka_wojny.pdf (dostęp: 20.12.2018).

Pierwotnie podsłuch prowadzono na niewielkie odległości i zazwyczaj wymagał on ingerencji w konstrukcję budynku już na etapie jego wznoszenia, w postaci na przykład wbudowanych kanałów akustycznych, zapewniających gospodarzom podsłuch oddalonych pomieszczeń. W Malborku znajduje się miejsce, w którym Wielki Mistrz Zakonu mógł słuchać rozmów odbywających się w pokojach gościnnych[37]. Podobne miejsce zwane zakrystią akustyczną znajduje się w Archikatedrze pod wezwaniem Jana Chrzciciela i Jana Ewangelisty w Lublinie przy ulicy Królewskiej 14. Łukowate sklepienie pomieszczenia umożliwia propagację słów wypowiedzianych szeptem w jednym z jego rogów do rogu przeciwległego. Niemniej pouczająca jest współczesna egzemplifikacja, ukazująca, iż całkiem niedawno wdrożenie systemu podsłuchowego wymagało wiele pomysłowości, tyleż umiejętności technicznych, a także nakładów finansowych i organizacyjnych. Takimi cechami i możliwościami wykazali się sprawcy najgłośniejszej afery podsłuchowej z lat 40. XX wieku. Właścicielka ekskluzywnego domu publicznym w Berlinie, znanego pod nazwą „Salon Kitty", Katharina Zammit została zmuszona przez Gestapo szantażem do współpracy. Autorem pomysłu był ówczesny szef Policji Bezpieczeństwa (Sipo) Reinhard Heydrich. Stosowane wówczas mikrofony były duże, miały niewielki zasięg i wymagały podłączenia kabli. Zatem w każdym podsłuchiwanym pomieszczeniu należało przeprowadzić wysokonakładowe prace montażowe – umieścić po kilka mikrofonów (miejscem ich instalacji było głównie oświetlenie górne) oraz aparatów fotograficznych. W tym celu wynajęto ostatnie piętro budynku i Gestapo pod przykrywką prowadzonego remontu zainstalowało mikrofony w dogodnych miejscach pokoi. Kable z ostatniego piętra biegły do piwnicy, gdzie technicy rejestrowali rozmowy na magnetofonach. Przedsięwzięcie wymagało również zatrudnienia personelu (poddanego 7-tygodniowemu przeszkoleniu), w tym około 20 dodatkowych prostytutek. Plan wdrożono w życie w marcu 1940 roku. Podsłuchiwano wszystkich bywalców domu publicznego, w tym zagranicznych dyplomatów oraz niemieckich funkcjonariuszy wysokiego szczebla, w tym generała SS Seppa Dietricha, dowódcę dywizji Leibstandarte Adolf Hitler. System został przypadkowo wykryty przez brytyjskiego funkcjonariusza wywiadu Rogera Wilsona, działającego jako rumuński dyplomata Ljubo Kolczew. Do wykrytej wiązki kabli podłączył swoje, które zostały poprowadzone

[37] Notabene podczas ważnych rozmów w pomieszczeniach śpiewał chór, tworząc jeden z pierwszych systemów zagłuszających.

do sąsiedniego budynku, gdzie do operacji dołączyli pracownicy wywiadu brytyjskiego[38].

W taki oto zasobochłonny sposób prowadzano dawniej operacje inwigilacyjne, do czasu wystarczającej miniaturyzacji urządzeń podsłuchowych oraz zapewnienia im bezprzewodowej komunikacji na znaczne odległości. Przeważnie zainstalowanie podsłuchu wiązało się z wykonaniem instalacji w mieszkaniu figuranta lub w wynajmowanym mieszkaniu sąsiadującym. Była to operacja skomplikowana, do której wykonania potrzebne było zaangażowanie wielu osób, w tym stworzenie właściwej legendy dla podejmowanych i widocznych dla postronnych osób działań oraz zamaskowanie śladów po instalacji (niejednokrotnie istniała konieczność, by do zamaskowania śladów wysyłać pracownika o zdolnościach artystycznych, aby dokładnie dobrał właściwą kolorystykę farb).

Wskutek miniaturyzacji instalacja urządzeń inwigilacyjnych jest obecnie nieporównywalnie tańsza, prostsza i bardziej efektywna. Nie są konieczni wykwalifikowani pracownicy, a same urządzenia można często pozyskać za zdecydowanie niewielką kwotę. Taka sytuacja powoduje, że inwigilacja stała się szeroko stosowaną metodą zdobywania informacji już nie tylko gospodarczych, wojskowych i politycznych, jak w przypadkach historycznych, ale i prywatnych (służy na przykład pozyskiwaniu dowodów w sprawach rozwodowych, w których jeszcze kilka lat temu stosowanie podsłuchu byłoby nieopłacalne).

Lista odkrytych i nagłośnionych przypadków jest długa, trudno tu o zachowanie jakiejkolwiek systematyczności i wyczerpywalności. Tytułem przykładu – w 2016 roku w gabinecie przewodniczącego Rady Miejskiej Ostrowa Wielkopolskiego wykryto urządzenie podsłuchowe – umieszczono je pod fotelem urzędnika[39]. Podobne urządzenie odnaleziono w urzędzie miejskim w Karpaczu[40]. Z kolei w Strzegomiu ujawniono w sejfie Urzędu Miejskiego kilka mikrofonów podsłuchowych, odbiornik typu skaner szerokopasmowy, urządzenie odsłuchowe oraz prosty skaner radiowy mogący służyć do wykrywania podsłuchów, jak też odsłuchiwania

---

[38] Więcej na temat tej operacji: T. Crowdy, *Historia szpiegostwa i agentury*, przekł. J. Mikołajczyk, Warszawa 2010, s. 260; B. Wołoszański, *Wojna, miłość, zdrada*, Warszawa 2010, s. 80.

[39] Past, *„Urządzenie podsłuchowe" w Urzędzie Miejskim w Ostrowie Wielkopolskim. Sprawę bada policja*, Gazeta.pl, 14.07.2016, http://wiadomosci.gazeta.pl/wiadomosci/7,114883,20398093,urzadzenie-podsluchowe-w-urzedzie-miejskim-w-ostrowie-wielkopolskim.html (dostęp: 20.12.2018).

[40] P. Kołpajew, *Podsłuch w urzędzie w Karpaczu*, 12.09.2014, https://wroclaw.tvp.pl/16818908/podsluch-w-urzedzie-w-karpaczu#! (dostęp: 20.12.2018).

ogólnie dostępnych (niekodowanych) przekazów[41]. Przypadki te wskazują, jak powszechne jest stosowanie urządzeń inwigilacyjnych, co często czyni się w sposób nie tylko nieprofesjonalny, ale również nieprzemyślany.

Kolejna istotną cechą dotyczącą opisywanego zjawiska jest wyraźna profesjonalizacja urządzeń i usług inwigilacyjnych. Jest to zjawisko równoległe do opisanego wyżej upowszechniania urządzeń podsłuchowych. Wartościowe poznawczo wydaje się zestawienie dwóch przykładów – historycznego i współczesnego, wydobywających na zasadzie ostrego kontrastu postęp, jaki dokonał się w zakresie profesjonalizacji urządzeń i usług inwigilacyjnych. Jeszcze w połowie XX wieku nie istniał wyspecjalizowany rynek takich urządzeń. Wiele z nich tworzyli wynalazcy zatrudniani przez władze państwowe, czyniąc to na potrzeby konkretnych operacji. Szeroko dyskutowanym w literaturze przedmiotu jest rosyjski system podsłuchowy „Złotousty", pierwsze pasywne urządzenie podsłuchowe[42]. Jego autorem, a ściślej – wynalazcą, był genialny uczony Lew Termen. Autor licznych wynalazków – między innymi instrumentu muzycznego nazwanego od jego nazwiska theremin[43]. Pierwsze urządzenie podsłuchowe zostało przez L. Termena opracowane prawdopodobnie w 1943 roku, w tzw. szaraszce – radzieckim zamkniętym ośrodku naukowo-badawczym dla więźniów podległym NKWD[44]. Podsłuch – już po odkryciu przez służby amerykańskie w 1952 roku – został określony mianem *The Thing*. Po raz pierwszy wynalazek zastosowano w 1945 roku. Z okazji amerykańskiego Dnia Niepodległości wypadającego 4 lipca grupa pionierów wręczyła jako prezent ambasadorowi Stanów Zjednoczonych w Moskwie Williamowi A. Harrimanowi tzw. Wielką Pieczęć, czyli drewnianą płaskorzeźbę przedstawiającą bielika amerykańskiego z piersią zasłoniętą tarczą w kolorach amerykańskiej flagi, trzymającego 13 strzał i gałązkę oliwną. Anegdota głosi, iż gdy ambasador zadał retoryczne pytanie, gdzie powiesić rzeźbę, odpowiedziano mu, że najlepiej w jego gabinecie – by dopiec Anglikom. Naturalnie właściwe służby dokonały starannego sprawdzenia

---

41 M. Moczulska, *Strzegom: urzędnicy na podsłuchu*, „Gazeta Wrocławska", 26.04.2011, https://gazetawroclawska.pl/strzegom-urzednicy-na-podsluchu/ar/396470 (dostęp: 20.12.2018).

42 Obszerna analiza tego przypadku wraz z wyjątkami z materiałów źródłowych znajduje się w: K.D. Murray, *The Great Seal Bug*, http://counterespionage.com/great-seal-bug-part-1/ (dostęp: 20.12.2018).

43 Więcej na temat wynalazcy: P. Nikitin, *Leon Theremin (Lev Termen)*, „IEEE Antennas and Propagation Magazine" 2012, nr 54(5).

44 W marcu 1939 r. L. Termen został aresztowany i skazany za rzekome szpiegostwo i działalność wywrotową na osiem lat ciężkich robót.

prezentu, był on podobno również poddany kwarantannie – czyli przetrzymany przez kilka tygodni poza głównymi pomieszczeniami ambasady. W końcu jednak umieszczono go, zgodnie z sugestią darczyńców, w gabinecie ambasadora nad jego biurkiem. Dopiero po upływie siedmiu lat od tego wydarzenia Amerykanie przypadkowo zorientowali się, że na terenie ambasady jest podsłuch – operatorzy radiowi, nasłuchując rosyjskiej aktywności radiowej, natrafili na głos własnego ambasadora. Korzystając z trwającego remontu ambasady, rozpoczęto poszukiwania z pomocą specjalistów. Po wielu dniach stwierdzono, że sygnał z „pluskwy" dobiega ze ściany za biurkiem ambasadora. Zdjęto płaskorzeźbę i rozkuto ścianę. Nic nie znaleziono. Źródłem sygnału okazała się sama płaskorzeźba, ale po pierwsze była sprawdzana, po drugie wisiała już siedem lat, a nie była podłączona do żadnego źródła zasilania, więc wydawało się to niemożliwe. Mimo to została rozmontowana i w środku znaleziono zaledwie zwykły drut oraz membranę. Amerykańscy specjaliści nie potrafili wyjaśnić zasady działania podsłuchu i po kilku miesiącach zdecydowano się przekazać urządzenie w ręce brytyjskiego eksperta MI5 Petera Wrighta[45], któremu rozpracowanie urządzenia zajęło dwa miesiące. Okazało się, iż z domu naprzeciwko amerykańskiej ambasady wysyłano radiową wiązkę o częstotliwości 800 MHz, celując w godło w gabinecie ambasadora. Gdy ktoś rozmawiał, fale głosowe powodowały wibracje membrany. Drgania przenoszone do anteny długości niespełna 23 centymetrów zmieniały trafiający w nią sygnał radiowy, odbijany do stacji nasłuchowej. Urządzenie nie potrzebowało zasilania, tak jak lustro nie potrzebuje energii, żeby odbijać światło.

Podobny system zastosowali Rosjanie w latach 1976–1984. W maszynach do pisania IBM Selectric, w które była wyposażona ambasada amerykańska w Moskwie, umieścili pręty wyposażone w magnetometry. Mierzyły one zmiany pola magnetycznego związane z charakterystycznym dla każdego znaku ustawieniem metalowych ramion pozycjonujących głowicę drukującą. Odczyty były zamieniane na sygnał radiowy i przesyłane do stacji nasłuchowej w pakietach po osiem znaków. Amerykańska Agencja Bezpieczeństwa Narodowego odkryła to dopiero po przeprowadzeniu badań w Stanach Zjednoczonych[46].

---

[45] Polskiemu (i nie tylko) czytelnikowi znany z pracy: P. Wright, *Łowca szpiegów*, przekł. W. Kalinowski, M. Możejko, 1991.

[46] Dokonano tego w ramach operacji Gunman. Więcej na temat tej operacji oraz tzw. Selectric Bug na stronie CryptoMuseum: *IBM Selectric Bug. Operation GUNMAN – How the Soviets Bugged IBM Typewriters*, https://www.cryptomuseum.com/covert/bugs/selectric/index.htm (dostęp: 20.12.2018).

Sztandarowym przykładem rozwoju rynku produktów służących monitorowaniu komunikacji pojedynczych osób jest włoskie przedsiębiorstwo informatyczne Hacking Team powstałe w 2003 roku, które założyli David Vincenzetti i Valeriano Bedeschi[47]. Swoje główne zadanie przedsiębiorstwo definiuje jako wytwarzanie systemów zdalnej kontroli (*Remote Control Systems*), a produkty przeznaczone są wyłącznie dla podmiotów takich jak instytucje państwowe i niektóre korporacje[48]. W 2015 roku z witryny firmy wykradziono około 400 GB tajnych informacji[49]. Ujawniono poufną korespondencję między programistami i przedstawicielami ich klientów, hasła dostępowe do systemów tworzonych przez Hacking Team oraz umowy. Na ich podstawie został opracowany raport ujawniający, iż z usług firmy skorzystało ponad 70 agencji rządowych całego świata (w tym polskie Centralne Biuro Antykorupcyjne), a suma kwot wszystkich zakupów wynosi około 30 mln euro. Oferta Hacking Team obejmowała między innymi: niezauważalne dla zainfekowanego oprogramowaniem HT użytkownika przechwytywanie wiadomości e-mail, rejestrowanie uderzeń klawiszy (*keylogging*), przeszukiwanie zbiorów danych na komputerze, zapisywanie czatów głosowych i wideo, aktywowanie kamer i mikrofonów w komputerze lub smartfonie, śledzenie lokalizacji *via* GPS, ekstrahowanie haseł sieci Wi-Fi oraz możliwość śledzenia w sieci transakcji z użyciem kryptowaluty Bitcoin. Ponadto Hacking Team intensywnie pracował nad nowymi rozwiązaniami inwigilacyjnymi, między innymi prowadzono badania nad dronami zdolnymi do atakowania sieci Wi-Fi. W raporcie międzynarodowej organizacji pozarządowej globalnie monitorującej przejawy ograniczeń wolności słowa – Reporterzy bez Granic (ang. Reporters Without Borders) wymieniono obok Hacking Team jeszcze cztery inne organizacje (Amesys, Blue Coat, Gamma, Trovicor), nazywając je pięcioma największymi wrogami Internetu i piętnując tym samym wytwarzanie przez nie na potrzeby służb dyspozycyjnych

[47] Więcej na temat oferty Hacking Team: S. Špaček, P. Celeda, M. Drašar, M. Vizváry, *Analyzing an Off-the-Shelf Surveillance Software. Hacking Team Case Study*, 2.06.2017, http://spi.unob.cz/papers/spi2017.html https://is.muni.cz/repo/1382042/2017-SPI-hacking-team-case-study-presentation.pdf (dostęp: 20.12.2018)] (także na stronie przedsiębiorstwa http://www.hackingteam.it (dostęp: 20.12.2018).

[48] A. Batey, *The Spies Behind Your Screen*, „Telegraph", 24.10.2011, https://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html (dostęp: 20.12.2018).

[49] Wykradzione informacje (część z nich zaopatrzono w wygodną wyszukiwarkę) znajdują się na stronach Transparency Toolkit: *Hacking Team Archive*, https://transparencytoolkit.org/project/hacking-team-archive/ (dostęp: 20.12.2018).

państw oprogramowania naruszającego prywatność komunikacji i zbiorów danych[50].

Trzeci aspekt to dostrzegalny wyraźnie trend instytucjonalizacji zjawiska inwigilacji, czyli powstawania wyspecjalizowanych agend i programów działania służących inwigilacji. Doskonałym tego przykładem są Stany Zjednoczone. Po II wojnie światowej rozpoczęto prace nad miniaturyzacją samych urządzeń podsłuchowych i ich źródeł zasilania oraz nad opracowywaniem innych niż „klasyczne" metod podsłuchowych. W tym celu w 1951 roku utworzono w ramach Centralnej Agencji Wywiadowczej (CIA) Technical Services Staff (od 1960 roku Technical Services Division) zajmującą się opracowywaniem i badaniem urządzeń inwigilacyjnych. W początkowym okresie liczyła ona zaledwie 50 pracowników, jednak już po dwóch latach działania liczba pracowników zwiększyła się pięciokrotnie. Intensywne prace, jak się współcześnie okazało, były kontynuowane również na innej płaszczyźnie: masowego podsłuchu połączeń telefonicznych.

Jednym z budzących największe kontrowersje przedsięwzięć jest projekt National Security Agency (NSA) noszący nazwę Echelon[51]. Prace nad nim trwały już od 1947 roku, jednak pierwsze wiarygodne dotyczące go informacje trafiły do opinii publicznej dopiero w 1988 roku. Stało się to za sprawą Margaret Newsham, administratorki systemów komputerowych w stacji nasłuchowej Echelon Menwith Hill położonej w hrabstwie Yorkshire[52]. Z systemu tego korzystają obecnie agencje wywiadowcze nie tylko Stanów Zjednoczonych Ameryki Północnej, ale także Australii, Kanady, Nowej Zelandii oraz Wielkiej Brytanii[53]. System Echelon składa się z dwóch modułów: nasłuchu oraz analizy. Pierwszy z modu-

---

[50] Najnowszy raport pochodzi z 2013 r.: Reporters Without Borders, *Special Report on Internet Surveillance, Focusing on 5 Governments and 5 Companies "Enemies of the Internet"*, 15.03.2013, https://rsf.org/en/news/special-report-internet-surveillance-focusing-5-governments-and-5-companies-enemies-internet (dostęp: 20.12.2018).

[51] European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)*, Session document, FINAL A5-0264/2001, 11.07.2001, http://www.fas.org/irp/program/process/rapport_echelon_en.pdf (dostęp: 20.12.2018).

[52] D. Campbell, *Making History: The Original Source for the 1988 First Echelon Report Steps Forward*, 25.02.2000, cryptome.org/echelon-mndc.htm (dostęp: 24.12.2018); J. Rafa, *Złowrogi Echelon*, „PCKurier" 2000, nr 10, http://www.wsp.krakow.pl/papers/echelon.html (dostęp: 20.12.2018).

[53] H. Kozieł, *Systemy szpiegostwa elektronicznego*, 30.01.2006, http://www.psz.pl/124-polityka/hubert-koziel-systemy-szpiegostwa-elektronicznego http://www.pe24.pl/index2.php?option=com_content&do_pdf=1&id=2204 (dostęp: 20.12.2018).

łów składa się z co najmniej kilkunastu stacji nasłuchowych rozmieszczonych na całym świecie (Australia, Japonia, Kanada, Niemcy, Nowa Zelandia, Stany Zjednoczone, Wielka Brytania, prawdopodobnie Cypr) oraz stu parudziesięciu satelitów geostacjonarnych[54]. Przechwytywana jest komunikacja na wszystkich zakresach fal elektromagnetycznych: możliwy jest więc nasłuch radia, telefonii, w tym telefonii satelitarnej[55]. Mówi się, że system Echelon jest władny przechwycić nawet 90% komunikacji w ruchu międzynarodowym. Stacje nasłuchowe zaopatrzone są w oprogramowanie analityczne noszące nazwę Dictionary[56]. Umożliwia ono filtrowanie przekazów pod kątem określonych słów interesujących służby (tzw. *trigger words*, czyli słów-wyzwalaczy). Słowa te – podobno – automatycznie powodują uaktywnienie się nasłuchu systemu Echelon i odpowiednie raportowanie. Zautomatyzowane filtrowanie raportów oraz selekcja dokonywana przez analityków wyznaczają cele do dalszej obserwacji. Domyślać się można, jak wielkie środki finansowe i organizacyjne przeznaczane są na ten projekt.

Wymieniać można też inne liczne narzędzia służące współczesnym państwom do inwigilacji i nadzoru obywateli, jednak swoistym typem idealnym jawi się nowo ujawniony amerykański zestaw narzędzi noszący nazwę PRISM. Jest to program stworzony na zamówienie i używany przez NSA, a także CIA oraz inne służby. Jego istnienie ujawnił opinii publicznej Edward Joseph Snowden, były pracownik CIA, następnie zatrudniony w Booz Allen Hamilton mającej około 80 ośrodków na całym świecie i dostarczającej usługi informacyjne NSA. W lipcu 2013 roku E.J. Snowden ujawnił informacje, według których dobrowolnie lub pod naciskiem zgodziło się udostępniać dane o użytkownikach dziewięć następujących koncernów: Apple, America OnLine (AOL), Facebook, Google, Microsoft, Paltalk, Skype, Yahoo oraz YouTube. PRISM umożliwia odczytywanie następujących rodzajów wiadomości zdeponowanych przez użytkowników korzystających z usług wymienionych firm: e-maile, wiadomości z komunikatorów, filmy, zdjęcia, pliki przechowywane w chmurze, czaty głosowe, pliki przesyłane wewnątrz serwisów, wideokonferencje, czasy logowania, a także aktywność w profilach portali

[54] M. Assser, *Echelon: Big Brother without a Cause?*, BBC News, 6.06.2000, http://news.bbc.co.uk/2/hi/europe/820758.stm (dostęp: 20.12.2018).

[55] European Parliament, *Report on the Existence Of A Global System for the interception of private and commercial communications (ECHELON interception system)*, 11 lipca 2001, http://www.fas.org/irp/program/process/rapport_echelon_en.pdf (dostęp: 20.12.2018).

[56] Szerzej na ten temat: N. Hager, *Secret Power. New Zealand's Role in the International Spy Network*, Nelson 1996, s. 42–56.

społecznościowych. Jednocześnie E.J. Snowden ujawnił istnienie i wykorzystywanie innych programów szpiegowskich, między innymi oprogramowania Blarney służącego do monitorowania przepływu wiadomości e-mail i ruchu sieciowego. Zdemaskował również pozostającą na usługach NSA grupę hakerów noszącą nazwę Tailored Acess Operations zatrudniającą blisko 600 pracowników[57]. Ich główne zadanie – według E.J. Snowdena – polegało na infiltracji wskazanych komputerów i sieci na całym świecie. Istnienie PRISM, choć bez wskazania jego nazwy i z zastrzeżeniem, że programu używa się każdorazowo wyłącznie za wiedzą i zgodą sądu, potwierdził Dyrektor Wywiadu Narodowego (Director of National Intelligence)[58] James Robert Clapper[59]. Przykład Stanów Zjednoczonych ukazuje, jak w ciągu kilkudziesięciu lat powstały i funkcjonowały niezauważalnie potężne instytucje inwigilujące, których kadra liczy co najmniej kilka setek osób, zarówno urzędników państwowych i funkcjonariuszy, jak też przedstawicieli firm prywatnych.

Kolejny współczesny aspekt zjawiska inwigilacji to fakt, że konstytuuje się ono społecznie i że dostrzegalna jest swoista normalizacja. Kolejne afery podsłuchowe oraz ujawnione potężne narzędzia sprawiły, iż środki inwigilacji powszednieją; zjawisko można rozważać w kategoriach normalizacji dewiacji[60] bądź wręcz degradacji moralnej[61].

Rozważmy historyczny i współczesny przypadek społecznej reakcji na inwigilację. Na początku stycznia 1932 roku ujawniono w ulotkach krążących po Warszawie treść rozmowy telefonicznej ówczesnego premiera Kazimierza Bartla z prezydentem Ignacym Mościckim. Oznaczało to, iż linia telefoniczna pomiędzy Prezydium Rady Ministrów a pałacem w Spale musiała być na podsłuchu. Wyrazy oburzenia słyszano ze wszystkich stron sceny politycznej – na przykład zarówno endecka „Gazeta Warszawska", jak i prorządowy „Ilustrowany Kurier Codzienny"

---

[57] M.M. Aid, *Inside the NSA's Ultra-Secret China Hacking Group*, „Foreign Policy", 10.06.2013, http://www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group (dostęp: 20.12.2018).

[58] Dyrektor Wywiadu Narodowego (DNI) stoi na czele federacji 16 rządowych agencji wywiadowczych – Wspólnoty Wywiadowczej (Intelligence Community), jest głównym doradcą prezydenta i Rady Bezpieczeństwa Narodowego w sprawach wywiadowczych związanych z bezpieczeństwem narodowym.

[59] S. Waterman, *„ Prism" a Vital Program Used to Collect Personal Web Data*, „Washington Times", 7.06.2013, http://www.washingtontimes.com/news/2013/jun/7/prism-used-collect-personal-web-data-clapper-says/ (dostęp: 20.12.2018).

[60] A. Siemaszko, *Granice tolerancji. O teoriach zachowań dewiacyjnych*, Warszawa 1993.

[61] N. Dobos, *Two Concepts of Moral Injury: Moral Trauma and Moral Degradation*, [w:] T. Frame (red.), *Moral Injury: Unseen Wounds in an Age of Barbarism*, Sydney 2016.

potępiali zjawisko w kategoriach moralnych. Przeprowadzone śledztwo ujawniło sprawcę – był nim dziennikarz Jan Seinfeld, który wyspecjalizował się w zbieraniu poufnych informacji z urzędów centralnych. Pomimo znacznego oburzenia nie wyjaśniono nigdy sposobu, w jaki wszedł on w posiadanie informacji. Jedna z hipotez głosi, iż sanacyjne władze prowadziły inwigilację obywateli używając telefonicznych stacji podsłuchowych, a J. Seinfeld porozumiał się z funkcjonariuszami obsługującymi taką jednostkę, prawdopodobnie ich przekupując. Historia III Rzeczypospolitej w nieporównywalnie większym stopniu bogata jest w podsłuchy i również w sposób nieporównywalny – w osłabione reakcje na nie. W 2002 roku redaktor naczelny „Gazety Wyborczej" Adam Michnik zarejestrował w swoim gabinecie prywatną rozmowę między nim a znanym producentem filmowym Lwem Rywinem, który zaproponował zmiany w ustawie umożliwiające firmie Agora kupno telewizji Polsat w zamian za 17,5 mln dolarów na kampanię SLD i prezesurę Polsatu dla siebie. W 2006 roku posłanka Samoobrony Renata Beger nagrała spotkanie z czołowymi politykami Prawa i Sprawiedliwości – Adamem Lipińskim i Wojciechem Mojzesowiczem. W tym samym roku nagrany został premier Józef Oleksy przez Aleksandra Gudzowatego w siedzibie Bartimpeksu. J. Oleksy ujawnił liczne nieprawidłowości, do jakich dochodziło podczas rządów SLD oraz liczne informacje dotyczące prywatnego życia działaczy tej formacji. Rok później w toku dokonanej przez oficera Centralnego Biura Antykorupcyjnego działającego pod przykryciem (Tomasza Kaczmarka) kontrolowanej propozycji korupcyjnej zarejestrowano film, na którym posłanka Platformy Obywatelskiej Beata Sawicka przyjęła 50 tys. złotych w zamian za obietnicę wpłynięcia na przetarg publiczny. Z kolei w 2009 roku CBA ujawniło stenogramy z nagrań rozmów szefa klubu parlamentarnego Platformy Obywatelskiej Zbigniewa Chlebowskiego z Ryszardem Sobiesiakiem, biznesmenem działającym w branży hazardowej, zainteresowanym konkretnym kształtem ustawy o grach i zakładach. W latach 2014–2018 opublikowano szereg nagrań lub stenogramów z największej polskiej afery podsłuchowej – rozmowy zostały podsłuchane w restauracjach: Sowa & Przyjaciele, Amber Room oraz Osteria. Pierwszą reakcją obozu władzy było stanowcze oświadczenie, iż nikt nie zostanie zdymisjonowany, ponieważ byłoby to destabilizacją instytucji państwa[62]. Pierwsze dymisje nastąpiły dopiero rok później

[62] M. Mańkowski, *Donald Tusk: Dymisji i tak nie będzie. Polski rząd nie działa pod dyktando przestępców*, NaTemat.pl, 23.06.2014, https://natemat.pl/107269,donald-tusk-dymisji-i-tak-nie-bedzie-polski-rzad-nie-dziala-pod-dyktando-przestepcow (dostęp: 20.12.2018).

w rządzie Ewy Kopacz. Warto podkreślić, że treść rozmów, choć karygodna, nie wywołała szerszej reakcji społeczeństwa polskiego, ulicznych protestów podjęli się jedynie narodowcy[63], a w ogólnym społecznym czy medialnym odbiorze nie odnotowano oburzenia na akt podsłuchiwania, lecz raczej rodzaj *Schadenfreude*.

Zakończenie: antycypacje trendów

Przegląd historii techniki czyni dostrzegalnym kilka progów jakościowych, które pod względem łatwości użytkowania urządzeń i zakresu zbieranych informacji pokonały urządzenia inwigilacyjne. Uwidaczniają się trzy etapy już osiągnięte i jeden antycypowany, wyznaczając kolejne przełomy – „rewolucje inwigilacyjne". Pierwszy z przełomów to moment rozpoczęcia stosowania mikrofonu i przesyłu zdobytej informacji najpierw przewodami, a następnie drogą radiową, w miejsce podsłuchów „architektonicznych" lub – nazwijmy obrazowo – „analogowych", to jest ludzkich. Kolejną istotną zmianę wyznacza informatyzacja i powszechny dostęp do Internetu – zakres i kategorie informacji przesyłanych drogą elektroniczną zwiększyły się wówczas niepomiernie. Symbol kolejnego poziomu rozwoju, a zarazem nowej jakości w metodach inwigilacji stanowi smartfon – jako urządzenie osobiste, stale nam towarzyszące. Najbliższy z przewidywanych przełomów przyszłości wydaje się realny wraz z nastaniem tzw. Internetu rzeczy (*Internet of Things*), co umożliwi nieograniczoną obserwację i analizę nie tylko treści komunikacji ludzkiej, ale także dowolnych elementów behawioralnych – biologicznych i społecznych.

W perspektywie technologicznej i społecznej można przewidywać dwa zjawiska związane ze środkami inwigilacji elektronicznej. Po pierwsze, możliwą utratę kontroli nad systemami inwigilacyjnymi, co wiązać się może zarówno z autonomizacją tych systemów wskutek wdrażania algorytmów sztucznej inteligencji, jak również z czynnikiem ludzkim – rosnącą rolą swoistej technokracji, inżynierów i techników odpowiedzialnych za rozwój i obsługę tych systemów[64]. Rola, jaką odegrali

[63] IAR, *Protesty narodowców w całym kraju. „Rząd do dymisji"*, PolskieRadio.pl, 17.06.2014, https://www.polskieradio.pl/5/3/Artykul/1155094,Protesty-narodowcow-w-calym-kraju-Rzad-do-dymisji (dostęp: 20.12.2018).

[64] Zagadnienie autonomizacji i jej negatywnych skutków rozważa interesująco: K. Michalski, *Autonomizacja techniki i niepożądane skutki eliminowania człowieka jako źródła błędów*, „Filo-Sofija" 2017, nr 39(4/I).

Margaret Newsham, Edward Joseph Snowden i Chelsea [Bradley] Manning[65], wykazuje, że jest to żywioł nieprzewidywalny, ujawniane są bowiem najgłębiej skrywane inwigilacyjne tajemnice. Po wtóre, dostrzec można symptomy eskalacji wyścigu technicznego: środków podsłuchu i samoobrony, co w dalszej perspektywie może doprowadzić do ideologicznej i faktycznej negacji instytucji państwa przez grupy społeczne zjednoczone wokół idei wolności informacyjnej. Symptomy są już obecnie dostrzegalne – uformowało się silne środowisko skupione wokół technik zapewniających użytkownikom pełną prywatność i wyłączną kontrolę nad tworzonymi i przesyłanymi przez nich danymi (tzw. *Privacy Enhancing Technologies*, PET). Powstało już na przełomie lat 70. i 80. ubiegłego wieku, gdy dokonano technologicznego przełomu w ochronie prywatności elektronicznych danych. Whitfield Diffie i Martin Hellman opracowali metodę szyfrowania asymetrycznego (klucz publiczny, klucz prywatny), wówczas także stworzyli matematyczny koncept pierwszej kryptowaluty[66]. Jacob Appelbaum, współautor (wraz między innymi z Julianem Assange'm) książki *Cypherpunks. Freedom and the Future of the Internet*, niezależny dziennikarz i specjalista z zakresu cyberbezpieczeństwa, trafnie ujął znaczenie tego wynalazku: „Silna kryptografia może opierać się nieograniczonemu stosowaniu przemocy. Żadna siła przymusu nigdy nie rozwiąże problemu matematycznego"[67].

Amorficzny, lecz liczny i silny ruch na rzecz anonimowości rozwinął się istotnie od tego czasu, tworząc ideologiczno-doktrynalne treści (zarówno niezbyt obszerne, jak i niezbyt zaawansowane merytorycznie), lecz przede wszystkim silnie i konsekwentnie obudowując się w rozmaite „technologie wolności".

Jeśli chodzi o ideologiczno-doktrynalne treści, należy w pierwszej kolejności wymienić powstałą na przełomie lat 80. i 90. XX wieku grupę Cypherpunks (nazwa powstała *ad hoc*, w wyniku sytuacyjnego żartu) organizującą comiesięczne spotkania dotyczące prywatności oraz rządo-

[65] Informator WikiLeaks Chelsea [Bradley] Manning (postanowił zmienić płeć i teraz nosi imię Chelsea) miał stopień starszego szeregowego wojsk lądowych, został aresztowany w 2010 r. za przekazanie WikiLeaks ponad 700 tys. dokumentów wojskowych i dyplomatycznych, a także plików wideo dotyczących operacji wojskowej USA w Iraku.

[66] W. Gogłoza, *Cypherpunks, WikiLeaks i widmo kryptograficznej anarchii*, https://wgogloza.com/umcs/informatyka-prawnicza/cypherpunks/ (dostęp: 20.12.2018).

[67] W oryginale: „Strong cryptography can resist an unlimited application of violence. No amount of coercive force will ever solve a math problem". J. Assange, J. Appelbaum, A. Müller-Maguh, J. Zimmerman, *Cypherpunks. Freedom and the Future of the Internet*, Nowy Jork – Londyn 2012, s. 5.

wej i korporacyjnej kontroli informacji. Impuls do działania grupie nadał opublikowany w połowie lat 80. artykuł Davida Chauma *Security without Identification: Transaction Systems to Make Big Brother Obsolete*[68]. Istotne znaczenie należy przypisać treściwemu manifestowi Chucka Hammilla *Od kuszy do kryptografii, czyli psucie szyków państwa przy pomocy techniki* (*From Crossbows to Cryptography. Thwarting the State via Technology*), widzącego w nieskrępowanym dzieleniu się informacją akt oddziaływania na władze silniejszy niż przemoc[69]. Nazwę własną ruchu – kryptoanarchizm – wprowadził w 1992 roku Timothy C. May, amerykański pisarz, inżynier elektronik, dawny pracownik firmy Intel[70]. Jest on autorem innych ważkich dla kryptoanarchistycznego ruchu publikacji, jak *Cyphernomicon*[71], *True Nyms and Crypto Anarchy*[72]. Wartościowym i właściwie zamykającym listę lektur kryptoanarchistów wykładem wydaje się również praca zbiorowa *Crypto Anarchy, Cyberstates, and Pirate Utopias*[73].T.C. May jest autorem najbardziej nośnej koncepcji kryptoanarchizmu – tzw. rynku zabójców (*Assassination Market*), który ukazuje stopień determinacji w drastycznym ograniczeniu informacyjnych apetytów państw[74].

Rynek zabójców spopularyzowany został przez amerykańskiego naukowca, wynalazcę i dysydenta Jamesa Daltona Bella w klasycznym dla kryptoanarchistów 10-częściowym eseju zatytułowanym *Assassination Politics*. Rynek zabójców stanowi metaprojekt globalnego, trwałego wyeliminowania sfery politycznej ze stosunków międzyludzkich dzięki anonimowej komunikacji i anonimowemu, elektronicznemu pieniądzowi w Internecie. Na poziomie wdrożeniowym *Assassination market* to strona internetowa zaopatrzona w narzędzia zabezpieczające tożsamość użytkowników, na której przyjmowane są zakłady[75]. Przedmiotem zakładu jest

---

68 D. Chaum, *Security without Identification. Transaction Systems to Make Big Brother Obsolete*, „Communications of the ACM" 1985, nr 28(10).

69 Ch. Hammill, *Od kuszy do kryptografii, czyli psucie szyków państwa przy pomocy techniki*, przekł. J. Sierpiński, „Kultura i Historia" 2007, nr 11, http://www.kulturaihistoria.umcs.lublin.pl/archives/701 (dostęp: 20.12.2018).

70 T.C. May, *The Crypto Anarchist Manifesto*, Activism.net, 22.11.1992, https://www.activism.net/cypherpunk/crypto-anarchy.html (dostęp: 20.12.2018).

71 T.C. May, *Cyphernomicon. Cypherpunks FAQ and More, Version 0.666*, 10.09.1994, http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html (dostęp: 20.12.2018).

72 T.C. May, *True Nyms and Crypto Anarchy*, 2001, http://www.isfdb.org/cgi-bin/title.cgi?195636 (dostęp: 20.12.2018).

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

74 T.C. May, *Cyphernomicon*…

75 J. Bell, *Assassination Politics*, 1997, http://outpost-of-freedom.com/jimbellap.htm (dostęp: 20.12.2018).

śmierć osoby publicznej, uprzednio (po wniesieniu opłaty rejestracyjnej) zgłoszonej (tzw. *dead pool*). Każdy może zaproponować przewidywaną przez siebie datę, zawierając zakład i wpłacając kwotę, którą uzna za adekwatną. Wygrywa, otrzymując pulę wpłat, ten z uczestników, który najdokładniej przewidzi czas śmierci osoby, której zakład dotyczy. Jest to w istocie zakamuflowany tytułowy rynek zabójców: któż bowiem bardziej precyzyjnie przewidzi datę śmierci ofiary niż jej zabójca, a uczestnicy zakładu to w istocie zakamuflowani zbiorowi zleceniodawcy darzący daną osobę publiczną negatywnymi uczuciami. Im ich więcej, tym pula zakładu wyższa, w tym większym stopniu staje się finansowo opłacalne dla wystarczająco zdeterminowanej jednostki podjęcie zabójstwa politycznego. W założeniu globalność i sieciowość projektu zapewnią niemal każdorazowo opłacalność dokonania zabójstwa, rychło doprowadzając do permanentnej destabilizacji, a następnie, w dalszej perspektywie, całkowitej eliminacji sfery politycznej. Z technicznego punktu widzenia (anonimowa komunikacja oraz anonimowy pieniądz) obecnie nie istnieją przeszkody w realizacji takiego projektu. Przez pewien czas – od 2013 roku – w sieci TOR funkcjonował rynek zabójców pod adresem assmkedzgorodn7o.onion[76]. Pomysłodawcą, twórcą i administratorem serwisu była osoba nosząca pseudonim Kuwabatake Sanjuro[77], kryptoanarchista kierowany przesłankami ideologicznymi, głęboko przekonany, iż inicjatywa ta zapoczątkuje serie zabójstw polityków, doprowadzając do ziszczenia się anarchistycznego raju: zniesienia wszelkich form rządów na całym świecie.

Siłą kryptoanarchizmu są jednak wdrożenia technologiczne – powstały liczne produkty zapewniające bezpieczeństwo informacyjne użytkownikom Internetu – między innymi silnie anonimizujące użytkowników sieci The Onion Router wraz z dedykowaną przeglądarką internetową TOR Browser[78], Freenet[79] oraz Invisible Internet Project[80], niepozostawiający śladów użytkowania lokalnie i anonimizujący zdalnie system operacyjny Linux Tails[81] – dedykowany użytkownikom pragnącym zachować naj-

[76] Od 2015 r. strona nie funkcjonuje, jednak zdeponowane bitcoiny nie zostały podjęte przez właściciela witryny.

[77] Główna postać, samuraj, w japońskim filmie *Straż przyboczna* (reż. Akira Kurosawa, 1961).

[78] *TOR Project*, https://www.torproject.org (dostęp: 20.12.2018).

[79] *Freenet*, https://freenetproject.org/author/freenet-project-inc.html (dostęp: 20.12.2018).

[80] *Invisible Internet Project*, https://geti2p.net/pl/ (dostęp: 20.12.2018).

[81] *TAILS (The Amnesic Incognito Live System)*, https://tails.boum.org (dostęp: 20.12.2018).

wyższy stopień prywatności, VeraCrypt[82] (nierozwijany już TrueCrypt) umożliwiający szyfrowanie dowolnych danych silnymi algorytmami. Dostępnych jest także szereg mniej znanych produktów, jak pozwalający dowolnie zmieniać tożsamość w Internecie Advanced Onion Router[83], liczne usługi bezpiecznych, szyfrowanych czatów, komunikatorów oraz kont pocztowych[84].

Te dwa nurty: dynamiczny rozwój systemów inwigilacyjnych oraz równolegle technik samoobrony przed inwigilacją są nie tylko rywalizacją o charakterze technologicznym. W dalszej perspektywie sytuacja taka może doprowadzić do poważnej i nieodwracalnej erozji zaufania społecznego wobec instytucji państwa, skutkując postrzeganiem tych instytucji jako opresywnych i totalitarnych. Z kolei państwa mogą nasilać kulturowo-społeczną deprecjację prywatności jako wartości samej w sobie oraz penalizować akty anonimizacji działań i ukrywania tożsamości.

Streszczenie

Tekst ogniskuje się na rozmaitych aspektach inwigilacji z użyciem narzędzi elektronicznych. Autorzy poszukują odpowiedzi na szereg pytań. Po pierwsze, jakie typy negatywnych zjawisk generują i są intensyfikowane przez technologie inwigilacji elektronicznej? Po wtóre, jak głęboki jest stan „bezbronności inwigilacyjnej" współczesnych społeczeństw, to jest jakie są możliwości urządzeń służących inwigilacji? Po trzecie, czy istnieje możliwość praktycznego przeciwstawienia się im i – jeśli tak – w jaki sposób? Po czwarte, jaka jest geneza tych zjawisk i jakie spodziewane scenariusze przyszłości można szkicować na podstawie antycypacji zaobserwowanych trendów? Tak zdefiniowany zbiór pytań badawczych wymagał oglądu zarazem z dwóch perspektyw: socjologicznej i technicznej. Autorzy dostrzegają i analizują szereg negatywnych zjawisk związanych z inwigilacją elektroniczną – jej eskalację, profesjonalizację, instytucjonalizację i normalizację.

[82] *VeraCrypt*, https://www.veracrypt.fr/en/Downloads.html (dostęp: 20.12.2018).

[83] *Team Elite*, https://www.te-home.net/?do=work&id=advor (dostęp: 20.12.2018).

[84] Tę jakże obszerną grupę zagadnień autorzy poruszają koncepcyjnie i praktycznie w toku kursów prowadzonych przez nich na Uniwersytecie Otwartym Uniwersytetu Warszawskiego: *Nie daj się podsłuchać, nie daj się zhakować – warsztaty cybersamoobrony dla humanistów*.

Paweł Tomczyk, Daniel Mider, Józef Grzegorczyk

Electronic Surveillance as a Method ob Obtaining Information – Evaluation and Forecasts

The text focuses on one of the elements belonging to the surveillance society – surveillance with the use of electronic tools. The authors attempt to answer the following questions. What types of negative phenomena are produced and intensified by electronic surveillance technologies? How deep is the state of the „vulnerability" of modern societies, what are the possibilities of surveillance devices? Is it possible to practically oppose them, how and what are the limits? What is the genesis of these phenomena and what future scenarios can be sketched based on the anticipation of observed trends? A set of research questions defined in this way required both sociological and technical perspectives at the same time. The authors recognize the negative phenomena associated with electronic surveillance: escalation, professionalization, institutionalization and normalization.

Key words: *social informatics, surveillance society, electronic surveillance, infobrokering*

Bibliografia

Aid M.M., *Inside the NSA's Ultra-Secret China Hacking Group*, „Foreign Policy", 10.06.2013, http:// www.foreignpolicy.com/articles/2013/06/10/inside_the_nsa_s_ultra_secret_china_hacking_group (dostęp: 20.12.2018).

Assange J., Appelbaum J., Müller-Maguh A., Zimmerman J., *Cypherpunks. Freedom and the Future of the Internet*, Nowy Jork – Londyn 2012.

Assser M., *Echelon: Big Brother without a cause?*, BBC News, 6.06.2000, http://news.bbc.co.uk/2/hi/europe/820758.stm (dostęp: 20.12.2018).

Batey A., *The Spies Behind Your Screen*, „Telegraph", 24.10.2011, https://www.telegraph.co.uk/technology/8899353/The-spies-behind-your-screen.html (dostęp: 20.12.2018).

Bell J., *Assassination Politics*, 1997, http://outpost-of-freedom.com/jimbellap.htm (dostęp: 20.12.2018).

Błoński M., *Najbardziej zaawansowana operacja hakerska w historii*, http://kopalniawiedzy.pl/Equation-Group-haker-szpiegostwo-NSA,21930 (dostęp: 20.12.2018).

Campbell D., *Making History: The Original Source for the 1988 First Echelon Report Steps Forward*, 25.02.2000, cryptome.org/echelon-mndc.htm (dostęp: 20.12.2018).

Chaum D., *Security without Identification. Transaction Systems to Make Big Brother Obsolete*, „Communications of the ACM" 1985, nr 28(10).

Choi H.-J., i in., *Reconstruction of Leaked Signal From USB Keyboards*, 2016, http://www.researchgate.net/publication/309327769_Reconstruction_of_leaked_signal_from_USB_keyboards (dostęp: 20.12.2018).

Dobos N., *Two Concepts of Moral Injury: Moral Trauma and Moral Degradation*, [w:] T. Frame (red.), *Moral Injury: Unseen Wounds in an Age of Barbarism*, Sydney 2016.

Eck W. van, *Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?*, „North-Holland Computers & Security" 1985, nr 4.

Elibol F., Sarac U., Erer I., *Realistic Eavesdropping Attacks on Computer Displays with Low-Cost and Mobile Receiver System*, [w:] *Proceedings of the 20th European Signal Processing Conference (EUSIPCO)*, 2012, http://www.eurasip.org/Proceedings/Eusipco/Eusipco2012/Conference/papers/1569583239.pdf (dostęp: 20.12.2018).

European Parliament, *Report on the Existence of a Global System for the Interception of Private and Commercial Communications (ECHELON Interception System)*, Session document, FINAL A5-0264/2001, 11.07.2001, http://www.fas.org/irp/program/process/rapport_echelon_en.pdf (dostęp: 20.12.2018).

Frankland R., *Side Channels, Compromising Emanations and Surveillance. Current and Future Technologies*, Londyn 2011, http://pdfs.semanticscholar.org/87a4/182d66ab649a35eff0267c5e3a73bb2a5087.pdf (dostęp: 20.12.2018).

Gandy O., *Data Mining and Surveillance In the Post – 9/11 Environment* [w:] K. Ball, F. Webster (red.), *The Intensification of Surveillance. Crime, Terrorism and Warfare in the Information Era*, Londyn 2003.

Guri M., Kedma G., Kachlon A., Elovici Y., *AirHopper. Bridging the Air-Gap between Isolated Networks and Mobile Phones using Radio Frequencies*, 2014, https://www.wired.com/wp-content/uploads/2014/11/air-hopper-malware-final-e-141029143252-conversion-gate01.pdf (dostęp: 8.01.2019).

Guri M., Monitz M., Mirski Y., Elovici Y., *BitWhisper. Covert Signaling Channel between Air-Gapped Computers using Thermal Manipulations*, „Cryptography & Security" 2015.

Guri M., Solewicz Y., Daidakulov A., Elovici Y., *Fansmitter. Acoustic Data Exfiltration from (Speakerless) Air-Gapped Computers*, 2016, http://www.wired.com/wp-content/uploads/2016/06/Fansmitter-1.pdf (dostęp: 20.12.2018).

Hager N., *Secret Power. New Zealand's Role in the International Spy Network*, Nelson 1996.

Kania B., *VGASIG. FM Radio Transmitter Using VGA Graphics Card*, 2009, https://bk.gnarf.org/creativity/vgasig/vgasig.pdf (dostęp: 8.01.2019).

Kuhn M.G., *Compromising Emanations: Eavesdropping Risks of Computer Displays*, „Computer Laboratory" 2003, nr 577.

Kuhn M.G., *Electromagnetic Eavesdropping Risks of Flat-Panel Displays*, 2004, http://www.cl.cam.ac.uk/~mgk25/pet2004-fpd.pdf (dostęp: 20.12.2018).

Lawry T., *An Acoustic-Electric Bridge: Traversing Metal Barriers Using Ultrasound*, http://www.ttivanguard.com/ttivanguard_cfmfiles/pdf/miami11/miami11session7014.pdf (dostęp: 20.12.2018).

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

Lyon D., *The Electronic Eye. The Rise of Surveillance Society*, Minneapolis 1994.

May T.C., *The Crypto Anarchist Manifesto*, Activism.net, 22.11.1992, https://www.activism.net/cypherpunk/crypto-anarchy.html (dostęp: 20.12.2018).

May T.C., *Cyphernomicon. Cypherpunks FAQ and More, Version 0.666*, 10.09.1994, http://www.cypherpunks.to/faq/cyphernomicron/cyphernomicon.html (dostęp: 20.12.2018).

May T.C., *True Nyms and Crypto Anarchy*, 2001, http://www.isfdb.org/cgi-bin/title.cgi?195636 (dostęp: 20.12.2018).

Michalski K., *Autonomizacja techniki i niepożądane skutki eliminowania człowieka jako źródła błędów*, „Filo-Sofija" 2017, nr 39(4/I).

Miller P., *Keyboard "Eavesdropping" Just Got Way Easier, Thanks to Electromagnetic Emanations*, Engadget, 20.10.2008, http://www.engadget.com/2008/10/20/keyboard-eavesdropping-just-got-way-easier-thanks-to-electrom/?guccounter=1 (dostęp: 20.12.2018).

Murray K.D., *The Great Seal Bug*, http://counterespionage.com/great-seal-bug-part-1/ (dostęp: 20.12.2018).

Nikitin P., *Leon Theremin (Lev Termen)*, „IEEE Antennas and Propagation Magazine" 2012, nr 54(5).

Pavithran M., *Eavesdropping on GSM*, „International Journal of Engineering Research in Computer Science and Engineering" 2016, nr 3(9).

Reis K., *The Eavesdropping Society. Electronic Surveillance and Information Brokering*, „Patents, Copyrights, Trademarks, and Literary Property", June 2001.

Simon B., *The Return of Panopticism: Supervision, Subjection and the New Surveillance*, „Surveillance & Society" 2005, nr 3(1).

Špaček S., Celeda P., Drašar M., Vizváry M., *Analyzing an Off-the-Shelf Surveillance Software. Hacking Team Case Study*, 2.06.2017, http://spi.unob.cz/papers/spi2017.html (dostęp: 20.12.2018).

Vuagnoux M., Pasini S., *Compromising Electromagnetic Emanations of Wired Keyboards, 2007–2009 Security and Cryptography Laboratory – LASEC/EPFL*, 2009, https://lasec.epfl.ch/keyboard/ (dostęp: 20.12.2018).

Waterman S., *„ Prism" a Vital Program Used to Collect Personal Web Data*, „Washington Times", 7.06.2013, http://www.washingtontimes.com/news/2013/jun/7/prism-used-collect-personal-web-data-clapper-says/ (dostęp: 20.12.2018).