Wprowadzenie

Opracowania dotyczące problemów bezpieczeństwa teleinformatycznego nierzadko otwierają sugestywne opisy wysublimowanych, ale zarazem bardzo skutecznych ataków na sieci komputerowe, prowadzących do poważnych zakłóceń funkcjonowania wszystkich sfer życia nowoczesnego społeczeństwa. Sprawcy, najczęściej nazywani cyberterrorystami, kilkoma kliknięciami doprowadzają do przerw w dostawach prądu elektrycznego czy też wody, uniemożliwiają odbiór telewizji lub blokują funkcjonowanie Internetu, powodując w konsekwencji krachy giełdowe i bankructwa banków, a nawet śmierć setek osób w wypadkach lotniczych, kolejowych i przemysłowych. Jak do tej pory żaden z takich katastroficznych scenariuszy się nie zrealizował. Nie oznacza to jednak, że problemy bezpieczeństwa teleinformatycznego można bagatelizować. Obraz zagrożeń pojawiających się w tym specyficznym wymiarze bezpieczeństwa państwa jest bowiem skomplikowany, dorównując barwnością fikcyjnym scenariuszom.

W ostatnich dniach kwietnia 2007 r. w Estonii, uwikłanej wówczas w konflikt polityczny z Rosją, doszło do zaskakujących zakłóceń ruchu internetowego. Lawinowo wzrosła ilość danych przesyłanych pod określone adresy, głównie rządowe serwery z informacyjnymi witrynami WWW. Dość szybko doprowadziło to do ich przeciążenia i – w konsekwencji – niedostępności portali estońskich instytucji rządowych dla użytkowników Internetu. Stało się jasne, że miał miejsce celowy atak. W ciągu następnych kilku dni podobne ataki powtórzyły się, a ich siła gwałtownie wzrosła. W wyniku zalewu danymi w ilości kilkakrotnie większej niż maksymalna przepustowość estońskiej infrastruktury internetowej została ona praktycznie sparaliżowana. Internet, stanowiący w Estonii istotny, wręcz podstawowy, kanał komunikacji zawodowej i publicznej, rozwijany dynamicznie w ciągu ostatniej dekady i będący chlubą tego kraju, niemal przestał działać. Pojawiły się sugestie, że jest to kompleksowy, drobiazgowo

zaplanowany atak na estoński Internet, przeprowadzony przez bliżej niezidentyfikowaną, choć prawdopodobnie pochodzącą głównie z Rosji grupę osób; mówiono o cyberterroryźmie, cyberwojnie, cybersabotażu. W kilka miesięcy po tym wydarzeniu media na całym świecie donosiły o aktach cyberszpiegostwa – bezprecedensowej w swej skali kradzieży danych z komputerów wielu najważniejszych instytucji rządowych USA, włącznie z Pentagonem, zorganizowanej przez nieznaną grupę sprawców. W tym samym czasie eksperci z dziedziny bezpieczeństwa teleinformatycznego zwrócili uwagę na fakt, że na świecie działają setki tysięcy komputerów zainfekowanych odpowiednio spreparowanym oprogramowaniem, które bez wiedzy i woli ich właścicieli pozwala na zdalne przejmowanie nad nimi kontroli i wykorzystywanie do różnych celów. Największa taka nielegalna sieć, ze względu na swoje rozmiary nazwana *Kraken* (tak jak mityczny potwór morski), liczyć miała około 800 tys. maszyn. Temat aktów szpiegostwa wymierzonych przeciwko rządowym sieciom USA i innych państw, głównie sojuszników z NATO, powrócił w mediach światowych także na początku 2009 r. Eksperci z Kanady zaprezentowali raport na temat grupy określającej siebie nazwą *GhostNet*, która rzekomo zajmuje się „zawodowo" szpiegostwem komputerowym. Z kolei w marcu 2009 r. media przestrzegały przed nowym, potencjalnie niebezpiecznym wirusem *Conficker*, który 1 kwietnia miał sparaliżować setki tysięcy komputerów – tego dnia nic jednak się nie wydarzyło, choć niektórzy eksperci wskazywali, że wirus może się jeszcze uaktywnić.

O narastających problemach w sferze bezpieczeństwa teleinformatycznego w ostatnich latach mówiono również w Polsce. Media coraz częściej podejmowały choćby temat oszustw dotykających posiadaczy kont bankowych on-line. Policja ujawniła przypadki ataków internetowych na nieostrożnych klientów banków, którzy, oszukani w odpowiedni sposób, ujawniali swoje dane złodziejom – cyberprzestępcom. Wielkości skradzionych w ten sposób środków jednak nie ujawniono. Jednocześnie, w ciągu kilku kolejnych miesięcy polska policja informowała o serii działań wymierzonych przeciw osobom rozpowszechniającym pornografię dziecięcą w Internecie – skomplikowane operacje prowadzone przede wszystkim w cyberprzestrzeni doprowadziły do zatrzymań, w skali całej Polski, łącznie kilkuset osób.

W kontekście każdego z tych wydarzeń mówiono o bezpieczeństwie teleinformatycznym (informatycznym), posługując się jednak czasem odmiennymi terminami[1]. Również w stosunku do ich sprawców stosowano, zamiennie i niekonsekwentnie, różnorodne, a ponadto z reguły nieprecyzyjne określenia[2]. Podejmowano także próby klasyfikowania tych zdarzeń, umieszczania ich na mapie zagrożeń związanych z wykorzystywaniem technologii teleinformatycznych. Wysiłki te dawały jednak zazwyczaj obraz nadmiernie uproszczony, uwypuklający jedynie wybrane aspekty poruszanych problemów, a całkowicie pomijający inne. Dodatkowo sama dyskusja na te tematy prowadzona była przy użyciu specyficznego technicznego żargonu, co nie tylko zniechęcało do udziału w niej osoby mniej zorientowane w problematyce sieci komputerowych, ale też utrudniało zrozumienie istoty problemu.

Sytuacja ta jest konsekwencją wieloznaczności pojęcia bezpieczeństwa teleinformatycznego oraz zróżnicowania sposobów jego definiowania. Wieloaspektowość i wielopłaszczyznowość tego zagadnienia wynika z kolei z różnorodności i dużej liczby poziomów, na których należy je rozpatrywać. Może się ono bowiem odnosić do bardzo różnych podmiotów, począwszy od użytkownika indywidualnego (poziom najniższy) – przeciętnego obywatela posługującego się komputerem osobistym – przez przedsiębiorstwa i instytucje, wykorzystujące w swej codziennej działalności całe sieci teleinformatyczne, aż po samo państwo (jego struktury administracyjne, organy i służby czy też gospodarkę), a nawet system międzynarodowy ujmowany całościowo (poziom najwyższy). Na każdym z tych poziomów zakres pojęcia bezpieczeństwa teleinformatycznego będzie inny, odmienne będą też skala i powaga następstw jego naruszeń oraz metody i środki jego zapewniania. Co więcej, za zagrożenia uznawane będą różne zjawiska, procesy, wydarzenia czy działania.

---

[1] Najbardziej rozpowszechnione określenia, często używane w odniesieniu do zagadnień bezpieczeństwa teleinformatycznego, traktowane z reguły – choć nie zawsze zasadnie – jako synonimy i wykorzystywane wymiennie, to m.in. bezpieczeństwo informacyjne (*information security*) i cyberbezpieczeństwo (*cybersecurity*).

[2] W mediach najczęściej mówiono o cyberprzestępcach, cyberterrorystach, hakerach, przestępcach internetowych a także po prostu o oszustach i złodziejach.

Identyfikacja oraz właściwa ocena rangi i charakteru zagrożeń jest bodaj najbardziej skomplikowanym wyzwaniem, towarzyszącym analizie problemów bezpieczeństwa teleinformatycznego. Niektóre z nich mają bowiem charakter ściśle fizyczny – polegają na groźbie faktycznego zniszczenia materialnych narzędzi służących do przechowywania, przetwarzania lub przesyłania cyfrowej informacji. Tego rodzaju niebezpieczeństwo może towarzyszyć choćby atakom bombowym na obiekty, w których znajdują się systemy komputerowe przechowujące i przetwarzające określone dane, ale też być wynikiem klęsk żywiołowych (powodzi, pożarów, trzęsień ziemi itp.) lub katastrof technicznych. Większość z zagrożeń bezpieczeństwa teleinformatycznego wiąże się jednak z działaniami prowadzonymi w cyberprzestrzeni, przy wykorzystaniu odpowiedniego sprzętu i oprogramowania. Wówczas negatywnemu oddziaływaniu poddawana jest sama informacja utrwalona w formie elektronicznej, a nie urządzenia służące do jej przechowywania i przetwarzania. Skutki takiej aktywności zazwyczaj nie wykraczają poza cyberprzestrzeń i objawiają się, ujmując rzecz ogólnie, nieprawidłową pracą systemów komputerowych i zakłóceniami wykonywanych przez nie funkcji. Niemniej jednak, następstwa tego rodzaju działań mogą również przejawiać się w świecie fizycznym, np. w postaci wadliwego funkcjonowania jakichś urządzeń, których sprawność działania zależy od dopływu danych elektronicznych. Dodatkowo pamiętać trzeba, iż poważnym problemem może być również sama niemożność skorzystania z sieci komputerowych, a tym samym – z oferowanych przez nie usług elektronicznych. Wreszcie, w pewnych sytuacjach zagrożenie bezpieczeństwa może się łączyć z samą treścią informacji, czego przykładem jest choćby dostępna przez Internet pornografia dziecięca czy też propaganda nawołująca do nienawiści rasowej lub religijnej.

Złożoność problematyki bezpieczeństwa informatycznego utrudnia znalezienie cech wspólnych wszystkim zagadnieniom uznawanym za przynależące do tej dziedziny. Mimo to można przyjąć, że istotą bezpieczeństwa teleinformatycznego, bez względu na poziom, na którym je rozpatrujemy – użytkownika indywidualnego, zbiorowego, państwa czy systemu międzynarodowego, jest zdolność określonego podmiotu do pozyskania i zachowania, w formie niezmienionej bez jego zgody i wiedzy, wszelkiego rodzaju informacji utrwalonej w postaci cyfrowej oraz możliwość jej bezpiecznego (tzn. nienarażonego na

przechwycenie, zniszczenie lub nieuprawnioną modyfikację) przetwarzania, przesyłania i upowszechniania[3]. Dodatkowo nie można zapominać, zważywszy na współczesny stopień integracji infrastruktury teleinformatycznej, powszechność jej wykorzystania oraz łatwość dostępu do niej, o znaczeniu powiązań między poszczególnymi poziomami tak rozumianego bezpieczeństwa teleinformatycznego. W ich wyniku bowiem zarówno bezpieczeństwo teleinformatyczne państwa zależy do pewnego stopnia od stanu zabezpieczeń komputerów i tym podobnych urządzeń znajdujących się w posiadaniu użytkowników indywidualnych, jak i odwrotnie, bezpieczeństwo danych przechowywanych lub przesyłanych przez poszczególne jednostki z wykorzystaniem ich własnego sprzętu uzależnione jest od poziomu odporności na rozmaite groźby infrastruktury teleinformatycznej na szczeblu narodowym. To zaś niewątpliwie dodatkowo komplikuje samo zagadnienie bezpieczeństwa teleinformatycznego, utrudniając tym samym wysiłki na rzecz jego skutecznego zapewniania.

Wielowymiarowość zagadnień bezpieczeństwa teleinformatycznego oznacza też możliwość odmiennych interpretacji zarówno poszczególnych pojęć z tego zakresu, jak i samej istoty tego wymiaru bezpieczeństwa. W rezultacie różni badacze tego zagadnienia oraz praktycy, odpowiedzialni za zapewnianie bezpieczeństwa teleinformatycznego na poszczególnych jego poziomach, pojmują przedmiot swojej pracy nieco odmiennie. Inaczej na kwestie bezpieczeństwa teleinformatycznego spogląda bowiem zawodowy informatyk, mający za zadanie utrzymanie sprawnego funkcjonowania instytucjonalnej sieci komputerowej np. przedsiębiorstwa (czyli administrator sieci), a inaczej wojskowy specjalista, koncentrujący się na zapewnieniu jednostkom wojskowym nieprzerwanej łączności. Odmienne podejście mają też np. policjant, zajmujący się zwalczaniem umieszczanej w Internecie pornografii dziecięcej lub innych nielegalnych treści oraz polityk odpowiedzialny za stabilność całego państwa. Każda z tych osób ogranicza się z reguły przy analizie i ocenie zagadnień bezpieczeństwa teleinformatycznego, co naturalne i zrozumiałe, do pers-

[3] W tym kontekście przytoczyć można często powtarzaną „triadę" warunków utrzymania bezpieczeństwa teleinformatycznego, tj. integralność (spójność, nienaruszona struktura i treść informacji), poufność (zabezpieczenie informacji przed nieuprawnionym dostępem) oraz dostępność (możliwość niezakłóconego dostępu uprawnionych podmiotów do informacji).

pektywy własnej specjalności. Z tego powodu uznaje za priorytetowe inne problemy i wyzwania, przyjmuje inną hierarchię zadań i celów, a w konsekwencji – poszukuje innych rozwiązań.

Odmienne definicje bezpieczeństwa teleinformatycznego, inaczej pojmowany zakres tego zagadnienia oraz odpowiedzi na zidentyfikowane problemy sformułowane bez należytego uwzględnienia wszystkich możliwych implikacji, powodują z kolei, że znacznie utrudniona jest współpraca i koordynacja działań prowadzonych z myślą o poprawie stanu bezpieczeństwa teleinformatycznego, zwłaszcza w skali ogólnopaństwowej. Zdolność zaś do efektywnej kooperacji przy przeciwdziałaniu zagrożeniom bezpieczeństwa teleinformatycznego ma niewątpliwie centralne znaczenie dla skutecznego i całościowego rozwiązywania problemów bezpieczeństwa teleinformatycznego na poziomie państwa, a w konsekwencji zapewne również pozostałych użytkowników technologii informatycznych.

Dlatego też główną ideą przyświecającą opracowaniu tego zbioru było właśnie ukazanie różnorodności perspektyw, z jakich patrzeć można (i należy) na problemy bezpieczeństwa teleinformatycznego, oraz doprowadzenie do swoistego „spotkania" tych, często bardzo odmiennych, punktów widzenia. Powinno to bowiem umożliwić wypracowanie właściwej odpowiedzi na pojawiające się w tej sferze wyzwania. Polityk decydujący o kształcie strategii kraju w odniesieniu do zagrożeń bezpieczeństwa narodowego w wymiarze teleinformatycznym nie może przecież oczekiwać wdrożenia rozwiązań technicznie niewykonalnych. Natomiast informatyk dbający o stabilność nadzorowanej przez niego sieci musi pamiętać o szerszym kontekście problemu, np. konieczności pogodzenia wymogów bezpieczeństwa teleinformatycznego z innymi priorytetami państwa w dziedzinie bezpieczeństwa narodowego. Stąd też tak ważne jest pogłębienie wśród osób zajmujących się bezpieczeństwem informatycznym (niezależnie, jak przez nich definiowanym) świadomości różnorodności możliwych ujęć tego problemu, ułatwienie poznania specyfiki poszczególnych jego wymiarów, a także unaocznienie potrzeby łączenia rozmaitych podejść do tego zagadnienia w celu lepszego zrozumienia jego istoty i wagi. Można tego dokonać jedynie przez rozwój dialogu ukazującego różnorodne perspektywy, z jakich należy na to zagadnienie spoglądać. Nie będzie on zapewne prowadził do wypracowania jednej, powszechnie obowiązującej i akceptowanej przez wszystkich definicji

zakresu tej problematyki, ani też nie pozwoli ustalić niebudzącej niczyich wątpliwości hierarchii wyzwań i listy priorytetowych zadań w dziedzinie bezpieczeństwa informatycznego państwa. Niemniej jednak wydaje się, że już samo uświadomienie złożoności zagadnienia oraz potrzeby ciągłej koordynacji i komunikacji działań czasem bardzo różnych podmiotów będzie miało duże znaczenie przy wypracowywaniu właściwej strategii – spójnego programu działań na rzecz poprawy bezpieczeństwa teleinformatycznego państwa.

Otwierające zbiór opracowanie Marka Madeja, pełniące zarazem funkcję swoistego wprowadzenia do pozostałych zamieszczonych w nim artykułów, koncentruje się na istocie rewolucji informatycznej jako czynniku kształtującym współczesne środowisko międzynarodowe i stanowiącym warunek obecnego rozwoju oraz upowszechniania technologii informatycznych, zwłaszcza zaś na jej wpływie na szerzej rozumiane bezpieczeństwo państw oraz charakter prowadzonych przez nie polityk w tym względzie. Kolejny artykuł w zbiorze, autorstwa Patryka Dawidziuka, Borysa Łąckiego i Marka Stolarskiego, przybliża czytelnikom istotę i znaczenie stanowiącego swoisty „szkielet" cyberprzestrzeni Internetu, ukazując zarówno przebieg jego historycznej ewolucji, jak i różnorodność dzisiejszych form jego wykorzystania. Autorzy dokonali w nim również przeglądu najważniejszych kategorii zagrożeń bezpieczeństwa teleinformatycznego wiążących się z funkcjonowaniem Internetu. Tekst przygotowany przez Pawła Łysakowskiego przybliża natomiast – na przykładzie Polski – rolę i znaczenie sieci teleinformatycznych w funkcjonowaniu systemu płatniczego państw. Zważywszy zarówno na newralgiczną funkcję struktur finansowych we współczesnej gospodarce, jak i wyjątkowo daleko posunięty proces ich informatyzacji, bez dokonania analizy tego zagadnienia trudno byłoby ukazać specyfikę i wagę problemów bezpieczeństwa teleinformatycznego współczesnych państw.

Autorzy dwóch następnych artykułów omawiają bliżej specyfikę poszczególnych typów zagrożeń bezpieczeństwa informatycznego, przyjmując za punkt odniesienia poziom państwowy. W pierwszym z nich Piotr Sienkiewicz i Halina Świeboda zajmują się zjawiskiem walki informacyjnej, a więc możliwościami i sposobami wykorzystywania technologii informatycznych przez siły zbrojne państw. Obok szerokiej i szczegółowej prezentacji poglądów wielu uznanych badaczy na istotę i specyfikę walki informacyjnej, autorzy artykułu

starają się też wyznaczyć faktyczną rolę oraz rangę tego rodzaju działań nie tylko w trakcie walk z nieprzyjacielskimi siłami zbrojnymi, ale też w toku rywalizacji z innymi przeciwnikami, w tym grupami niepaństwowymi. To ostatnie zagadnienie bardziej szczegółowo analizuje Marcin Terlikowski w tekście poświęconym wyjątkowo kontrowersyjnej kwestii tzw. cyberterroryzmu oraz pokrewnym mu (a czasem z nim mylonym) formom wykorzystania technologii informatycznych przez podmioty pozapaństwowe, takim jak działalność hakerów czy haktywizm. Autor skupia się na potencjalnych skutkach działań cyberterrorystów i im podobnych podmiotów oraz ich znaczeniu w ramach całościowo ujmowanego bezpieczeństwa narodowego.

Bardzo istotne w kontekście polityki bezpieczeństwa państwa zagadnienia podejmuje artykuł Marcina Ludwiszewskiego dotyczący sposobów monitorowania i oceny stanu bezpieczeństwa teleinformatycznego przez odpowiednie służby państwowe. Analizując przypadek Polski, autor charakteryzuje struktury zobowiązane do pełnienia tych funkcji, wskazując zarazem podstawy prawne ich działalności oraz przedstawiając najważniejsze zagrożenia i wyzwania, z jakimi muszą się one mierzyć. Ocenia też ich dotychczasowe osiągnięcia oraz wskazuje możliwe kierunki przyszłego rozwoju ich działań.

Artykuł Jana Burego porusza temat stosunkowo rzadko podejmowany przez badaczy, a bez wątpienia zasługujący na uwagę, zwłaszcza w kontekście masowego dziś wykorzystywania technik informatycznych w komunikacji – problem wyzwań towarzyszących szyfrowaniu i kodowaniu danych. Ujmując zagadnienie w perspektywie historycznej, autor przybliża zarówno metody i narzędzia kodowania danych, jak i sposoby i środki przełamywania tego rodzaju zabezpieczeń. Zastanawia się również nad kategoriami podmiotów zainteresowanych szyfrowaniem i odszyfrowywaniem informacji przechowywanych lub przesyłanych z wykorzystaniem technologii informatycznych, ocenia poziom współcześnie stosowanych przez państwa zabezpieczeń danych w formie elektronicznej oraz podejmuje próbę prognozy sytuacji w tym względzie.

Kolejne dwa opracowania dotyczą spraw w większym stopniu związanych z wykorzystaniem technologii informatycznych przez struktury administracji rządowej oraz tempem rozwoju i charakterem współpracy w tej sferze w ramach Unii Europejskiej. Agnieszka Bógdał-Brzezińska omawia proces budowy w Polsce tzw. e-governmentu,

a więc wdrażania rozwiązań opartych na technologiach informatycznych do praktyki działania polskiej administracji publicznej. Patrząc na to zagadnienie przez pryzmat inicjatyw proponowanych i zalecanych przez UE, dokonuje oceny rezultatów tych wysiłków nie tylko pod kątem efektywności struktur administracyjnych państwa, ale też wpływu na jego bezpieczeństwo. Krzysztof Silicki przedstawia natomiast zakres i główne kierunki współpracy w UE w wymiarze bezpieczeństwa informatycznego. Nie ogranicza się przy tym do prezentacji organów i instytucji odpowiedzialnych w Unii Europejskiej za tego rodzaju zadania oraz omówienia dokonań w tym względzie w postaci rozmaitych ukończonych lub wciąż prowadzonych projektów, ale wskazuje też najpoważniejsze słabości, niedociągnięcia i braki tego aspektu unijnej współpracy.

Zbiór zamyka dokonana przez Rafała Tarnogórskiego analiza najważniejszego prawno-międzynarodowego dokumentu dotyczącego kwestii bezpieczeństwa teleinformatycznego, czyli Konwencji o cyberprzestępczości opracowanej pod auspicjami Rady Europy. Omówienie postanowień konwencji uzupełnia zamieszczony w zbiorze jej pełny tekst.

Analizowane w niniejszej książce zagadnienia z pewnością nie ukazują w pełni zakresu problematyki bezpieczeństwa teleinformatycznego, ani też nie reprezentują wszystkich możliwych sposobów jej ujęcia oraz oceny. Mamy jednak szczerą nadzieję, że przez tę „niepełność" zbiór przyczyni się do rozwoju dyskusji o problemach bezpieczeństwa teleinformatycznego, zachęcając czytelników do polemiki i uzupełnień. To zaś z pewnością przysłużyłoby się głębszemu zrozumieniu problemów i, wiążących się z rozwojem technologii informatycznych oraz cyberprzestrzeni, wyzwań, z którymi zmierzyć się muszą dziś i w przyszłości współczesne państwa, w tym Polska.

Marek Madej, Marcin Terlikowski