Bogusław Olszewski
Uniwersytet Wrocławski

Ataki cyber-fizyczne a system bezpieczeństwa narodowego

Słowa kluczowe: system cyber-fizyczny, bezpieczeństwo międzynarodowe, cyberprzestrzeń

Uwagi wstępne

Klasyczne cyberataki skupiają się głównie na zawartości informacyjnej, obierając jako cel zarówno urządzenia umożliwiające wymianę danych w obrębie Sieci, jak i przechowywane na nich zasoby, naruszając integralność, poufność i dostępność danych (tzw. triada CIA). Powszechność i dynamiczny rozwój systemów obliczeniowych oraz rozległość łączącej ich infrastruktury telekomunikacyjnej poszerzyły zakres możliwych podatności na atak daleko poza zakłócenie i ograniczenie funkcji urządzeń będących elementami globalnej sieci informacyjnej, realizowanych zwłaszcza w warstwie World Wide Web. Technologie telekomunikacyjne (*information and communication technologies*, ICT) umożliwiają współcześnie nie tylko oddziaływanie na poziomie cyfrowym (logicznym) dla uzyskania pożądanych zdarzeń w dowolnym punkcie cyberprzestrzeni, ale dzięki systemom cyber-fizycznym (*cyber-physical systems*, dalej C-F) stanowią o zaistnieniu tychże w świecie rzeczywistym. Systemy te łączą świat fizyczny i cyberprzestrzeń, umożliwiając wpływanie na rzeczywistość materialną z poziomu warstwy cyfrowej. Pozwalają na ingerencję z jednej lokacji fizycznej w drugą, z wykorzystaniem Internetu jako medium transmisyjnego generującego zamierzone efekty kinetyczne. Dotychczasowy paradygmat charakterystyczny dla świata ery preindustrialnej, kiedy oddziaływanie na elementy świata materialnego wymagało podjęcia adekwatnych działań w obrębie tej samej płaszczyzny, uległ zmianie.

Współcześnie, w efekcie trzeciego etapu rewolucji naukowo-przemysłowej związanego z informatyzacją, systemy automatyki występują powszechnie w połączeniu z urządzeniami IT. Wielorakie konfiguracje umożliwiają ich nadzór z dowolnego miejsca globu, podobnie odczyt i modyfikację parametrów procesów produkcyjnych czy sterowanie elementami układów hydroinżynieryjnych. Na potrzeby niniejszego artykułu przyjęto definicję Helen Gill z National Science Foundation, w myśl której systemy C-F są: „Fizycznymi, biologicznymi i inżynierskimi systemami, których operacje są zintegrowane, monitorowane i/lub kontrolowane przez centrum [rdzeń] obliczeniowe. Komponenty są w każdej skali usieciowione. przetwarzanie danych jest głęboko osadzone w każdym komponencie […] system wbudowany stanowi rdzeń obliczeniowy, zwykle wymaga natychmiastowej odpowiedzi, a sam system jest najczęściej rozproszony”[1].

Ataki cyber-fizyczne stanowią naruszenie bezpieczeństwa cyberprzestrzeni, oddziałują w sposób niepożądany na przestrzeń materialną, skutkując przejęciem kontroli nad kluczowymi aspektami systemu C-F oraz posiadają rozprzestrzeniający się efekt fizyczny. Stały się immanentną częścią współczesnego systemu bezpieczeństwa międzynarodowego, o którym Tomasz Aleksandrowicz pisze: „widoczne jest dążenie do zacierania granic pomiędzy bezpieczeństwem wewnętrznym i zewnętrznym”[2]. Ataki C-F mogą naruszyć (bezpośrednio lub pośrednio) stabilność systemu bezpieczeństwa narodowego oraz międzynarodowego. Wpływając na zachowania podmiotów państwowych i niepaństwowych zmieniają jego strukturę i dynamikę. Już kilka dekad temu Richard Ullman, mówiąc o koncepcji bezpieczeństwa i katalogu zagrożeń, zauważał ich ekspansję – obecnie coraz częściej podkreśla się znaczenie bezpieczeństwa ludzkiego (indywidualnego)[3]. Ten ostatni wymiar staje się nad wyraz istotny w kontekście systemów cyber-fizycznych, tym bardziej że „bezpieczeństwo splata się tymczasem również w zasadniczych swych wymiarach: jednostkowym, narodowym i międzynarodowym”[4].

[1] H. Gill, *A Continuing Vision: Cyber-Physical Systems*, Arlington 2008, s. 3, źródło: https://www.ece.cmu.edu (dostęp: 27.07.2016).
[2] T. R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 206.
[3] R.H. Ullman, *Redefining Security*, „International Security” 1983, vol. 8, no. 1, ss. 129-153.
[4] J. Stańczyk, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 47.

Elementy systemów cyber-fizycznych

Komponenty otoczenia cyber-fizycznego można podzielić na kilka podstawowych grup: przetworniki (czujniki oraz aktuatory – urządzenia wykonawcze), kontrolery – w tym programowalne kontrolery logiczne PLC (*Programmable Logic Controler*), systemy wbudowane (osadzone, *embedded systems*), rozproszone systemy sterowania DCS (*Distributed Control Systems*), SCADA (*Supervisory Control And Data Acquisition)* oraz tzw. Internet rzeczy (*Internet of Things*, dalej IoT).

Przetworniki (*transducers*) pozwalają na wymianę i translację stanów energetycznych z informacyjnych na fizyczne i odwrotnie. Wśród nich można wyróżnić czujniki (*sensors*) mierzące wilgotność, ciśnienie atmosferyczne, dystans, ruch, temperaturę, promieniowanie, stan danych funkcji organizmu itp., przesyłające odczyty stanów fizycznych w postaci sygnałów elektrycznych interpretowanych następnie przez system komputerowy. Kontrolery monitorują i korygują zadane warunki działania systemów pod wpływem sygnałów napływających ze zmieniającego się, otaczającego środowiska; aktuatory z kolei zamieniają sygnał elektryczny na ruch mechaniczny, umożliwiając zwrotne oddziaływanie kinetyczne. Systemy osadzone są najczęściej układami elektronicznymi opartymi na mikroprocesorze, są preprogamowane i posiadają ograniczoną funkcjonalność wynikającą z przeznaczenia danego urządzenia, zaś ich oprogramowanie jest, zgodnie z tzw. modelem Berkeley, „ściśle zintegrowane z zarządzanymi procesami fizycznymi”[5]. Typowy system osadzony składa się z interfejsu użytkownika, pamięci, procesora, konwerterów, czujników, portów diagnostycznych, programowalnych układów logicznych, układu wejścia/wyjścia i zasilania.

Sterowniki PLC są kontrolerami pozwalającymi organizować działania logiczne na poziomie urządzenia za pomocą tzw. drabinkowego języka programowania. Automatyzują nadzór nad maszyną, są dedykowaną stacją zdolną obsługiwać wiele rodzajów czujników i aktuatorów. Coraz częściej połączone z rozproszonymi systemami sterowania DCS, które należą do przemysłowych narzędzi kontroli, są zorientowane głównie na procesy produkcyjne przedsiębiorstwa. Stanowią swego rodzaju etap pośredni w łańcuchu kontroli i sterowania agregatami w rodzaju linii produkcyjnych, pozostają najczęściej długookresowo włączone do Sieci. Z kolei systemy SCADA są zorientowane na dane rozproszone geograficznie, a ich istotą jest możliwość odczytu i modyfikacji żądanej informacji (parametrów) w czasie

[5] E. A. Lee, *The Future of Embedded Systems*, źródło: https://chess.eecs.berkeley.edu (dostęp: 28.07. 2016).

rzeczywistym. Jako takie „pozwalają na uzyskanie szybkiego wglądu w faktyczny stan urządzeń produkcyjnych i wykonawczych […] umożliwiają szybką lokalizację alarmów, podstawowe logowanie danych czy też automatyczną reakcję na określone sygnały pochodzące z urządzeń”[6]. System SCADA w warstwie graficznej odpowiada za jednoznaczne zaprezentowanie dynamicznie zmieniającej się informacji. W systemie tego typu „zdefiniowane przez użytkownika algorytmy logiczne przyspieszają i wspomagają operatora w jego pracy”[7], a w szerszej perspektywie system SCADA jest „podstawowym źródłem danych dla systemów nadrzędnych i przemysłowych baz danych”[8]. Dostęp do odległych lokacji, które mogą być monitorowane i zarządzane przez operatora bezpośrednio lub zdalnie poprzez dedykowane urządzenia dostępowe, odbywa się przez transmisję danych telemetrycznych realizowaną za pomocą interfejsu RTU (*Remote Terminal Unit*)[9]. Systemy SCADA posiadają formę specjalistycznego oprogramowania uruchamianego na komputerach produkowanych seryjnie lub występują w postaci urządzeń z preinstalowanym oprogramowaniem, działającym wyłącznie na danej platformie fizycznej.

Ostatnią grupę, Internet rzeczy (*Internet of Things*), nazywany także Internetem wszystkiego, stanowi globalna infrastruktura fizycznych obiektów pozostających online, „to wzajemne połączenie unikatowych wbudowanych urządzeń komputerowych”[10]. W ramach Internetu, głównie na gruncie sieci dedykowanych wyłącznie dla IoT (Ethernet, a przede wszystkim bezprzewodowe: WiFi i Bluetooth), urządzenia wymieniają dane zebrane z otoczenia za pośrednictwem czujników. Ten typ komunikacji *machine-to-machine* (M2M) umożliwia współdzielenie danych w kierunku pełnej automatyzacji ich funkcji. Sprzęt AGD i RTV, aparatura medyczna, pojazdy, a w konsekwencji całe obszary fizyczne są traktowane jako inteligentne węzły (domy, dzielnice, miasta, państwa) i mogą stać się częścią sieci złożonej z miliardów elementów, tworzących w efekcie inteligentne otoczenie. Interpretacji i dalszej implementacji pozyskanych danych ma służyć koncepcja Big Data[11],

[6] *Systemy SCADA*, http://www.astor.com.pl (dostęp: 28.07.2016).
[7] *Ibidem*.
[8] *Ibidem*.
[9] Szerzej na ten temat: *Remote Terminal Unit (RTU)*, http://www.wbsetcl.in (dostęp: 28.07.2016).
[10] M. Miller, *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016, s. 23.
[11] Szerzej na ten temat: S. Mukherjee, R. Shaw, *Big Data – Concepts, Applications, Challenges and Future Scope*, „International Journal of Advanced Research in Computer and Communication Engineering” 2016, vol. 5, issue 2.

jako że tzw. inteligencja IoT jest wynikiem analizy i ekstrapolacji informacji przepływającej w postaci olbrzymiej ilości danych. Jakkolwiek pojęcie inteligencji jest nadużywane w celach marketingowych, to faktycznie - z uwagi na aspekty technologiczne i finansowe – koncepcja znajduje się w swoim początkowym stadium i „mówimy o dziesięcioleciach, które muszą upłynąć, nim większość urządzeń i systemów stanie się kompatybilna i skomunikowana z IoT"[12]. Według prognozy światowego lidera rozwiązań sieciowych Cisco, do 2020 roku liczba urządzeń w ramach Internetu rzeczy osiągnie 50 mld[13]. Jak dotychczas, IoT posiada przede wszystkim wymiar komercyjny i jako taki stanowi nową ofertę na stosunkowo niedużym rynku urządzeń tego typu. Brak spójnej polityki cyberbezpieczeństwa czyni je jednak już teraz łatwym celem dla wszystkich zainteresowanych wykorzystaniem ich podatności. IoT umożliwia penetrację Sieci jako jej stosunkowo najsłabiej zabezpieczony komponent, zwłaszcza że dostawcy tych rozwiązań operują szerokimi kontekstami – taki stan rzeczy czyni zagadnienie bezpieczeństwa międzynarodowego jeszcze bardziej nieostrym.

Systemy C-F a bezpieczeństwo międzynarodowe

Systemowe ujęcie bezpieczeństwa międzynarodowego wciąż lokuje państwa jako jego najistotniejsze i immanentne elementy, jednak nie są już one odizolowane ponieważ „inne podmioty społeczne występujące w stosunkach międzynarodowych oddziałują na państwa w takim wymiarze, który wynika ze stopnia współzależności i oddziaływań państw oraz stosunków, które posiadają w środowisku międzynarodowym"[14]. Instytucjonalne formy współpracy kreują i ustanawiają między państwami związki o charakterze systemowym, będące ostatecznie podstawą bezpieczeństwa międzynarodowego. Transformujący charakter *modus operandi* związanego z globalizacją bezpieczeństwa sprawia, że „systemowa postać stosunków międzynarodowych tworzy systemową postać bezpieczeństwa państwa"[15]. Uniwersalność modelu sieciowego pozwala określić ów kształtujący się paradygmat bezpieczeństwa narodowego takim samym mianem: „Sieciowy paradygmat bezpieczeństwa państwa zakłada zatem istnienie i funkcjonowanie stosunków międzyna-

[12] M. Miller, *op. cit.,* s. 29.
[13] D. Evans, *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, „Cisco White Paper" 2014, s. 3.
[14] J. Gryz, *Państwo w systemie bezpieczeństwa międzynarodowego*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol. 8, nr 2, s. 111.
[15] *Ibidem*.

rodowych w postaci sieci […] państwa stanowią węzły o charakterze stałym i zajmują pozycję *hubów*"[16]. Nie są one także monolityczne, jak chociażby w teoretycznym ujęciu realizmu, ale same stanowią konglomerat złożonych systemów – w tym systemów cyber-fizycznych. Przyjęcie tej optyki oznacza przejście na coraz niższe warstwy systemu, obejmując elementy dotychczas zupełnie pomijane w kontekście bezpieczeństwa międzynarodowego. Jest to naturalna konsekwencja i cecha charakterystyczna paradygmatu sieciowego, który „powoduje spadek znaczenia czynnika geograficznego i czynnika czasu przy równoczesnym wzroście roli czynnika technologicznego"[17] i w obrębie którego „wzrasta wrażliwość podmiotów na zagrożenia związane z wykorzystywaniem wysoko rozwiniętych technologii komunikacyjnych"[18].

Kooperacja na płaszczyźnie instytucjonalnej sprawia, że relacje systemowe pojawiają się nie tylko między państwami czy dużymi graczami na polu współczesnych stosunków międzynarodowych (korporacje, organizacje międzyrządowe, NGOs itp.). Globalny system bezpieczeństwa ulega postępującej fragmentacji, czego efektem jest sektorowa analiza bezpieczeństwa, której to zasadność jest obecnie z ww. względów dyskutowana. Jednocześnie, państwo jako wciąż najistotniejszy podmiot SM oddziałuje na swoje otoczenie, w którym „występują również inne podmioty pozapaństwowe, których zachowania stanowią o środowisku bezpieczeństwa międzynarodowego, występujących w nim strukturach i charakterze"[19]. System bezpieczeństwa państwa staje się z tego powodu konstruktem o nieostrych granicach, jako że „relacje międzynarodowe, jak i wewnętrzne przyjmują charakter sieciowy"[20]. A zatem, w jego zapewnieniu partycypują nie tylko znane dotychczas podmioty, ale i same komponenty ICT. W konsekwencji dychotomia: makroskalowa fragmentacja (dyfuzja bezpieczeństwa) – niskopoziomowa agregacja (IoT) staje się źródłem nowych napięć w systemie i czyni go dalece niespójnym. W kreowaniu polityki bezpieczeństwa coraz większą rolę odgrywają podsystemy tworzące jej dotychczasowe sektory, zaś „transformacja systemu bezpieczeństwa państwa, wynikająca z jego zachowań, identyfikowanych z podejmowanymi i niepodejmowanymi działaniami, wyrażana jest pod postacią zmiennych, których wpływ przekształca system bezpieczeństwa międzynarodowego"[21]. Wśród owych zmiennych

[16] *Ibidem*.
[17] *Ibidem*.
[18] *Ibidem*.
[19] J. Gryz, *op. cit.*, s. 112.
[20] T. R. Aleksandrowicz, *op. cit.*, s. 201.
[21] J. Gryz, *op. cit.*, s. 111.

(zależnych i niezależnych) znajdują się podatności generowane przez systemy C-F i posiadające charakter strukturalny.

Ataki z wykorzystaniem systemów C-F

W przypadku systemów cyber-fizycznych, których wspólnym mianownikiem pozostaje wszechobecna infrastruktura teleinformatyczna, zdolność negatywnego oddziaływania obejmuje niemal cały zakres przedmiotowy związany z bezpieczeństwem. Podział na sektory (industrialny, militarny, społeczny etc.) jako płaszczyzny oddziaływania staje się coraz bardziej efemeryczny ponieważ można do nich dotrzeć z innego, pozornie niezwiązanego poziomu. Do ingerencji w system bezpieczeństwa militarnego można chociażby wykorzystać elementy związane z IoT, podobnie podsystem bezpieczeństwa politycznego nie jest już ograniczony wyłącznie do sfery publicznej, ale interferuje np. z płaszczyzną bezpieczeństwa ludzkiego. Bezpieczeństwo państwa i polityka jego kształtowania w otoczeniu międzynarodowym znajduje odzwierciedlenie w uwzględnianiu takich koncepcji, jak tzw. regiony uczące się[22] czy inteligentne miasta (*smart cities*)[23]. W obliczu wielowymiarowych zagrożeń generowanych przez usieciowiony system bezpieczeństwa międzynarodowego warto przytoczyć kilka przykładów podatności związanych z systemami C-F, możliwych do wykorzystania w procesie jego destabilizacji.

Inteligentne miasta stają się węzłami (*hubami*) funkcjonującymi w oparciu o zasady determinowane przez paradygmat sieciowy. Zarówno zmodyfikowana istniejąca infrastruktura miejska, jak i aglomeracje tworzone od podstaw zawierają komponenty realizujące swoje funkcje w oparciu o systemy C-F[24]. Np. w ramach projektu EMPHASIS rząd Szwecji stworzył sieć sensorów w kanalizacji miejskiej, monitorujących ścieki pod kątem obecności substancji chemicznych wykorzystywanych do produkcji IEDs[25]; takie podejście wpływa na zachowania potencjalnych terrorystów, którzy będą zmuszeni konstruować ładunki poza monitorowanymi obszarami miejskimi, pozbywać się odpadów w inny sposób lub ostatecznie – mo-

[22] Zob. M. Godowska, *Region uczący się – uwarunkowania i determinanty rozwoju na przykładzie województwa małopolskiego*, „Przedsiębiorczość – Edukacja" 2012, vol. 8, ss. 278-286.
[23] Szerzej na ten temat: D. Szymańska, M. Korolko, *Inteligentne miasta – idea, koncepcje i wdrożenia*, Toruń 2015.
[24] Np. miasto Masdar w Zjednoczonych Emiratach Arabskich, zob. *About Masdar City*, źródło: http://www.masdar.ae (dostęp: 29.07.2016). Także Fujisawa SST w prefekturze Kanagawa na wyspie Honsiu – eksperymentalna dzielnica stworzona przez firmę Panasonic, zob. http://fujisawasst.com.
[25] Szerzej na ten temat: *EMPHASIS*, http://www.foi.se (dostęp: 30.07.2016).

dyfikować odczyty sensorów. Koncepcja *smart city* obejmuje m.in. monitoring środowiska (tutaj czujniki kontrolujące skład atmosfery mogą zostać przejęte tuż przed atakiem chemicznym), inteligentne oświetlenie (np. w amsterdamskiej dzielnicy Westergasfabriek) pozwalające pogrążyć w mroku dzielnice stanowiące cel akcji terrorystycznej lub operacji antyterrorystycznej, powszechnie tworzone są inteligentne systemy zarządzania odpadami[26], w których dostęp do sieci jest realizowany przez pojemniki występujące w roli punktów dostępowych (*hot spots*). Ponadto, inteligentne sieci energetyczne (*smart grid*) stanowiące część infrastruktury krytycznej i zasilające miasta generują wiele nowych wektorów ataku C-F: identyfikacja przed planowaną kradzieżą aktywności domowników w oparciu o odczyty dobowego poboru energii, włamanie do sieci domowej i modyfikacja parametrów urządzeń AGD w celu dokonania zniszczeń itp.

Podobne możliwości generuje system inteligentnego zarządzania transportem, jako że kolejne centra miejskie wdrażają w praktyce ideę inteligentnej organizacji ruchu (*smart traffic lights*). Elektryfikacja stanowiła pierwszy etap procesu zapowiadającego ten stan rzeczy, umożliwiając pośrednie manipulowanie przez dezinformację (telegraf)[27], zaś po wprowadzeniu elektromechanicznych urządzeń sterujących w postaci sprzęgła sygnałowego, a później zwrotnicy, także zdalne fizyczne oddziaływanie na ruch kolejowy[28]; podobnie zastosowanie czujnika sankowego było krokiem w kierunku automatyzacji w torowym ruchu miejskim. Obecnie szeroko rozumiana ingerencja w zautomatyzowany system sygnalizacji świetlnej może być na różne sposoby wykorzystana jako atak główny lub dodatkowa zmienna sprzyjająca jego przeprowadzeniu. Także tramwaje są wyposażone w układy zdalnego sterowania w paśmie promieniowania podczerwonego lub radiowym i stanowią kolejną podatność w obszarze inteligentnej komunikacji miejskiej[29].

Inteligentny transport obejmuje zatem nie tylko zautomatyzowane systemy organizacji ruchu, ale same pojazdy, które z punktu widzenia inżynierii systemów

[26] *Optimising Waste Collection*, http://www.enevo.com (dostęp: 30.07.2016).

[27] Zob. H. Hickson, *Wild, Wild West: Act One, Scene One*, http://www.gbcnv.edu (dostęp: 28. 07.2016); 7 kwietnia 1880 w Elko (Nevada) na podstawie sfałszowanego telegramu wprowadzono w błąd obsługę i pasażerów przejeżdżającego pociągu, prowokując dłuższe zatrzymanie maszyny oraz napiętą sytuację.

[28] Spektakularne efekty można uzyskać obierając za cel szybkie pociągi w rodzaju japońskiego *Shinkansen* (tzw. *Bullet Train*, jadący 160 km/h) czy francuskiego TGV.

[29] W 2007 roku nastolatek za pomocą samodzielnie skonstruowanego nadajnika doprowadził do kolizji tramwajów w Łodzi, zob. T. Jabłoński, M. Jach, *Jak 14-latek spowodował katastrofę*, http://lodz.naszemiasto.pl (dostęp: 30.07.2016).

C-F stanowią zestaw wielu czujników dostarczających dane do komputera pokładowego, interpretującego odbierane sygnały i sterującego kontrolerami drzwi, układu hamulcowego, silnika, układami kontroli prędkości pojazdu, dyszami, rotorami etc. Możliwy staje się cyberatak na podzespoły i elementy krytyczne dla bezpieczeństwa pasażerów – układ hamulcowy i kierowania (zwłaszcza zdalnego, tzw. technologia X-by-Wire[30]) czy poduszki powietrzne, podobnie jak przejęcie sygnału GPS takiego pojazdu w celu śledzenia trasy, a nieuprawniona transmisja danych może posłużyć do jego unieruchomienia, zafałszowania odczytów wpływających na bezpieczeństwo pasażerów czy doprowadzenia do kolizji (tzw. *car hacking*)[31]. Ingerencja może nastąpić wskutek włamania przez system rozrywki (*car audio*, Internet pokładowy) z wykorzystaniem *malware* zapisanego na nośnikach zewnętrznych (pamięci masowe), jak i urządzenia dostępowe, chociażby smartfony (WiFi, Bluetooth). Firma vol.vo wykorzystuje w swoich samochodach system typu *infotainment* o nazwie Sensus Connect, magazynujący wszelkie dane używane przez kierowcę w chmurze obliczeniowej[32]; jednocześnie pojazd tworzy punkt dostępu WiFi a system wykorzystuje kartę SIM właściciela. W tym kontekście możliwa jest modyfikacja zadanej trasy dojazdowej przez moduł GPS (*hijack*) lub przejęcie kontroli nad całym pojazdem[33]. W efekcie technologia C-F tworzy nowe drogi dostępu do spersonalizowanego celu ataku, jak podszycie się pod pracownika firmy ubezpieczeniowej – system pokładowy wysyła bowiem dane zebrane w trakcie jazdy do ubezpieczyciela pojazdu. Ewentualne upowszechnienie komunikacji *vehicle-to-vehicle* zachodzącej bezpośrednio między samochodami oznacza możliwość łatwiejszego ataku na polityków i innych decydentów realizowanego na gruncie prywatnym. Koncepcja inteligentnego transportu otwiera również drogę do skutecznego przejmowania dronów cywilnych i wojskowych (o czym świadczy przykład amerykańskiego Sentinela RQ-170 zhakowanego w 2011 r. w Iranie)[34]. Na obecnym etapie rozwoju systemów C-F ma miejsce dyskusja nad ww. zagadnieniami, których ważność podkreślają świadomi problemu politycy, jak chociażby senator

[30] Zob. R. Frank, *X-By-Wire: For Power, X Marks the Spot*, http://electronicdesign.com (dostęp: 31.07.2016).

[31] Zob. C. Miller, Ch.Valasek, *Adventures in Automotive Networks and Control Units*, http://ill matics.com (dostęp: 30.07.2016); J. Frank, *Keeping Cars Secure: Solutions for Implementing in the Era of the Connected Vehicle*, Munich 2013, http://www.nxp.com/ (dostęp: 30.07.2016).

[32] *Sensus Connect*, http://support.volvocars.com (dostęp: 30.07.2016).

[33] G. Templeton, *Hackers Hijack a Super Yacht With Simple GPS Spoofing, and Planes Could Be Next*, http://www.extremetech.com (dostęp: 30. 07.2016).

[34] A. Rawnsley, *Iran's Alleged Drone Hack: Tough, but Possible*, źródło: https://www.wired.com (dostęp: 30.07.2016).

Edward E. Markey[35], a także przedsiębiorstwa (np. IBM)[36]. Z drugiej strony nie brakuje głosów, że nie należy nadmiernie akcentować kwestii ataków C-F na samochody ponieważ producenci pracują nad adekwatnymi zabezpieczeniami[37].

W przypadku inteligentnych domów i budynków (*smart houses*, *smart buildings*) nowe podatności są generowane przez ich systemy ogrzewania, wentylacji i klimatyzacji (*heating, venting, and air conditioning*, HVAC). W razie przejęcia systemu kontrolnego tego typu w budynkach użyteczności publicznej, siedzibach administracji rządowej, resortów siłowych i organizacji międzynarodowych oznacza to nie tylko zablokowanie wyjść z pomieszczeń czy sterowanie temperaturą. Podanie prądu o wysokim natężeniu (w przypadku dostępu do Internetu funkcjonującego w oparciu o sieć energetyczną, PowerLine Ethernet) na transmiter sieciowy może spowodować uszkodzenie sprzętu lub porażenie jego użytkownika. Przejęcie routera obsługującego *smart house* lub *smart building* oznacza nie tylko potencjalny dostęp do danych przechowywanych na wszystkich przyłączonych urządzeniach (komputerach, tabletach, smartfonach, implantach, rozrusznikach serca), ale oddziaływanie za ich pomocą na zachowanie użytkowników, chociażby poprzez wprowadzanie zmian w terminarzach spotkań i kinetyczne, destrukcyjne oddziaływanie na sprzęt IT. W przypadku kombinowanego ataku C-F jest możliwe powiązanie danych z monitoringu implantów medycznych z daną osobą i zmiana warunków w zajmowanym przez nią pomieszczeniu prowadząca do utraty świadomości i śmierci. Inną drogę zapewnia sprzęt codziennego użytku pozostający na wyposażeniu inteligentnych domów.

Tzw. inteligentny telewizor pozostający *online* dysponuje wbudowaną kamerą i mikrofonem (wykorzystywanymi do sterowania systemem operacyjnym i aplikacjami), które mogą zostać aktywowane bez wiedzy mieszkańców. Podobnie jak w przypadku kamer komputerowych[38], umożliwia podgląd codziennej aktywności, w tym rejestrację wizerunku i głosu mieszkańców, członków dalszej rodziny czy odwiedzających[39], a ponadto przechwycenie prywatnych plików przeglądanych

[35] *Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk*, źródło: https://www.markey.senate.gov (dostęp: 30.07.2016).

[36] M. Borrett, G. Serio, *Code Is My Co-pilot: Security & Privacy in Connected Vehicles*, źródło: https://www-304.ibm.com (dostęp: 31.07.2016).

[37] L. Walford, *Why You Don"t Have to Worry About Your Connected Car Being Hacked*, http://www.autoconnectedcar.com (dostęp: 31.07.2016).

[38] Na gruncie prywatnym podobne zagrożenie stanowią konsole do gier podłączone do Sieci. Zarówno SmartTV, jak i konsole pozwalają powiązać ich hasła dostępowe z kontami poczty elektronicznej użytkowników.

[39] Nawet kiedy odbiornik jest wyłączony, co podczas konwentu Black Hat 2013 zademonstrował Seung Jin Lee z Uniwersytetu Koreańskiego, zob. D. Pauli, *Smart TVs a Spying Portal for Hackers,*

w s*mart tv* oraz wszelkich rozmów prowadzonych *online*[40]. Takie zagrożenie miałoby rację bytu np. w trakcie nieformalnych spotkań polityków w pokojach hotelowych lub salach konferencyjnych biur wyposażonych w podobne odbiorniki. Dodatkowo, inteligentne telewizory umożliwiają służbom specjalnym czy potencjalnym terrorystom zdobycie wielu bezpośrednich danych, pozwalając na skuteczne rozpoznanie miejsca operacji lub psychologiczne profilowanie obranych celów osobowych, nie wspominając o próbach nawiązania bezpośredniej łączności i szantażu. Inteligentny sprzęt AGD dostarcza podobnych możliwości, nawet jeśli zostałyby one ograniczone wyłącznie do rejestrowania obecności lokatorów w miejscu zamieszkania.

Podobnie, obecność intruza w sieci lub siedzibie korporacji może okazać się faktem dzięki systemom zarządzania infrastrukturą, wideokonferencji i nadzoru CCTV[41]. Instytucje mogą paść ofiarą własnej polityki zarządzania np. w przypadku urządzeń pracujących w technologii *Instant Ink*[42] – sukcesywne, bezpodstawne zamówienia tuszu po zhakowaniu drukarek online byłoby odczuwalne w skali przedsiębiorstwa tuż po automatycznym przelaniu należności z konta, podobnie jak wydruk kompromitujących materiałów bezpośrednio w biurze doprowadziłby do zmian personalnych (np. w przypadku ataku na CEO organizacji). Kolejne zagrożenia generuje druk 3D, zwłaszcza kiedy dzięki tej technologii powstają całe budynki i mosty – modyfikacja planów konstrukcyjnych przechowywanych w chmurze danych lub wpłynięcie na proces drukowania w trakcie jego trwania znalazłyby odzwierciedlenie w parametrach fizycznych takich elementów. Podobnie jak w przypadku samochodów, także na tym polu pojawiają się opinie bagatelizujące zagadnienia bezpieczeństwa systemów C-F[43].

Internet rzeczy staje się na wiele sposobów związany z dziedziną bezpieczeństwa na gruncie międzynarodowym, przede wszystkim ludzkiego (*human security*).

Researcher Finds, http://www.itnews.com.au (dostęp: 29.07.2016).

[40] D. Pauli, *Attackers Can Read USB Storage Attached to Samsung TVs*, http://www.itnews.com.au (dostęp: 31.07.2016).

[41] K. Zetter, *Most Popular Surveillance Cameras Can Be Hacked*, http://gizmodo.com (dostęp: 31. 07.2016); CCTV umożliwia np. monitoring fizycznej ochrony w celu uzyskania bezprzewodowego dostępu do SCADA.

[42] *HP Instant Ink - What Is HP Instant Ink?*, http://support.hp.com (dostęp: 31.07.2016).

[43] L. Fernandes, *Exploiting the „Printernet" of Things*, http://www.louellafernandes.com (dostęp: 31. 07.2016); A. Williams, *World's First 3D-printed Office Building Completed in Dubai*, http://newatlas.com (dostęp: 31.07.2016); M. Molitch-Hou, *Construction of World's 1st 3D Printed Bridge Begins in Amsterdam*, http://3dprintingindustry.com (dostęp: 31.07.2016); D. S. Maldow, *How to Defend Your Boardroom Against „Videoconferencing Hackers" and Other Mythical Creatures*, http://www.telepresenceoptions.com (dostęp: 31.07.2016).

Wśród nich na szczególną uwagę zasługują potencjalne ataki wymierzone w polityków i inne osoby decyzyjne w państwie lub organizacji międzynarodowej, których powodzenie może skutkować zmianą globalnego układu sił lub konfliktem zbrojnym. Środkiem prowadzącym do tego celu, poza klasycznym naruszeniem prywatności (poufności danych), jest w tym przypadku o wiele groźniejsze oddziaływanie cyber-fizyczne. Np. bezpośrednio na organizm biologiczny poprzez wspomniane już implanty bezprzewodowe[44], co stanowi obecnie na tyle realny problem, że były wiceprezydent USA, Dick Cheney, wyłączył w swoim rozruszniku serca funkcję monitorowania online[45]. Jak istotna jest to kwestia, niech świadczy niewyjaśniona śmierć hakera z firmy IOActive (Barnaby Jack)[46], który podczas konwencji Black Hat w Las Vegas (2013) miał publicznie udowodnić, że jest możliwa nie tylko modyfikacja oprogramowania rozruszników serca czy implantów, ale zabójstwo bezpośrednim, zdalnie indukowanym impulsem elektrycznym o napięciu kilkuset woltów[47]. Hacker zaznaczył, że może to posłużyć nie tylko do aktów cyfrowego skrytobójstwa, ale zostać wykorzystane w aktach cyberterroryzmu[48]. Hipotetycznie możliwe jest także wykorzystanie wszczepionego *chipa*, jako źródła infekcji nie tylko dla innych implantów w jego najbliższym otoczeniu, ale innych docelowych urządzeń niemedycznych (wirusem, *spyware* lub *malware*). Sprzyjają temu innowacje w dziedzinie *smart building*: pracownicy szwedzkiego biura używają *chipów* w codziennej pracy, co umożliwia ich ewentualne skopiowanie (sklonowanie), kradzież tożsamości i wejście nieuprawnionej osoby do budynku[49]. Nieautoryzowany dostęp do implantów medycznych oznacza nie tylko monitoring stanu zdrowia danego pacjenta, ale odkrycie nowych schorzeń bez jego wiedzy; podobnie można łatwo stwierdzić, że posiadacz danego smartfona (numeru telefonu) używającego glukometru iBGStar choruje na cukrzycę.

[44] Charakterystyka przykładowego rozrusznika pozostającego w trybie online firmy Etrinsa zob. *Etrinsa Pacemaker Family Technical Manual*, http://www.biotronikusa.com (dostęp: 31.07.2016).
[45] C. Franzen, *Dick Cheney Had the Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering*, http://www.theverge.com (dostęp: 31.07.2016).
[46] X. Jardin, *Hacker Barnaby Jack Dies Just Before Black Hat Presentation on Lethal Pacemaker Hacks*, http://boingboing.net (dostęp: 31.07.2016).
[47] R. Boyle, *Hackers Could Access Pacemakers From A Distance And Deliver Deadly Shocks*, http://www.popsci.com (dostęp: 31.07.2016).
[48] D. Pauli, *Hacked Terminals Capable of Causing Pacemaker Deaths*, http://www.itnews.com.au (dostęp: 31.07.2016).
[49] T. Buchanan, *Swedish Firm Microchips Employees*, http://www.independent.co.uk (dostęp: 31.07.2016).

Szpitale jako funkcjonalna całość także stały się poważnym źródłem zagrożeń ze strony systemów C-F[50]. Ich przykładem jest potencjalna intencjonalna modyfikacja oprogramowania urządzeń medycznych wpiętych do Sieci (ewentualnie dokonanie zmian jeszcze na etapie ich produkcji)[51]. Na polu medycyny pojawiły się urządzenia i systemy C-F generujące bezpośrednie ścieżki prowadzące do danej osoby pełniącej funkcje publiczne, a komponenty medyczne typu *smart* stanowią obecnie dużą grupę produktów konstytuujących *Internet of Things*. Urządzenia online monitorujące i wspomagające funkcje organizmu (pulsometry, implanty), inteligentne tabletki, które po połknięciu zbiorą dane na temat stanu organizmu i nadchodzące zautomatyzowane systemy podawania leków w czasie rzeczywistym jeszcze bardziej skomplikuje powyższy obraz, umożliwiając nieautoryzowaną ingerencję[52]. Uzupełniają go coraz powszechniejsze inteligentne ubrania, koszulki biometryczne zawierające komponenty elektroniczne przyspieszające spalanie tkanki tłuszczowej, gromadzące dane na temat organizmu w zintegrowanej pamięci etc[53].

Uwagi końcowe

Jakkolwiek ww. metody destabilizacji bezpieczeństwa państwa i systemu międzynarodowego za pośrednictwem systemów C-F wydają się być w pewnej mierze czysto hipotetyczne, ich rosnąca rola czyni podobne zagrożenia coraz bardziej realnymi. Konfliktogenny charakter otoczenia międzynarodowego i systemu jego bezpieczeństwa sprzyja poszukiwaniu nowych dróg negatywnego oddziaływania w celu uzyskania założonych sekwencji zdarzeń. W miarę dalszego upowszechniania systemów cyber-fizycznych, opracowanie nowych metod pożądanego oddziaływania zwrotnego w skali makro i mikro jest tylko kwestią czasu. Tym bardziej,

[50] W Stanach Zjednoczonych stanowią element infrastruktury krytycznej, zob. M. E. Callahan, *Cybersecurity*
and Hospitals. What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response, http://www.aha.org (dostęp: 31.07.2016).

[51] W latach osiemdziesiątych XX wieku błąd w oprogramowaniu aparatu do radioterapii Therac-25 doprowadził do śmierci kilku pacjentów chorych na nowotwór, zob. A. Fabio, *Killed by a Machine: The Therac-25*, http://hackaday.com (dostęp: 31.07.2016).

[52] S. Mitchell, N. Villa, M. Stewart-Weeks, A. Lange, *The Internet of Everything for Cities . Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities*, http://www.cisco.com (dostęp: 30.07.2016).

[53] M. Sawh, *Thin Ice Smart Vest Cools Your Body Down to Burn Fat*, http://www.wareable.com (dostęp: 31.07.2016); D. Thompson, *Under Armour's Best Idea: A Smart Shirt That Measures Heart Rate and G-Force*, http://www.theatlantic.com (dostęp: 31.07.2016). Podobnie obuwie sportowe, zob. J. Beverly, *First Run: Under Armour's Smart Shoes*, http://www.runnersworld.com (dostęp: 31.07.2016).

że historia cyberbezpieczeństwa systemów C-F zna już co najmniej kilkadziesiąt przypadków ich wykorzystania w procesie oddziaływania na bezpieczeństwo narodowe i międzynarodowe (np. Arizona Salt River Project w 1994 r., australijski atak w Maroochy w 2000 r., elektrownia jądrowa Davis Besse w Ohio 20 sierpnia 2003 r.)[54].

Ewolucja systemów cyber-fizycznych oznacza dalsze odejście od paradygmatu akcentującego centralną rolą aparatu państwowego w kierunku celowanych ataków wymierzonych w bezpieczeństwo ludzkie (tak w szerokim kontekście społecznym, jak i w przypadku członków władz), a ich ich zdolność oddziaływania na przestrzeń materialną poszerza zakres bezpieczeństwa militarnego. Chociaż na obecnym etapie wiele możliwości oferowanych przez systemy C-F pozostaje w sferze fikcji lub jawi się jako zupełnie nieprzydatne lub nieszkodliwe, ich stosunkowo łatwa dostępność sprawi, że akty cyber-fizycznej przemocy staną się najprawdopodobniej coraz częstsze[55]. Sprzyja temu wspomniana dyfuzja systemów bezpieczeństwa (wewnętrznego i międzynarodowego).

System bezpieczeństwa międzynarodowego jest wypadkową systemów bezpieczeństwa państw, relacji i oddziaływań (tzw. miękkich i twardych) zachodzących pomiędzy nimi. Systemy C-F stanowią materialno-wirtualną płaszczyznę znoszącą granice pomiędzy bezpieczeństwem wewnętrznym, narodowym i międzynarodowym czyniąc je coraz bardziej umownymi, a wektory ataków informatycznych ulegają kategoryzacji w zależności od charakteru obiektu referencyjnego. Rosnąca współzależność podmiotów stosunków międzynarodowych, która w perspektywie miała położyć kres siłowym metodom rozwiązywania konfliktów, staje się w istocie przyczyną dywersyfikacji sposobów osiągania tych samych celów, czyniąc je coraz bardziej wyrafinowanymi. W tej nowej rzeczywistości zagrożenia generowane przez systemy C-F mają charakter strukturalny i pod przykrywką *smart power* grawitują zdecydowanie w kierunku „twardych" oddziaływań.

[54] Zob. G. Loukas, *Cyber-Physical Attacks. A Growing Invisible Threat*, Amsterdam 2015, Fig. 2.3, s. 55.

[55] E. A. Lee, *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*, „Sensors" 2015, vol. 15, no. 3, ss. 4837-4869.

Bibliografia

About Masdar City, źródło: http://www.masdar.ae (dostęp: 29.07.2016).

Aleksandrowicz T. R., *Świat w sieci. Państwa, społeczeństwa ludzie. W poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014.

Beverly J., *First Run: Under Armour's Smart Shoes*, http://www.runnersworld.com (dostęp: 31.07.2016).

Borrett M., Serio G., *Code Is My Co-pilot: Security & Privacy in Connected Vehicles*, źródło: https://www-304.ibm.com (dostęp: 31.07.2016).

Boyle R., *Hackers Could Access Pacemakers From A Distance And Deliver Deadly Shocks*, źródło: http://www.popsci.com (dostęp: 31.07.2016).

Buchanan T., *Swedish Firm Microchips Employees*, źródło: http://www.independent.co.uk (dostęp: 31.07.2016).

Callahan M. E., *Cybersecurity and Hospitals. What Hospital Trustees Need to Know About Managing Cybersecurity Risk and Response*, źródło: http://www.aha.org (dostęp: 31.07.2016).

EMPHASIS, źródło: http://www.foi.se (dostęp: 30.07.2016).

Etrinsa Pacemaker Family Technical Manual, źródło: http://www.biotronikusa.com (dostęp: 31.07.2016).

Evans D., *The Internet of Things. How the Next Evolution of the Internet Is Changing Everything*, „Cisco White Paper" 2014.

Fabio A., *Killed by a Machine: The Therac-25*, http://hackaday.com (dostęp: 31.07.2016).

Fernandes L., *Exploiting the „Printernet" of Things*, źródło: http://www.louellafernandes.com (dostęp: 31.07.2016);

Frank J., *Keeping Cars Secure: Solutions for Implementing in the Era of the Connected Vehicle*, Munich 2013, http://www.nxp.com/ (dostęp: 30.07.2016).

Frank R., *X-By-Wire: For Power, X Marks the Spot*, źródło: http://electronicdesign.com (dostęp: 31.07.2016).

Franzen C., *Dick Cheney Had the Wireless Disabled on His Pacemaker to Avoid Risk of Terrorist Tampering*, źródło: http://www.theverge.com (dostęp: 31.07. 2016).

Gill H., *A Continuing Vision: Cyber-Physical Systems*, Arlington 2008, źródło: https://www.ece.cmu.edu (dostęp: 27.07.2016).

Godowska M., *Region uczący się – uwarunkowania i determinanty rozwoju na przykładzie województwa małopolskiego*, „Przedsiębiorczość – Edukacja" 2012, vol. 8.

Gryz J., *Państwo w systemie bezpieczeństwa międzynarodowego*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, vol. 8, nr 2.

Hickson H., *Wild, Wild West: Act One, Scene One*, źródło: http://www.gbcnv.edu (dostęp: 28.07.2016);

HP Instant Ink - What Is HP Instant Ink?, źródło: http://support.hp.com (dostęp: 31.07.2016).

http://fujisawasst.com.

Jabłoński T., Jach M., *Jak 14-latek spowodował katastrofę*, źródło: http://lodz.naszemiasto.pl (dostęp: 30.07.2016).

Jardin X., *Hacker Barnaby Jack Dies Just Before Black Hat Presentation on Lethal Pacemaker Hacks*, źródło: http://boingboing.net (dostęp: 31.07.2016).

Lee E. A., *The Future of Embedded Systems*, źródło: https://chess.eecs.berkeley.edu (dostęp: 28.07.2016).

Lee E. A., *The Past, Present and Future of Cyber-Physical Systems: A Focus on Models*, „Sensors" 2015, vol. 15, no. 3.

Loukas G., *Cyber-Physical Attacks. A Growing Invisible Threat*, Amsterdam 2015.

Maldow D. S, *How to Defend Your Boardroom Against „Videoconferencing Hackers" and Other Mythical Creatures*, źródło: http://www.telepresenceoptions.com (dostęp: 31.07.2016).

Miller C., Valasek Ch., *Adventures in Automotive Networks and Control Units*, źródło: http://illmatics.com (dostęp: 30.07.2016).

Miller M., *Internet rzeczy. Jak inteligentne telewizory, samochody, domy i miasta zmieniają świat*, Warszawa 2016.

Mitchell S., Villa N., Stewart-Weeks M., Lange A., *The Internet of Everything for Cities . Connecting People, Process, Data, and Things To Improve the 'Livability' of Cities and Communities*, źródło: http://www.cisco.com (dostęp: 30.07.2016).

Molitch-Hou M., *Construction of World's 1st 3D Printed Bridge Begins in Amsterdam*, źródło: http://3dprintingindustry.com (dostęp: 31.07.2016);

Mukherjee S., Shaw R., *Big Data – Concepts, Applications, Challenges and Future Scope*, „International Journal of Advanced Research in Computer and Communication Engineering" 2016, vol. 5, issue 2.

Optimising Waste Collection, źródło: http://www.enevo.com (dostęp: 30.07.2016).

Pauli D., *Attackers Can Read USB Storage Attached to Samsung TVs*, źródło: http://www.itnews.com.au (dostęp: 31.07.2016).

Pauli D., *Hacked Terminals Capable of Causing Pacemaker Deaths*, źródło: http://www.itnews.com.au (dostęp: 31.07.2016).

Pauli D., *Smart TVs a Spying Portal for Hackers, Researcher Finds*, źródło: http://www.itnews.com.au (dostęp: 29.07.2016).

Rawnsley A., *Iran's Alleged Drone Hack: Tough, but Possible*, źródło: https://www.wired.com (dostęp: 30.07.2016).

Remote Terminal Unit (RTU), źródło: http://www.wbsetcl.in (dostęp: 28.07.2016).

Sawh M., *Thin Ice Smart Vest Cools Your Body Down to Burn Fat*, źródło: http://www.wareable.com (dostęp: 31.07.2016).

Sensus Connect, źródło: http://support.volvocars.com (dostęp: 30.07.2016).

Stańczyk J., *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996.

Systemy SCADA, źródło: http://www.astor.com.pl (dostęp: 28.07.2016).

Szymańska D., Korolko M., *Inteligentne miasta – idea, koncepcje i wdrożenia*, Toruń 2015.

Templeton G., *Hackers Hijack a Super Yacht With Simple GPS Spoofing, and Planes*

Could Be Next, źródło: http://www.extremetech.com (dostęp: 30. 07.2016).

Thompson D., *Under Armour's Best Idea: A Smart Shirt That Measures Heart Rate and G-Force*, http://www.theatlantic.com (dostęp: 31.07.2016).

Tracking & Hacking: Security & Privacy Gaps Put American Drivers at Risk, źródło: https://www.markey.senate.gov (dostęp: 30.07.2016).

Ullman R. H., *Redefining Security*, „International Security" 1983, vol. 8, no. 1.

Walford L., *Why You Don"t Have to Worry About Your Connected Car Being Hacked*, źródło: http://www.autoconnectedcar.com (dostęp: 31.07.2016).

Williams A., *World's First 3D-printed Office Building Completed in Dubai*, źródło: http://newatlas.com (dostęp: 31.07.2016);

Zetter K., *Most Popular Surveillance Cameras Can Be Hacked*, źródło: http://giz modo.com (dostęp: 31.07.2016)