JÓZEF PIOTR KNAP
Warszawski Uniwersytet Medyczny – Zakład Epidemiologii
i Komenda Główna Straży Granicznej
panknap1@gmail.com

ARKADIUSZ KOSOWSKI
Centrala Narodowego Funduszu Zdrowia
Departament ds. Służb Mundurowych
AK.gabi@o2.pl

CYBERATAK KONTRA MEDYCYNA
CYBERATTACK CONTRA MEDICINE

ABSTRACT

The „new" and growing problem of cybersecurity in the field (areas) of modern medicine *sensu largo* – is described. Authors stressed theoretical, practical (including: clinical) and legal problems of cyberattacks and bioterrorist attacks against medicine (e.g. contra patents, medical devices and hospital/outpatients clinic networks). Actual worldwide situation of cybersecurity in this issue is discussed.

Keywords: *cybersecurity, cyberattacks, cyberterrorism, medical devices*

STRESZCZENIE

W opracowaniu przedstawiono „nowy" i narastający problem zagrożeń cyberbezpieczeństwa w obszarze najszerzej pojętej współczesnej medycyny. Rozważono teoretyczne, praktyczne i legislacyjne skutki cyberataków i działań cyberterroru jako zagrożenia: dla konkretnych chorych, dla urządzeń medycznych, dla teleinformatycznych sieci w służbie zdrowia, dla potencjalnych działań ratowniczych. Ukazano aktualną sytuację cyberbezpieczeństwa w medycynie światowej, z zaakcentowaniem Polski.

Słowa kluczowe: *cyberbezpieczeństwo, cyberataki, cyberterroryzm, urządzenia medyczne*

WPROWADZENIE

Cyberatak jest zawsze uderzeniem w informację. Także w informację będącą podstawą każdego działania diagnostycznego, leczniczego i organizacyjnego w służbie zdrowia. Cyberatak jest więc – różnego rodzaju – zakłóceniem wytwarzania, przechowywania, przesyłania i wykorzystywania informacji, a także uderzeniem w jej dokładność, sprawdzalność i wiarygodność, czyli – prawdziwość.

Przybliżmy pojęcia do niedawna – jeszcze na przełomie wieków – mało znane i całkiem abstrakcyjne, zwłaszcza w aspekcie bezpośrednich zagrożeń dla medycyny. Klaryfikacja taka wydaje się konieczna, gdyż jest to pierwsze w polskim piśmiennictwie opracowanie dotyczące – szeroko pojętych – aspektów medycznych cyberbezpieczeństwa. Przytoczymy, w klasycznym ujęciu, zarówno pojęcia ogólne (podstawowe), jak i nowe, obowiązujące definicje zawarte w aktach normatywnych. Wciąż całkowicie nowe – i co więcej: całkiem obce w swej pozornej nierzeczywistości i wirtualnej abstrakcji – są bowiem same pojęcia „cyberprzestrzeni" i „cyberataku". Z trudnością uświadamiamy sobie i przyjmujemy bowiem zarówno wzajemne przenikanie się tego, co rzeczywiste, namacalne, z tym, co wirtualne. „Wirtualne" – a więc stworzone w umyśle ludzkim, ale istniejące w rzeczywistości lub mogące zaistnieć. Co więcej, zaskakuje nas, że cyberprzestrzeń, postrzegana wielokroć jako odrębny świat, mało konkretny i jakby nierzeczywisty, ma tak przemożny wpływ na codzienne realne bytowanie. W nowych, zaskakujących odsłonach powracają tu odwieczne problemy filozoficzne, wraz ze sporem o uniwersalia, w którym problem cyberprzestrzeni kontruje stanowisko nominalistów negujących rzeczywiste istnienie powszechników. Słynne tezy: „1.13. Światem są fakty w przestrzeni logicznej" czy „5.61. Logika wypełnia świat; granice świata są też jej granicami. W logice nie można zatem powiedzieć: to a to w świecie jest, a tamtego nie ma (...)", zawarte w „Tractatus logico-philosophicus" Ludwiga Wittgensteina (1889–1951) z roku 1922 (Wittgenstein, 2011), ukazywały całkiem nowe pojęcie „przestrzeni logicznej", i wraz z pracami największych polskich logików (Łukasiewicza, Leśniewskiego, Tarskiego, Ajdukiewicza i innych) tego okresu dawały asumpt do powstania pojęć wirtualnego cyberświata, wypełnionego jednak nad wyraz realnymi strukturami informacji i jej transferu. Należy ponadto przypomnieć, że jeśli – w swych założeniach ogólnych, ale i w praktyce codzienności – informacja powinna być przekazem **prawdy, to cyberatak**

uderza też w prawdę, także w kategoriach etycznych, powodując **dezinformację** również i w wymiarze aksjologicznym.

Pomijając, z konieczności, ale i z braku wystarczających kompetencji, genezę i kształtowanie się ontycznych i metodologicznych poglądów w omawianej kwestii, analizowaną zresztą przez polskich autorów (Berdel-Dudzińska, 2001; Sienkiewicz, 2015), nie można pominąć tu wielkiego wkładu znakomitego polskiego pisarza – futurologa, ale i wybitnego filozofa, lekarza z wykształcenia, Stanisława Lema (Jastrzębski, 2003; Okołowski, 2005). Idee odnośnie do styku informatyki, przestrzeni wirtualnych i filozofii zostały przezeń potężnie sformułowane już na początku lat 60. XX wieku, głównie w dziele „Summa technologiae", ale i w późniejszych, jak „Filozofia przypadku", „Golem XIV", „Bomba megabitowa", „Okamgnienie" i „Rasa drapieżców. Teksty ostatnie". W 1984 roku pisarz kanadyjski William Gibson użył po raz pierwszy określenia „cyberprzestrzeń" w kultowej dziś powieści „Neuromancer". W okresie tym zaczęto również podnosić aspekty socjologiczne („społeczności wirtualne", „społeczeństwo informatyczne") omawianego problemu i rozpatrywać jego wymiar światowy – w ścisłej łączności semantycznej i tematycznej z globalizacją (Szponar, 2004).

Warto jednak pamiętać, że omawiane tu zjawiska narodziły się, choć w niepomiernie węższym zakresie i daleko mniejszej złożoności, już wraz z pojawieniem się przed niemal 100 laty radia. Wiadomości przenoszone, jak to wówczas mówiono „na falach eteru", miały także potężną moc rażenia. Słynna audycja radiowa Orsona Wellesa (1915–1985) z 1938 roku o lądowaniu Marsjan, której rzekomy autentyzm wywołał w USA panikę – jest takiego wpływu pierwszym donośnym sygnałem (przykładem).

„Informacja (łac. *informatio* – przedstawienie, wizerunek; *informare* – kształtować, przedstawiać) – treść komunikatu, sens przekazywanej wiadomości. Potocznie: wiadomość, komunikat (ujęcie przedmiotowe), ale także: powiadomienie o czymś, zakomunikowanie czegoś, przekazanie wiadomości dotyczącej czegoś indywidualnemu lub zbiorowemu odbiorcy (ujęcie czynnościowe)" (Błasiak i Koszowy, 2003). Twórcą klasycznej ilościowej teorii informacji (1949) jest Claude Elwood Shannon (1916–2001). Ze zbitki pojęć „informacja" i „automatyka" w latach 70. XX wieku powstało określenie **informatyki**, ściśle związane z gromadzeniem, przechowywaniem, przetwarzaniem i przesyłaniem (transferowaniem) informacji za pomocą sprzętu komputerowego (telekomunikacja) – i później – sieci informatycznych (tele-

informatyka), które (coraz bardziej złożone i powszechne) zaczęły od połowy lat 90. XX wieku prowadzić do powstania „społeczeństwa informatycznego". Są to zagadnienia już bezpośrednio związane z treścią tego artykułu. Z kolei pojęcia z przedrostkiem „cyber" – mają swój źródłosłów w terminie „cybernetyka" wprowadzonym przez Norberta Wienera (1894–1964) w 1947 roku.

„Cybernetyka (gr. *he kybernetike* – sztuka sterowania, kierowania) – nauka o procesach sterowania i łączności w maszynach i organizmach żywych (abstrahująca od materialnego podłoża tych zjawisk) oraz o sposobach przekazywania informacji między częściami układu i między układami; jest działem matematyki stosowanej" (Lubański, Szymański, Zięba, 2001). Cybernetyka jest więc nauką o procesach informacyjnych (Tadeusiewicz, 2009) i stanowiła, jak to określał jeden z jej współtwórców, zarazem wybitny neurolog i psychiatra, W. Ross Ashby (1903–1972), nowe podejście do szeregu zjawisk oraz umożliwiła **wykrycie** pewnych mechanizmów kontroli w systemach żywych (i nie tylko), jak na przykład „sprzężenie zwrotne" (*feedback*), „sieci neuronowe", „algorytmy genetyczne" czy „sztuczna inteligencja", które okazały się niezbędne w zrozumieniu mechanizmów automatyki, informatyki, telekomunikacji, a i w samym tworzeniu tych pojęć (Ashby, 1963; Tadeusiewicz, 2009).

Pojęcie **cyberprzestrzeni** zostało wprowadzone do polskiego systemu prawnego w 2011 roku (Dz.U. 2011, nr 222 poz. 1323). We wprowadzeniu do tej ustawy napisano: „działalność w cyberprzestrzeni staje się nieodzownym warunkiem funkcjonowania państwa i społeczeństwa". W roku 2013 Rada Ministrów przyjęła Politykę Ochronną Cyberprzestrzeni.

- W listopadzie 2015 roku Rada Ministrów RP (uchwała 210/2015) przyjęła zaktualizowany „Narodowy Program Ochrony Infrastruktury Krytycznej (NPOIK)". Uchwała zawiera rozbudowany załącznik „Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje".
- W roku 2015 ogłoszona została „Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej", w której zrekapitulowano poszczególne pojęcia i definicje (podane skrótowo powyżej) oraz podano przesłanki – strategiczne kierunki działań – na rzecz stworzenia zintegrowanego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej.
- Przywódcy krajów NATO, zebrani na szczycie natowskim dnia 8 lipca 2016 roku w Warszawie, uznali cyberbezpieczeństwo za nową strefę działań operacyjnych, taką jak przestrzeń powietrzna, morze i ląd.

REGULACJE PRAWNE ODNOŚNIE DO CYBERBEZPIECZEŃSTWA W MEDYCYNIE

Wśród licznych już polskich aktów prawnych i dokumentów związanych z cyberbezpieczeństwem jedynie dwa odnoszą się bezpośrednio do zagrożeń cyberatakiem obszaru działań medycznych:

A. Ustawa z dnia 17 lutego 2005 roku o informatyzacji, działalności podmiotów realizujących zadania publiczne (Dz.U. 2005, nr 64 poz. 565; tekst jednolity: Dz.U. 2014, poz. 114). Zgodnie z jej art. 2.1. przepisy ustawy stosuje się (z pewnymi zastrzeżeniami) między innymi do:
   - samodzielnych publicznych zakładów opieki zdrowotnej,
   - ZUS i KRUS,
   - Narodowego Funduszu Zdrowia itd.

B. Rozporządzenie Ministra Zdrowia z dnia 9 listopada 2015 roku w sprawie rodzajów, zakresu i wzorów dokumentacji medycznej oraz sposobu jej przetwarzania (Dz.U. 2015, poz. 2069, z 8 grudnia 2015 r.). Rozporządzenie to należy traktować jako akt wykonawczy w stosunku do:
   - ustawy z dnia 15 kwietnia 2011 roku o działalności leczniczej (Dz.U. 2011, nr 112 poz. 654) – z późniejszymi zmianami,
   - ustawy z dnia 28 kwietnia 2011 roku o systemie informacji w ochronie zdrowia (Dz.U. 2011, nr 113 poz. 657). Ustawa ta nakłada na placówki ochrony zdrowia obowiązek informatyzacji dokumentacji medycznej; tak więc wszystkie podmioty prowadzące działalność leczniczą powinny wdrażać system **Elektronicznej Dokumentacji Medycznej (EDM**), co – w założeniu – ma znacznie usprawnić funkcjonowanie systemu ochrony zdrowia. Zgodnie z art. 5 cytowanej ustawy z dnia 28 kwietnia 2011 roku, System Informacji w ochronie zdrowia obejmuje bazy danych funkcjonujące w ramach:
     1. Systemu Informacji Medycznej (SIM).
     2. Dziedzinowych systemów teleinformatycznych, np.:
        - Systemu Rejestru Usług Medycznych NFZ („RUM -NFZ”),
        - Systemu Statystyki w Ochronie Zdrowia,
        - Systemu Ewidencji Zasobów w Ochronie Zdrowia,
        - systemu wspomagania Ratownictwa Medycznego,
        - Systemu Monitorowania Zagrożeń itd.

Wyobraźmy sobie skutki zmasowanego ataku na wymienione struktury, który ponadto przebiegać może z całkowitą utratą danych zawartych w ww. systemach.

C. Pośrednio, problemu medycznego (katastrofy) dotyczy także art. 3, ust. 1, pkt 4 ustawy z dnia 3 sierpnia 2011 roku o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych, mówiący: „katastrofę naturalną lub awarię techniczną mogą wywołać również zdarzenia w cyberprzestrzeni oraz działania o charakterze terrorystycznym".

Cytowana ustawa z dnia 17 lutego 2005 roku definiuje dwa ważne pojęcia. Są to:

- **Interoperacyjność** – „zdolność różnych podmiotów oraz używanych przez nie systemów teleinformatycznych i rejestrów publicznych do współdziałania na rzecz osiągnięcia wzajemnie korzystnych i uzgodnionych celów, z uwzględnieniem współdzielenia informacji i wiedzy (...)".
- **Krajowe Ramy Interoperacyjności (KRI)** – „zestaw wymagań semantycznych, organizacyjnych i technologicznych dotyczących interoperacyjności systemów teleinformatycznych i rejestrów publicznych". Podstawowe w tym zakresie jest rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 roku, znowelizowane i podane w postaci tekstu jednolitego jako obwieszczenie Prezesa Rady Ministrów z dnia 14 stycznia 2016 roku w sprawie ogłoszenia jednolitego tekstu rozporządzenia Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz.U. 2016, poz. 113).

W rozporządzeniu tym wprowadzono też dalsze definicje w omawianym temacie; przytoczymy cztery z nich:

- obiekt przestrzenny – w rozumieniu przepisów ustawy z dnia 4 marca 2010 roku o infrastrukturze informacji przestrzennej (Dz.U. 2016, poz. 113),
- podatność systemu teleinformatycznego – właściwość systemu teleinformatycznego, która może być wykorzystana przez co najmniej jedno zagrożenie,

- polityka bezpieczeństwa informacji – zestaw efektywnych, udokumentowanych zasad i procedur bezpieczeństwa wraz z planem ich wdrożenia i egzekwowania,
- zagrożenia systemu teleinformatycznego – potencjalna przyczyna niepożądanego zdarzenia, które może wywołać szkodę w systemie teleinformatycznym.

System zarządzania bezpieczeństwem informacji jest w Polsce oparty o Polską Normę PN-ISO/IEC 27001 [wprowadza ISO/IEC 27001: 2013 (E) (E)]. Tam też zawarte są definicje, jak np.:

- bezpieczeństwo informacji,
- zdarzenie związane z bezpieczeństwem informacji,
- incydent związany z bezpieczeństwem informacji,
- system zarządzania bezpieczeństwem informacji.

Z kolei ustawa z dnia 6 listopada 2008 roku o prawach pacjenta i Rzeczniku Praw Pacjenta (Dz.U. 2008, nr 52 poz. 417, z późn. zm.) porusza zagadnienia praw chorego, które mogą być naruszone wskutek cyberataku (np. bezprawne ujawnienie danych osobowych).

METODYCZNE I REALNE PROBLEMY CYBERATAKÓW W MEDYCYNIE

Ten nieco zawiły wstęp usprawiedliwia autorów o tyle tylko, że ukazuje z jednej strony już istniejący spis aktów prawnych, dotyczący jednak głównie tezauryzacji, przekazywania i ochrony danych teleinformatycznych, z drugiej zaś – zderza niejako istniejącą już w polskim prawodawstwie legislaturę z niezmierną złożonością wieloaspektowego oraz interdyscyplinarnego problemu określonego przez nas najogólniej: „cyberatak kontra medycyna".

Anglosaskie pojęcie **urządzeń medycznych – *Medical Devices* (MD)** jest zdefiniowane bardzo szeroko i precyzyjnie zarazem: „**Medical Devices:** An instruments, apparatus, implement, machine, contrivance, implant, in vitro reagent, or rather similar or related article, including a component part, or accessory (...) intended for use in the diagnosis of disease or other conditions, or in the cure, mitigations, treatment or prevention of disease (...)" (Williams i Woodward, 2015). Sądzimy, że definicja powinna być szeroko przyjęta. Całokształt zagadnień związanych z MD (także

więc ich cyberbezpieczeństwa) stał się przedmiotem, wydanej ostatnio, obszernej monografii (Fiedler, 2016). W cytowanej, metodycznej i źródłowej pracy Williams i Woodward rozwinęli również charakterystykę pojęcia „cyberbezpieczeństwa" (*cybersecurity*), właśnie w odniesieniu do *Medical Devices* i szpitalnych (zakładowych) sieci (*network*) tych urządzeń. Za właściwą dla zastosowania odnośnie do medycyny uważają oni następującą, również ostatnio podaną, definicję (Craigen i Diakun-Thibault, 2014): **„Cybersecurity** entails the safeguarding of computer networks and the information they contain from penetration and from malicious damage or disruption".

Precyzyjną charakterystykę cyberataków na urządzenia medyczne (*Medical Devices*) i szpitalne sieci informatyczne (*hospital networks*) oraz ich konsekwencje medyczne i prawne przedstawiła Katherine B. Wellington z Uniwersytetu Yale, USA (Wellington, 2013). W zależności od celu, na który ukierunkowany jest cyberatak, wyróżniła:

1. Cyberatak na indywidualną aparaturę medyczną (*C. on Individual Medical Devices*).
2. Cyberatak na szpitalne sieci informatyczne (*C. on Hospital Networks*).
3. Cyberatak nakierowany na kradzież informacji medycznych.

Cele 1, 2, 3 – mogą się na siebie wzajemnie nakładać i zazębiać pojęciowo, co dotyczy zarówno sieci generatorów danych (dane kliniczne i laboratoryjne chorych, ceny i stany składowe leków itd.), jak i ich przesyłu i właściwego odbioru.

Cyberatak na indywidualną aparaturę medyczną (*C. on Individual Medical Devices*) może doraźnie zagrażać życiu i zdrowiu chorego. Zatrzymanie lub zbrodnicze przeprogramowanie pracy urządzenia monitorującego i/lub kontrolującego funkcje życiowego organizmu chorego człowieka może doprowadzić do zgonu (i to zgonu, którego ustalenie przyczyny może być bardzo trudne). Narażeni będą więc pacjenci pozostający na oddechu kontrolowanym lub wspomaganym (respiratory), poddawani zabiegom nerkozastępczym (hemodializy – „sztuczne nerki"), detoksykacyjnym (hemofiltracja, plazmafereza, separatory komórkowe itd.), noworodki przedwcześnie urodzone pozostające w tzw. inkubatorach, chorzy poddawani terapii hiperbarycznej, pacjenci poddawani precyzyjnym zabiegom operacyjnym za pomocą urządzeń stereotaktycznych (neurochirurgia) i robotów chirurgicz-

nych oraz poddawani różnego rodzaju radioterapii z powodu nowotworów, bardzo liczni już dziś w rozwiniętych społeczeństwach chorzy z wszczepionymi stymulatorami pracy serca i defibrylatorami, czy wreszcie diabetycy korzystający z pomp insulinowych. Zwłaszcza trzy ostatnio wymienione urządzenia, niejako bezpośredniego stałego wsparcia chorego organizmu, są szczególnie narażone na atak indywidualny (Halperin i wsp., 2008; Nathanel i wsp., 2011). Oto na przykład przeprogramowanie pompy insulinowej, tak by sygnalizowała zbyt wysoki poziom glukozy w organizmie (hiperglikemia), spowoduje wyrzut zbytecznej w istocie dawki insuliny, co prowadzić może do gwałtownego zgonu w mechanizmie ostrego niedocukrzenia (hipoglikemii) (Nathanel i wsp., 2011). Oceniono w 2008 roku, że wobec potencjalnych aktów cyberterroru skierowanych przeciw wszczepionym stymulatorom pracy serca i defibrylatorom nie dysponujemy praktycznie żadną skuteczną obroną („software radio attack and zero-power defenses") (Halperin i wsp., 2008). Po filmie fabularnym „Homeland", obrazującym skuteczny cyberatak na stymulator serca prezydenta USA, były wiceprezydent USA Dick Chenay ujawnił, że jego wszczepiony defibrylator został zmodyfikowany w obawie przed cyberatakiem.

Obecnie trwają na świecie wielokierunkowe, interdyscyplinarne i wręcz gorączkowe prace nad „uszczelnieniem" cyberbezpieczeństwa urządzeń teleinformatycznych stosowanych w służbie zdrowia. W 2015 roku wielka rządowa Agencja do Spraw Żywności i Leków (FDA – *Food and Drug Administration*) wdrożyła oficjalne działania dotyczące cyberbezpieczeństwa w zakresie swej odpowiedzialności ustawowej (FDA, 2014, także FDA, 2016).

Jeśli chodzi o cyberatak na szpitalne sieci informatyczne (*C. on Hospital Networks*) oraz cyberatak nakierowany na kradzież informacji medycznych, akty cyberterroru uderzają zarazem w oba punkty, rozróżnione przez Wellington, jedynie w celach dydaktycznych i klasyfikacyjnej poprawności. Wytworzony chaos (opisany poniżej) zagraża, zarówno bezpośrednio, jak i pośrednio, zdrowiu i życiu chorych, generuje wielkie straty ekonomiczne i może dezorganizować pracę służby zdrowia na wielkich obszarach, a nawet na terenie całego kraju (np. USA).

Określone przez Katherine Wellington zasadnicze kierunki i rodzaje cyberataków nie wyczerpują możliwości i zasięgu uderzenia w struktury bezpośrednio i pośrednio związane z medycyną: zdrowiem publicznym, bezpieczeństwem zdrowotnym, nadzorem epidemiologicznym – najogól-

niej – w **infrastrukturę krytyczną** w rozumieniu art. 5 pkt 7 ustawy o zarządzaniu kryzysowym z dnia 26 kwietnia 2007 roku. W pewnym uproszczeniu infrastrukturę krytyczną można określić jako rzeczywiste i cybernetyczne systemy, niezbędne do minimalnego funkcjonowania państwa. Wymieńmy tu przykładowo uderzenie w Państwowe Ratownictwo Medyczne, określone ustawą z dnia 8 września 2006 roku (Dz.U. 2006, nr 191 poz. 1410 z późn. zm.) – wraz z systemem wspomagania Ratownictwa Medycznego (Dz.U. 2011, nr 113 poz. 657), w system zaopatrzenia w leki i sprzęt medyczny i ich ogólnokrajową dystrybucję, w system tezauryzacji danych medycznych zbieranych w celach statystycznych, demograficznych i epidemiologicznych, nieraz przez dziesiątki lat. Zwłaszcza precyzyjne cyberataki przeciwko działaniom ratowniczym podejmowanym w stosunku do katastrof, zarówno naturalnych, jak i wywołanych przez człowieka (także intencjonalnie – właśnie jako akt cyberterroru), mogą być atakami na infrastrukturę krytyczną konkretnego państwa o potencjalnie trudnych nawet do wyobrażenia, tragicznych następstwach. Z zasygnalizowaną tu jedynie problematyką cyberbezpieczeństwa muszą być więc dogłębnie zaznajomione struktury obrony i ochrony państwa i przedstawiciele wszystkich służb czuwających, a więc ludzie tworzący tzw. grupy supozycyjne (Maciejewski, 2014), w tym oczywiście – służb medycznych i ratunkowych.

Jak częstym zjawiskiem są cyberataki na MD? Precyzyjna odpowiedź nie jest możliwa poza ogólnymi stwierdzeniami o wybitnym zróżnicowaniu pomiędzy poszczególnymi państwami i kontynentami oraz niewątpliwym narastaniu rozmiaru zjawiska w skali globu. Stany Zjednoczone Ameryki Północnej są niewątpliwie państwem, w którym zjawisko to występuje najczęściej i na największą skalę, lecz dane o cyberatakach kontra medycyna pochodzą już także z innych kontynentów i krajów (np. Chiny, Australia).

Oto niekompletna lista przykładów:

- W latach 2009–2013 odnotowano 804 włamania do zastrzeżonych informacji medycznych, naruszając 29 276 385 zapisów (*records*) dotyczących pacjentów. Tylko w 2013 roku nastąpiły włamania do danych o 7 095 145 pacjentach. W 2012 roku nastąpił wzrost naruszonych danych pacjentów o 137,7%.
- W latach 2013–2014 przeprowadzono w USA dwa cyberataki na sieć Beecher's Hospital, dezorganizując prace i wręcz powodując chaos w 20 szpitalach o 31 000 łóżek w 29 stanach.

- W pojedynczym największym ataku hakerskim na Community Health Systems (CHS) wykradziono 4 029 530 danych (*records*) dotyczących chorych z 206 szpitali w 29 stanach USA.
- Atak na US Department of Veteran Affairs doprowadził do wykradzenia około 50 tysięcy danych.
- Rok 2016. Zaatakowano system MedStar Washington Hospital Centre: 10 szpitali i 250 przychodni. Chorzy leczeni byli bez wyników badań laboratoryjnych, co obrazuje dowodnie, że ataki tego typu są przykładem cyberterroru skierowanego bezpośrednio przeciwko życiu i zdrowiu ludzi.
- Jedyny w swoim rodzaju cyberatak *a rebours* przeprowadziła 15 marca 2003 roku w USA rządowa amerykańska Agencja do spraw Walki z Narkotykami (DEA – *Drug Enforcement Administration*). Po raz pierwszy w historii DEA przeprowadziła oficjalny atak przeciwko sklepom sprzedającym narkotyki, dopalacze i fajki wodne. Chociaż cyberatak był „łagodny", miał charakter głównie prewencyjny: osoby wchodzące na witrynę internetową tych sklepów wchodziły w istocie na stronę agencji DEA, która wyświetla treści ostrzegające przed zakupami, spotkał się z nasiloną polemiką.

W Polsce, z krakowskiego szpitala przekazano blisko 500 tysięcy złotych na konto oszusta, który podszywając się pod dostawcę leków, poinformował w e-mailu o zmianie konta bankowego.

Powyższe dane są nie tylko przykładowe, ale i z pewnością niepełne odnośnie do rozeznania rzeczywistej skali „cyberataków kontra medycyna" w USA, jak i ich kosztów finansowych, pomijając – jakże istotne – imponderabilia związane ze skutkami w postaci śmierci i dodatkowych schorzeń pacjentów, wynikających z aktów bioterroru przeciwko, najszerzej pojętym, strukturom medycznym. Zachodzą tu bowiem dwa znane w epidemiologii, a nakładające się zjawiska dotyczące ich rzeczywistej częstości. Jednym jest niepełne ich zgłaszanie (*underestimation*), drugim – dalece niepełne rozpoznanie (*underdiagnosed*) hakerskich cyberataków na urządzenia i infrastrukturę medyczną. Ponadto prominentne ofiary cyberataków (wielkie sieci szpitali, centrale dystrybucji leków, korporacje farmaceutyczne, systemy ubezpieczeniowe) niechętnie przyznają się – jako świadczeniodawcy „usług" medycznych, do braku ich bezpieczeństwa. Część danych jest także z pewnością utajnionych. Ponadto w Polsce cyberataki na struktury me-

dyczne mogą być z pewnością nierozpoznane i przypisywane (jak często?) „zwykłym" awariom sprzętu i omyłkom operatorów.

We wszystkich państwach rozwiniętych postępuje coraz powszechniejsze stosowanie – wprowadzonych już w poprzednich latach – technologii informacyjnych w służbie zdrowia. Jedna z zasadniczych (flagowych) inicjatyw Unii Europejskiej: „Strategia Europy 2020" – wprowadza pojęcie Agendy Cyfrowej, której celem ma być „maksymalizacja społecznego i ekonomicznego potencjału technologii informacyjnych i telekomunikacyjnych (ICT)", w tym ich wprowadzenie do wszystkich „usług medycznych", jak żargonowo i pozbawiając ich personalistycznego nazywania, określa się całokształt działań profilaktycznych, diagnostycznych i leczniczych współczesnej medycyny. W dosłownie każdym dokumencie oficjalnym, publikacji czy dyskusji na temat poprawy wydajności ochrony zdrowia publicznego pojawiają się pojęcia „E-health" lub „e-zdrowie". Pojawiły się oficjalne inicjatywy interoperacyjności i telemedycyny, np.: „Calliope" (interoperacyjność w e-zdrowiu), „epSOS" (platforma e-usług dla pacjentów europejskich), „Renewing Health", „eHealth for Regions for Regions. Integrated Structures in the Baltic Sea Area". Opisany proces postępuje od kilku lat również w Polsce, np. wprowadzony system „Ewuś". Awaryjność rozwiązań sieciowych znamy z codziennej praktyki („system się zawiesił", „awaria systemu"); jednak skala zagrożeń cyberatakami (a nawet sama ich możliwość) nie jest jeszcze u nas, odnośnie do ochrony zdrowia, brana poważnie pod uwagę (poza pierwszymi sygnałami ze strony prywatnych właścicieli sieci laboratoriów diagnostycznych). Paradoksalnie, pewnym atutem jest w Polsce niewątpliwe zapóźnienie w procesach informatyzacji służby zdrowia i struktur pokrewnych. Oczekiwać należy, że informatyzacja – także w służbie zdrowia – postępować będzie u nas równolegle z tworzeniem systemów zabezpieczających: niezwykle złożonych, drogich i nadal nie w pełni skutecznych. Interdyscyplinarne i międzyresortowe wypracowanie takich zabezpieczeń systemowych nie jest zadaniem łatwym ani tanim. Prace takie zostały już podjęte wspólnie z Ministerstwem Cyfryzacji, między innymi w ramach działań tworzenia „e-państwa" i Narodowego Operatora Sieci Strategicznych (Burgemeister, 2016; Ruman, 2016).

Podsumowaniem realności zagrożenia cyberatakami cyberterroryzmem mogą być słowa prezydenta USA Baracka Obamy, wypowiedziane 12 lutego 2013 roku: „America must also face the rapidly growing threat from

cyber-attacks… We cannot look back years from now and Wonder with we did nothing in the face of real threats to our security and our economy".

A może należy postawić półżartem obrazoburczą tezę, że najbardziej zacofani (opóźnieni w informatyzacji) są najbardziej bezpieczni?

WNIOSKI

1. Realne i pojawiające się już zagrożenie za strony cyberataków (cyberterroryzmu) wymierzonego we wszystkie struktury najszerzej pojętej współczesnej medycyny jest nowym, ale gwałtownie narastającym wyzwaniem nie tylko dla decydentów służby zdrowia, ale i dla władz wszystkich cywilizowanych państw świata.
2. Wymóg zapewnienia cyberbezpieczeństwa w stosunku do działalności medycznej (chorych, aparatury medycznej, sieci teleinformatycznej służby zdrowia, farmakoekonomiki) staje się jednym z najważniejszych globalnych wyzwań stających przed medycyną obecnej doby.
3. Szacowanie ryzyka takich cyberataków (wraz z oceną ich źródeł, metod, szkodliwości) oraz systemowe i interdyscyplinarne wdrażanie działań zaradczych (wraz z oceną ich realnej skuteczności i efektywności – także „cost-benefit analysis") wymaga natychmiastowych działań, podjętych już zresztą w wielu krajach świata (USA, Australia, Nowa Zelandia, Chiny i inne), a zapoczątkowanych ostatnio także w Polsce.

Bibliografia

Ashby W.R. (1963). *Wstęp do cybernetyki*. Państwowe Wydawnictwa Naukowe. Warszawa.

Błasiak Z.A., Koszowy M. (2003). *Informacja*, [w:] A.M. Krąpiec, A. Lobato, P. Jaroszyński, H. Kiereś, Z.J. Zdybicka (red. nauk.). *Powszechna Encyklopedia Filozofii*. Tom 4 (Go-Iq). Wyd. PTTA – SITA. Lublin. s. 824–829.

Bógdał-Brzezińska A., Gawrycki M.F. (2003). *Cyberterroryzm i problemy bezpieczeństwa narodowego we współczesnym świecie*. ASPA-JR. Warszawa.

Burgemeister S. (14 czerwca 2016 r.). Realizacja okresowego audytu wewnętrznego w zakresie bezpieczeństwa teleinformatycznego. Przykłady dobrych praktyk. MSWiA. Pierwsza Konferencja szkoleniowa audytorów wewnętrznych w resorcie spraw wewnętrznych i administracji. MSWiA. Warszawa. Materiały e-mailowe, s. 24–58.

Craigen D., Diakun-Thibault N., Purse R. (2014). *Defining Cybersecurity*. „Technology Innovation Management Review", nr 4 (10), s. 13–21.

Doktryna Cyberbezpieczeństwa Rzeczypospolitej Polskiej. Biuro Bezpieczeństwa Narodowego. Warszawa 2015.

Fiedler B.A. (red.) (2016). *Managing Medical Devices within a Regulatory Framework*. Elsevier. Amsterdam.

Halperin D., Heydt-Benjamin T.S., Ransford B., Clark S.S., Defen B. et al. (2008). *Implantable Cardiac Deffibrillations: Software Radio Attack and Zero-Power Defenses*, [w:] *Security and Prevency*. SP 2008 IEEE Symposium. Oakland, California, USA. May 18–22, 2008, s. 129.

Jastrzębski J. (2003). *Chaos na cenzurowanym, późna eseistyka Lema*. „Zagadnienia Filozofii w Nauce", XXXIII, s. 47–63.

Kowalewski J., Kowalewski M. (2014). *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*. „Telekomunikacja i Techniki Informacyjne", nr 1–2, s. 24 –32.

Kramer D.B., Baker M., Ransford B., Molina-Markham A., Stewart Q., Fu K., Reynolds M.R. (2012). *Security and Privacy Qualities on Medical Devices: An Analysis of FDA Postmarket Surveillance*. PLoS One. 7(7), e40200.

Lubański M., Szymański A., Zięba S. (2001). *Cybernetyka*, [w:] A.M. Krąpiec, A. Lobato, P. Jaroszyński, H. Kiereś, Z.J. Zdybicka (red. nauk.). *Powszechna Encyklopedia Filozofii*. Tom 1 (A-C). Wyd. PTTA – SITA. Lublin, s. 326–329.

Maciejewski J. (2014). *Grupy dyspozycyjne. Analiza socjologiczna*. Wydanie II. Wydawnictwo Uniwersytetu Wrocławskiego. Wrocław.

Mider D. (2013). *Analiza pojęcia cyberterroryzmu. Próba uporządkowania chaosu*. Annales Universitatis Mariae Curie-Skłodowska. Lublin – Polonia. Sectio K., XX, 2, s. 81–114.

Okolowski P. (2005). *Stanisław Lem*, [w:] W. Mackiewicz (red.), *Polska filozofia powojenna*. AW Witmark. Warszawa, Tom III, s. 179–204.

Patelak A. (2005). *Cyberterroryzm a bezpieczeństwo Rzeczypospolitej.* II. *Problem cyberterroryzmu w polityce ONZ, UE, NATO, USA i Rosji*. „Biuletyn Centralnego Ośrodka Szkolenia Straży Granicznej", 34 (3), s. 81–95.

Ruman S. (22–28 sierpnia 2016). *Powołajmy narodowego operatora sieci strategicznych*. „W Sieci".

Sienkiewicz P. (2015). *Ontologia cyberprzestrzeni*. „Zeszyty Naukowe Wyższej Szkoły Informatyki", nr 13, s. 89–102.

Szpunar M. (2004). *Społeczności wirtualne jako społeczności – próba ujęcia socjologicznego*, [w:] M. Radochoński, B. Przywara (red.) *Jednostka – grupa – cybersieć. Psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*. WSiZ. Rzeszów , s. 157–184.

Tadeusiewicz R. (red.), (2009). *Neurocybernetyka teoretyczna*. Wydawnictwa Uniwersytetu Warszawskiego. Warszawa.

Talbot D. (2012, October 17). *Computer Viruses are "Rampant" an Medical Devices in Hospitals*. Massachussets Institute of Technology (MIT). Technology Review.

US Food and Drug Administration (FDA). *Content of Premarket Submision for Management of Cybersecurity in Medical Devices*. US FDA, 2014 [Accessed June 9, 2015].

Wellington K.B. (2013). *Cyberattacks on medical devices and hospital networks: legal gaps and regulatory solutions*. „Santa Clara High Technology Law Journal", 30, 2, s. 138–200.

Williams P.A.H., Woodward A.J. (2015). *Cybersecurity vulnerabilities in medical devices: a complex environmental and multifaceted problem*. Medical Devices (Auckland). 8, s. 305–316.

Wittgenstein L.: *Tractatus logico-philosphicus*. Tłum. B. Wolniewicz. PWN. Warszawa 2011.

Źródła internetowe

Berdel-Dudzińska M. (bez daty, po 2011). *Pojęcie cyberprzestrzeni we współczesnym polskim porządku prawnym*. Profinfo.pl.