Marek Górka
Politechnika Koszalińska

Wyzwania dla polityki bezpieczeństwa w kontekście cyberzagrożeń

Wraz z szybkim i intensywnym rozwojem technologii informatycznych i komunikacyjnych nastąpiła znaczna zmiana perspektywy świata. Komputery odgrywające kluczową rolę w rozwoju technologicznym zaczęły tworzyć wirtualny świat, gdzie każdy element ludzkiego życia ma swój alternatywny odpowiednik, począwszy od zakupów, pieniędzy po związki międzyludzkie. Te technologiczne innowacje nie tylko redefiniują ludzkie życie, lecz także na nowo definiują przestępczość i terroryzm. Niepokojące są nowe typy cyberataków, których przeprowadzenie jest możliwe dzięki temu, że infrastruktura państwa w przeważającej części jest obsługiwana przez komputery. Dynamiczny rozwój technologii oraz uzależnienie od cyberprzestrzeni mogą prowadzić nie tylko do problemów technicznych dla jednej instytucji bądź grupy ludzi, ale do zagrożeń mających konsekwencje dla całych narodów i państw. Teza ta, choć jest oczywista i zrozumiała dla użytkowników cybertechnologii w XXI w., to jednak jeszcze dwie dekady temu nie była postrzegana w kategoriach polityki bezpieczeństwa państwa.

W literaturze przedmiotu jest podawanych wiele opisów i przykładów współczesnych cyberzagrożeń, a także skutków, jakie one niosą dla państwa i jego obywateli. David Wall jako redaktor pracy *Crime and the Internet*[1], wraz z innymi autorami opisuje obawy, które towarzyszą od czasu rozwoju Internetu. Popularnym pytaniem w toczących się debatach na temat cyberbezpieczeństwa jest to, czy cybertechnologia w rękach nieodpowiedzialnego człowieka może się stać największym zagrożeniem dla pokoju na świecie od czasu II wojny światowej.

Niewłaściwe wykorzystanie, w tym przypadkowe nadużycia lub utrata kluczowych własności intelektualnych oraz kradzież danych dotyczących stanu państwa, firm czy też upublicznienie informacji na temat zdrowia najważniejszych osób w państwie, mogą mieć istotny wpływ na bezpieczeństwo publiczne. Książka pod

[1] *Crime and the Internet*, ed. D. Wall, New York 2001.

redakcją Ruth Taplin *Managing Cyber Risk in the Financial Sector*[2] dotyka właśnie tematu instytucji w cyberprzestrzeni, która w okoliczności cyberataku może mieć poważne konsekwencje na przykład dla sektora finansowego. Włamanie przez osoby wrogo nastawione do określonej firmy może powodować nie tylko straty finansowe, lecz także prowadzić do przerwania jej działalności bądź uszkodzenia jej majątku fizycznego oraz utraty dobrego wizerunku publicznego. Temat zagrożeń cybernetycznych dla funkcjonowania instytucji w sektorach państwowym i prywatnym jest coraz bardziej popularnym i znaczącym problemem dla całego obszaru polityki bezpieczeństwa państwa.

Okazuje się również, że cyberbezpieczeństwo jest obszarem badawczym wymagającym interdyscyplinarnego podejścia w zapobieganiu cyberzagrożeniom. Wiedza z zakresu zarządzania ryzykiem, ale i wiedza w obszarze technologii, prawa, wywiadu, systemu bankowego składa się na wszystko to, co można obecnie nazwać polityką bezpieczeństwa.

Artykuł próbuje zdefiniować słowo *cyberprzestępczość*, a także porusza problem różnych rodzajów cyberprzestępstw, ze szczególnym uwzględnieniem takiego zjawiska jak *phishing*. Niniejsza analiza jest także próbą zrozumienia, dlaczego tak wiele cyberprzestępstw jest nieujawnionych. Wskazano także kilka problemów, które bezpośrednio wiążą się z zadaniami organów ścigania w zakresie cyberprzestępstw. Opisując działania policji w obszarze cyberbezpieczeństwa, praca podkreśla problemy, które wymagają rozwiązania, na przykład brak koordynacji w egzekwowaniu prawa, brak wspólnego porozumienia na szczeblu międzynarodowym w sprawie natury cyberprzestępczości czy też brak wymiany informacji między instytucjami.

Główną ideą pracy jest wskazanie, że czynniki gospodarcze i instytucjonalne w obliczu cyberataków zmuszają do wielu działań profilaktycznych nie tylko ze strony państwa, lecz także zwykłych obywateli. A zatem fundamentem do prowadzenia skutecznej polityki cyberbezpieczeństwa są nie tylko prawne, technologiczne, ale przede wszystkim behawioralne mechanizmy obronne stosowane przez osoby prywatne. W tym zakresie istotna jest innowacyjność, zwłaszcza że cyberzagrożenia mogą przybierać różne formy, a nowe narzędzia inwazji cybernetycznej są stale aktualizowane.

Celem niniejszego artykułu jest zbadanie wybranych aspektów cyberzagrożeń i ich wpływu na funkcjonowanie państwa oraz jego obywateli. Drugim celem pracy jest analiza związku, który zachodzi między technologią informacyjną a polityką bezpieczeństwa państwa. Treści artykułu wskazują więc na atrybuty cybertechnologii, które mogą wpływać na decyzje podejmowane przez politycznych decydentów. Celem pracy jest także podkreślenie, że polityka bezpieczeństwa państwa, która w wyniku zagrożeń o różnym charakterze coraz częściej przybiera naturę hybrydową, uwzględnia zarówno tradycyjny, jak i cybernetyczny wymiar zagrożeń.

[2] *Managing Cyber Risk in the Financial Sector*, ed. R. Taplin, New York 2016.

W niniejszej pracy analiza badawcza jest skoncentrowana na sprofilowaniu cyberzagrożeń na podstawie najczęściej zachodzących przypadków cyberincydentów. Jednak podjęta w artykule klasyfikacja poszczególnych zjawisk nie odpowiada na pytanie, które z tych zagrożeń mogą mieć największy zakres oddziaływania na państwo i społeczeństwo, a tym samym które z nich stanowią największe zagrożenie dla porządku publicznego. Wynika to bowiem z natury tych procesów, których konsekwencje są trudne do przewidzenia. Dlatego tak ważna jest – sygnalizowana w pracy – potrzeba edukacji w zakresie bezpieczeństwa cybernetycznego. Ponadto opisane w artykule możliwości zaistnienia poszczególnych cyberincydentów oraz ich źródła stanowią punkt wyjścia do podjętych rozważań na temat działań o charakterze prewencyjnym. Praca ma także charakter syntetyczny, jest bowiem próbą przybliżenia stanu badań na podstawie wybranej zagranicznej literatury przedmiotu.

Centralnym punktem pracy jest polityka bezpieczeństwa, przed którą pojawiają się wciąż nowe wyzwania. To właśnie państwo jako główny gwarant i monopolista co do użycia siły zapewnia bezpieczeństwo swoim obywatelom. Niestety, wiele cyberzagrożeń – w przeciwieństwie do tych tradycyjnych – nie jest widocznych, a ponadto cyberprzestrzeń stanowi element niebezpieczeństwa nie tylko dla egzystencji ludzi, ale też instytucji państwowych. Tym samym można postawić tezę, że funkcjonowanie infrastruktury informatycznej jest kluczowym problemem współczesnej polityki bezpieczeństwa.

Wybrane poziomy cyberbezpieczeństwa

Uwaga, jaką poświęca się obecnie polityce bezpieczeństwa i która odnosi się do wielu współczesnych zagrożeń, zmusza do postawienia pytania, czy można mówić także o polityce cyberbezpieczeństwa. Zważywszy na fakt, że cyberprzestrzeń stanowi odzwierciedlenie niemal wszystkich aspektów życia zbiorowego, pytanie wydaje się nie tylko uzasadnione, ale i konieczne dla zrozumienia współczesnych zagrożeń.

Podejmując się kompleksowej próby oceny cyberprzestrzeni, można zauważyć, że jest to domena składająca się z wielu warstw, które wzajemnie się przenikają, jak sfera państwowa i prywatna lub cywilna i militarna czy też działalność jednostkowa i zbiorowa. Koncepcja funkcjonowania cyberprzestrzeni nie jest wyłącznie stosowana w dziedzinie wojskowej, a tym samym nie odnosi się tylko do ofensywnych i defensywnych działań związanych z cyberwojną. Cyberoperacje są przeprowadzane w wielu wymiarach funkcjonowania społeczeństwa. Przykład stanowią operacje w zakresie finansów sektora prywatnego, telekomunikacji czy też handlu detalicznego, w których szczególny nacisk kładzie się na zapobieganie kradzieży danych.

Obecnie występujące w cyberprzestrzeni zagrożenia są znacznie bardziej różnorodne niż na przykład kradzież tożsamości. Cyberzagrożenia, choć są powszechnie znane, to jednak często ich natura oraz specyfika jest słabo poznana. Globalne rozprzestrzenianie zagrożeń cybernetycznych rozciąga się od działań wrogiego państwa przez podmioty o charakterze niepaństwowym po organizacje ekstremistyczne i radykalne. Popularne w debacie publicznej są pojęcia odnoszące się do takich określeń, jak *malware*, wirusy, złośliwe kody czy też ataki typu Distributed Denial of Service (DDoS).

Symboliczną już ilustracją możliwości oraz zagrożenia cyberataków są wydarzenia z 2010 r. w Iranie. Wirus o nazwie kodowej Stuxnet, którego twórcami byli specjaliści ze Stanów Zjednoczonych i Izraela, przeniknął do irańskiego programu nuklearnego, doprowadzając do niebezpiecznych awarii systemu i zakłóceń operacji podczas procesu wzbogacania uranu[3].

Wiele krajów stosuje również systemy komputerowe w związku z wyborami. Sytuacja, w trakcie której zdeterminowany haker w celu manipulacji danymi atakuje niepewne i słabe systemy odpowiedzialne za przesyłanie i liczenie głosów wyborczych, może mieć wpływ na ostateczne wyniki głosowania. Możliwość zaistnienia paraliżu, który doprowadzi chaosu, destabilizacji oraz braku zaufania do rządu, jest bardzo realna. Internet to także źródło oraz nośnik powielania fałszywych i dyskredytujących informacji, które również mogą wpływać na szanse wyborcze kandydata ubiegającego się o wysokie stanowisko państwowe.

Dużym wyzwaniem związanym z funkcjonowaniem ludzi w cyberprzestrzeni jest utrzymanie porządku i troska o przestrzeganie prawa w Internecie. Ważna w tym przypadku jest także profilaktyka. Jako uzupełnienie tematu należy wskazać rolę w zapobieganiu przestępczości. Jeden ze sposobów zwalczania cyberzagrożeń polega na wykorzystaniu nowych produktów i technologii. Część organizacji pozarządowych aktywnie wspiera instytucje publiczne i stara się zidentyfikować luki w zabezpieczeniach nowych technologii i zachęcać przedstawicieli przemysłu do modyfikowania projektów w celu zmniejszenia możliwości popełnienia przestępstwa bez pogorszenia użyteczności cybertechnologii.

Inna taktyka polega na aktywnym projektowaniu urządzeń do kontroli lub blokowania możliwych cyberzagrożeń. W tym celu wprowadza się do urządzeń technologię, która może wyeliminować negatywne zjawiska przez stosowanie różnego rodzaju blokad. Wymaga to zazwyczaj używania oprogramowania zabezpieczającego, szyfrowania, filtrów spamowych itp. Jednak wpływ wielu z tych środków ogranicza również indywidualną swobodę. Wyzwaniem jest stosowanie rozwiązań technologicznych w celu osiągnięcia celów w zakresie zapobiegania przestępczości, z jednoczesnym osiągnięciem akceptowalnej równowagi między bezpieczeństwem a prywatnością[4].

[3] W.D. Bryant, *International Conflict and Cyberspace Superiority Theory and Practice*, New York 2016, s. 56.

[4] D.S. Wall, *The Internet as a Conduit for Criminals* [w:] *Information Technology and the Criminal Justice System*, ed. A. Pattavina, London 2005, s. 77–98.

W przypadku większości przedsiębiorstw i organizacji informacje są – bądź powinny być – traktowane jako wrażliwe aktywa ze szczególną uwagą odpowiedzialnego za nie personelu. Na przykład operatorzy systemów, odpowiedzialni za proces transferów finansowych, muszą być bardzo czujni i dostarczać jasnych wytycznych przy realizacji operacji finansowych[5].

Znaczenie cyberwywiadu

Coraz większa siła polityczna i handlowa Internetu zachęca do udziału w nowym modelu gospodarczym, w którym kapitałem jest informacja. Jeszcze w latach 90. XX w. cyberprzestrzeń nie była w centrum zainteresowań służb wywiadowczych, jednak obecnie jest uważana za najważniejszy element tajnych służb.

Wywiad oparty na zaawansowanych technologiach ma kluczowe znaczenie dla skuteczności działania każdego podmiotu funkcjonującego w przestrzeni publicznej. Technologia jest pożądanym produktem dla obcych państw, zwłaszcza tych wrogo nastawionych. Ten rodzaj szpiegostwa jest szkodliwy, zwłaszcza że tak wiele kontraktów i projektów między instytucjami państwowymi a sektorem publicznym jest uzależnionych od komputerów i Internetu. Nic więc dziwnego, że zagrożenia wynikające z działań cyberwywiadu i realizowane przez obce państwa i organizacje stały się poważnym problemem międzynarodowym.

Zakładając, że sektor prywatny – szczególnie w demokracjach liberalnych – ma ogromny wpływ na jakość i stopień funkcjonowania państwa, można założyć, że wszelkie problemy związane z cyberbezpieczeństwem w zakresie inicjatyw prywatnych będą miały ogromne odzwierciedlenie na poziom bezpieczeństwa państwa. Działania wywiadowcze dostarczają decydentom uporządkowanego podejścia do identyfikacji zagrożeń, a także są kluczowym elementem w przygotowywaniu odpowiedzi na wrogie i szkodliwe działania w poszczególnych sektorach gospodarczych.

Odpowiedzialność za cyberbezpieczeństwo nie opiera się wyłącznie na służbach państwowych. Sektor prywatny coraz częściej współpracuje z rządem w celu wymiany i rozpowszechniania informacji. Ale fakt ten niesie za sobą także konsekwencje dla obu stron. Wiele wątpliwości wzbudzają kwestie związane z ochroną danych w obszarze biznesu.

Można postawić i taką tezę, że rozwój gospodarczy wielu krajów zależy i będzie zależał od cyberbezpieczeństwa. Służby państwowe w zakresie gospodarki w analogiczny sposób dokonują oceny zagrożeń i ich wpływu na funkcjonowanie przedsiębiorstw państwowych oraz prywatnych. Podjęte tego typu wysiłki umożliwiają zrozumienie otoczenia, w którym funkcjonuje określony podmiot oraz pomagają

[5] S. Arumuga, *Impact of Cyber Crime on Virtual Banking*, źródło: https://www.researchgate.net/publication/228151273_Impact_of_Cyber_Crime_on_Virtual_Banking [dostęp: 2.04.2017].

dostrzec ryzykowne sytuacje. Pracownik odpowiedzialny za cyberbezpieczeństwo i pracujący w sektorze prywatnym musi monitorować otoczenie własnej organizacji w celu analizy wpływu, jaki wywiera ono na ewolucję funkcjonowania instytucji. Istnieje także potrzeba przewidzenia, w jaki sposób zmiany mogą kształtować priorytety strategiczne i kierunki rozwoju własnego podmiotu oraz obcych i często konkurencyjnych organizacji. W tym znaczeniu cyberbezpieczeństwo instytucji jest rozpatrywane w kontekście dostępu do zasobów, potencjalnych zagrożeń i warunków środowiska pracy.

Cyberataki

Niemal wszystkie współczesne instytucje i organizacje funkcjonują na co dzień w oparciu na technologiach, dlatego cyberbezpieczeństwo dla każdej z nich jest priorytetem. Jednak należy zdawać sobie sprawę, że nie każdy przeciwnik bądź konkurent zmierza do wykorzystania tych technologii w celu dokonania awarii czy paraliżu po przeciwnej stronie[6].

Przykładem tego są działania podejmowane przez haktywistów, które w wielu przypadkach obierają sobie za cel publiczną dyskredytację adresata, na skutek której ucierpi reputacja wybranej organizacji. Haktywiści są to osoby lub organizacje, które włamują się do systemów komputerowych, uzasadniając to celami politycznymi lub społecznymi[7].

Drugim rodzajem podmiotu tworzącego cyberzagrożenia są cyberprzestępcy, którzy dążą do uzyskania zysku z kradzieży danych. Cyberprzestępca często zmusza ofiarę do zapłacenia okupu za klucz do dostępu do swoich danych za pomocą płatności online.

Trzecim zagrożeniem dla organizacji państwowych jest wspomniany wyżej obcy wywiad, który przekazuje informacje do swojego mocodawcy na temat nowych

[6] W literaturze przedmiotu za główną różnicę między atakiem cybernetycznym i cyberterroryzmem uważa się kwestię intencji czy też motywacji sprawcy. Osoba dokonująca cyberataku może mieć między innymi motywy finansowe. Natomiast najważniejszą intencją cyberterrorysty jest zawsze motyw polityczny, społeczny lub religijny, za: A. Dean, *Cyber Threats in the 21st Century*, „Security" 2012, no. 49/9, s. 70–76.

[7] Haktywizm jest uznawany za hybrydową aktywność cybernetyczną. To wykorzystanie technologii komputerowych w ułatwianiu protestów online, powodowaniu zamieszek lub nieposłuszeństwa w cyberprzestrzeni przez celowe zakłócenie przepływu informacji. „Hacking" można opisać jako aktywność wykonaną w celu sprawdzenia swoich umiejętności. Jednak te działania mogą być wykorzystywane przez przestępców i grupy terrorystyczne. Haktywizm z intencją polityczną różni się od cyberterroryzmu. Działalność hakerów jest ukierunkowana na uzyskiwanie i ujawnianie poufnych danych, często w celu skompromitowania swoich ideologicznych przeciwników, za: T. Jordan, P.A. Taylor, *Hacktivism and Cyberwars Rebels with a cause?*, London–New York 2014, s. 1–19.

produktów, planów i innych istotnych danych. Tajne służby finansowane przez państwo są profesjonalnie zorganizowane i mają skuteczne narzędzia, aby uruchomić swoje ataki. W wielu przypadkach podmioty te używają złośliwego oprogramowania, aby skutecznie dokonywać cyberataków, które powodują ogromne szkody dla przedsiębiorstw i organizacji.

Cyberataki są coraz bardziej wyrafinowane, a uszkodzenia, do których dochodzi, wynikają z możliwości unikania przez szkodliwe oprogramowanie barier antywirusowych. Ukierunkowane ataki często wykorzystują luki w obrębie komputerów lub sieci, które nie są znane ich dystrybutorom oraz osobom i organizacjom z nich korzystających, dzięki czemu te zaawansowane programy mogą zostać w niezauważony sposób przemycone.

Dostęp do sieci przez nieupoważnione podmioty oraz kradzież danych przez dłuższy okres może nie powodować szkód w komputerze lub w sieci, co byłoby natychmiast zauważone. Obce służby mają na celu długoterminowe utrzymanie dostępu do źródeł, co daje możliwość kontrolowania oraz monitorowania baz danych o wysokiej wartości wywiadowczej, takich jak jednostki rządowe i branże finansowe bądź produkcyjne.

Cyberataki są ogromnym zagrożeniem dla bezpieczeństwa narodowego i gospodarki. Ich celem stają się żywotne zasoby państwa, usługi finansowe, agencje rządowe, korporacje medialne i niezliczona liczba firm z sektora prywatnego. Szczególnie intrygujące, a zarazem najgroźniejsze dla bezpieczeństwa państwa jest połączenie sił i możliwości wrogich podmiotów, takich jak cyberprzestępcy, cyberterroryści, hakerzy i służby państwowe.

Zaawansowane cyberataki przeciwko infrastrukturze krytycznej stanowią dowód na to, że zagrożenia płynące z cyberprzestrzeni mogą poważnie zdestabilizować sytuację w przestrzeni publicznej. Między innymi z tego powodu rządy wielu państw traktują cyberprzestrzeń jako domenę operacji wojskowych. Podejmowane próby w zakresie działań zaradczych mają zasadnicze znaczenie dla wykrywania ukierunkowanych cyberataków oraz przy wdrażaniu skutecznych reakcji.

Phishing

Rozwój technologii informacyjnych wymusił zmiany w systemie kontroli dostępu w sektorach IT i sektorach bankowych. Istnieje wiele technologii służących do przeciwdziałania włamaniom, ale obecnie żadna metoda nie jest całkowicie skuteczna. Najbardziej niebezpieczne oszustwa skierowane na codzienne działania bankowe są określane jako *phishing*. Przestępcy próbujący dokonać tego rodzaju oszustwa przedstawiają się jako osoby godne zaufania w komunikacji elektronicznej. Dokonują tego w celu uzyskania poufnych informacji, takich jak nazwy użytkowników, hasła, dane karty kredytowej itp.

Większość bankowości elektronicznej posiada coraz bardziej profesjonalne i przemyślane elementy zabezpieczeń, takie jak szyfrowanie, określanie maksymalnych limitów pieniężnych, autoryzacja klienta czy też uwierzytelnianie instrukcji płatniczych. Istnieje wiele technologii dostępnych w celu przeciwdziałania włamaniom do sieci, ale żadna metoda nie jest całkowicie bezpieczna. Sposobem na zwiększenie bezpieczeństwa są działania odbywające się na trzech poziomach: pierwszy z nich dotyczy bezpieczeństwa urządzeń technologicznych, drugi edukacji użytkowników w zakresie cyberbezpieczeństwa, trzeci odnosi się do monitorowania sieci pod kątem słabości i naruszeń[8].

Każda usługa bankowa dostarczana klientowi za pomocą systemu komputerowego jest nazywana wirtualną bankowością. Głównymi czynnikami wpływającymi na bankowość wirtualną są wymagania klientów, coraz szersze, globalne relacje handlowe oraz dynamiczny rozwój technologii. Popularność, jaką cieszą się wirtualne usługi bankowe wśród klientów, wynika przede wszystkim z szybkości, wygody i całodobowego dostępu. Między innymi z tych powodów można przypuszczać, że prawdopodobnie tego typu cyberusługi finansowe będą dominować w przyszłości[9].

Próby wyłudzenia informacji są skierowane na dane klientów banków, niezbędne do wykonywania usług płatniczych online. Analizy tego zjawiska wykazują, że cyberoszuści potrafią ustalić, w jaki sposób potencjalna ofiara ma związek z wybraną instytucją finansową, a następnie przesłać do tej ofiary sfałszowany e-mail[10].

Większość metod fałszowania wiadomości wykorzystuje jakąś formę oszustwa technicznego, która ma na celu utworzenie łącza w e-mailu oraz łudząco podobnej strony internetowej, która prowadzi ofiarę do fikcyjnej organizacji. Niestandardowe adresy URL lub użycie poddomeny to najczęstsze sposoby wykorzystywane przez phisherów. Inną popularną metodą jest „przekierowanie" linku zakotwiczonego w prawidłowym tekście do strony stworzonej przez oszustów. Następnym sposobem jest używanie łączy zawierających symbol „@", które pierwotnie przeznaczone są jako sposób na podanie nazwy użytkownika i hasła. Na przykład link typu „http: //www.google.com@twoj.bank.com/" może skłonić zwykłego obserwatora do przekonania, że otworzy stronę pod adresem „www.google.com", podczas gdy w rzeczywistości kieruje przeglądarkę na inną stronę. Takie adresy URL zostały wyłączone w programie Internet Explorer, a przeglądarki internetowe Mozilla i Opera zdecydowały się na wyświetlenie komunikatu ostrzegawczego bądź na umożliwienie kontynuowania pracy na tej witrynie lub jej anulowanie. Niektóre oszustwa phishingowe używają poleceń JavaScript w celu zmiany paska adresu.

[8] K. Jansson, R. von Solms, *Phishing for phishing awareness*, „Behaviour & Information Technology" 2013, vol. 32/6, s. 584–593; D.L. Cook, V.K. Gurbani, M. Daniluk, *Phishwish: a simple and stateless phishing filter,* „Security and Communication Networks" 2009, vol. 2/1, s. 29–43.

[9] S. Arumuga, *Impact...*

[10] K. Jaishankar, *Identity related Crime in the Cyberspace: Examining Phishing and its impact*, „International Journal of Cyber Criminology" 2008, vol. 2.1, s. 10–15.

Można to zrobić przez umieszczenie obrazu prawidłowego adresu URL na pasku adresu albo zamknięcie oryginalnego paska adresu i otwarcie nowego z legalnym adresem URL[11].

Ten rodzaj kradzieży staje się coraz popularniejszy ze względu na łatwość, z jaką niepodejrzewający niczego ludzie często ujawniają osobiste informacje oszustom, w tym numery kart kredytowych, numery ubezpieczenia społecznego, imiona członków rodziny itp. Istnieje również realna możliwość, że złodzieje tożsamości mogą pozyskiwać informacje przez dostęp do rejestrów publicznych. Po uzyskaniu tych informacji phisherzy mogą używać danych osobowych do tworzenia fałszywych kont w imieniu ofiary czy też uniemożliwiać ofiarom dostęp do własnych kont.

Popularną metodą ataku phishingowego jest także wysyłanie e-maili, które ostrzegają użytkownika z niewielkim lub nieznacznym wyprzedzeniem, że konto zostanie zamknięte, dopóki osoba będąca właścicielem depozytu nie potwierdzi ponownie danych wymaganych przy operacjach finansowych. Do częstych przypadków można zaliczyć także otrzymywanie poczty HTML z dołączonymi formularzami zgłoszeniowymi. Wszelkie informacje przesłane za pośrednictwem poczty elektronicznej są zazwyczaj opatrzone uzasadnionym i wiarygodnym komunikatem[12].

Obecnie, gdy coraz więcej instytucji zapewnia większy dostęp online swoim klientom, profesjonalni przestępcy z powodzeniem wykorzystują techniki phishingowe w celu kradzieży danych umożliwiających podszywanie się pod dowolną osobę lub bezpośrednie pozyskiwanie w nielegalny sposób środków finansowych.

Niechęć do ujawniania cyberprzestępstw

W przeciwieństwie do nadmiernej mobilizacji środków zaradczych w zakresie cyberbezpieczeństwa istnieje niedostateczna liczba zgłaszanych przypadków cyberprzestępczości. Istnieje również spora liczba interpretacji dotyczących osób bądź organizacji, które są ofiarami cyberprzestępczości. Okazuje się, że nie tylko ofiary mogą się różnić między sobą, ale wyrządzone im szkody mogą być odmiennie postrzegane.

Środowisko cybernetyczne uniemożliwia próby uzyskania pełnego obrazu poziomów cyberprzestępstw, ponieważ informacje o takich przypadkach nie przepływają do policji w taki sam sposób jak informacje o tradycyjnych przestępstwach. Jedynym sposobem, w jaki można naprawdę zdobyć wiarygodne statystyki

[11] S. Arumuga, *Impact...*

[12] D. Kaur, S. Kalra, *Five-tier barrier anti-phishing scheme using hybrid approach*, „Information Security Journal: A Global Perspective" 2016, vol. 25/4–6, s. 247–260; G. Varshney, M. Misra, P.K. Atrey, *A survey and classification of web phishing detection schemes*, „Security and Communication Networks" 2016, vol. 9/18, s. 6266–6284.

dotyczące indywidualnej wiktymizacji, są badania ankietowe. W tym przypadku należy poczynić kilka uwag. Otóż jedną z grup społecznych, które są szczególnie narażone na cyberprzemoc lub cyberprzestępstwa, są młodzi ludzie. Jest to o tyle specyficzne środowisko, że zazwyczaj jest bardzo hermetyczne i nieufne. Ponadto cyberagresja w przypadku ofiar jest bardzo trudno dostrzegalna.

Analogiczna sytuacja występuje także wśród ofiar cyberprzestępczości w pozostałych przedziałach wiekowych. Osoby dorosłe są również niechętne do przyznania się, że były ofiarami cyberoszustw lub też nie zdawały sobie sprawy z tego, że od jakiegoś czasu nimi były. Do takich przypadków można zaliczyć najbardziej niebezpieczne oszustwa skierowane na codzienne działania bankowe. Jedną z takich metod jest wspomniany phishing, który jest działalnością przestępczą wykorzystującą cybertechnologię wraz z technikami manipulacji społecznej. W wyniku tych oszustów próbuje się uzyskać poufne informacje, takie jak nazwy użytkowników, hasła i dane karty kredytowej, podszywając się pod osobę, która w odczuciu społecznym jest godna zaufania w komunikacji elektronicznej. W przypadku cyberprzestępstw o charakterze finansowym stosunkowo niewiele jest przypadków zgłaszanych bezpośrednio policji, a skarżący są często odsyłani do swoich banków, które również są ofiarami.

Na poziomie personalnym może się pojawić niechęć do zgłaszania przestępstw ze względu na konsekwencje osobiste, takie jak wstyd czy stygmatyzacja społeczna. Na poziomie korporacyjnym istnieje zaś obawa przed negatywnym wpływem na polityczny, moralny lub biznesowy wizerunek organizacji. A zatem skutki niekorzystnej reklamy znacznie zmniejszają chęć firm do zgłaszania przypadków cyberprzestępstw organom ścigania. W takiej postawie jest także pewien element egoizmu, ponieważ korporacje, ukrywając przed opinią publiczną wstydliwe przypadki, nie przestrzegają innych organizacji przed podobnymi sytuacjami. W ten sposób nie dbają o ujawnienie zagrożeń i przeciwdziałanie im, a tym samym nie troszczą się o bezpieczeństwo publiczne tylko o własny wizerunek publiczny[13].

Służby policyjne a cyberzagrożenia

Technologie internetowe i medialne stanowią konkretne wyzwania dla systemów wymiaru sprawiedliwości w sprawach karnych. Wyzwania te leżą przede wszystkim w zdolnościach organizacji i ich kultur zawodowych do stawiania czoła nowym wymaganiom oraz zdolności profesjonalistów w ramach tych organizacji. Nacisk jest położony na policję, ponieważ to ona jako instytucja publiczna pierwsza reaguje na cyberprzestępstwa.

W większości krajów zachodnich policja posiada struktury lokalne, ale istnieją również poziomy krajowe lub federalne (np. w Niemczech, w Stanach

[13] D.S. Wall, *The Internet...*, s. 77–98.

Zjednoczonych czy w Wielkiej Brytanii) oraz międzynarodowe organizacje policyjne (np. Europol, Interpol), które badają przestępstwa i zajmują się zbieraniem informacji wywiadowczych oraz analizą zjawiska przestępczości zorganizowanej.

Jak wspomniano wcześniej, niewiele przestępstw związanych z cyberprzestrzenią jest zgłaszanych policji. W większości przypadków służby policyjne reagują w momencie pojawienia się zawiadomienia od osób publicznych lub placówek lokalnych do zbadania przestępstw komputerowych.

Współcześnie przestępstwa kryminalne coraz częściej wymagają elektronicznych dowodów w celu ustalenia motywów i miejsca pobytu, a wiele z nich znajduje się na nośnikach pamięci i dotyczy między innymi danych o ruchu internetowym i rejestrów telefonów komórkowych. Niektóre służby policyjne utworzyły własne jednostki, podczas gdy inne wchodzą w strategiczne sojusze z innymi siłami policyjnymi w celu świadczenia usług z zakresu cyberbezpieczeństwa[14].

Często pojawiającą się uwagą ze strony organów ścigania jest to, że instytucje te nie mają możliwości dotrzymania kroku przestępcom, szczególnie w odniesieniu do coraz bardziej zaawansowanych procesów informatycznych. Taka sytuacja wzmacnia popularny pogląd, że przestępcy na poziomie zaawansowania technologicznego wyprzedzają policję. W tym stereotypie jest pewien element prawdy, ponieważ policja w większości przypadków zazwyczaj zajmuje się sprawami rutynowymi, które podlegają z góry określonym regułom postępowania oraz ścisłym ograniczeniom budżetowym. Utrudnia to natychmiastowe przyporządkowanie największych zasobów do pojawiających się spraw, a tym samym zdolności reagowania policji.

Do obowiązków pracy w policji należy wiele wyzwań dotyczących rozwiązywania nowych problemów związanych z cyberbezpieczeństwem. Są one dość powszechne we wszystkich gospodarkach neoliberalnych.

Pierwszym wyzwaniem jest uzyskanie finansowania w ramach istniejących zasad przyznawania zasobów i zarządzania nimi. Skupienie środków na konkretnym temacie często trudno uzasadnić w indywidualnych przypadkach. Strategie dotyczące policji są ograniczane do decyzji podejmowanych na poziomie centralnym z jednoczesnym oczekiwaniem na skuteczne efekty pracy.

Drugie wyzwanie polega na tym, że siły policyjne mają mniejsze szanse na finansowanie dochodzeń oraz zrealizowanie celu, gdy przestępstwo jest odmiennie postrzegane w różnych jurysdykcjach.

Trzecim wyzwaniem jest reagowanie na działania przestępcze. Większość publicznych działań policji opiera się na lokalnych i rutynowych działaniach.

[14] R. Leukfeldt, S. Veenstra, W. Stol, *High Volume Cyber Crime and the Organization of the Police: The results of two empirical studies in the Netherlands*, „International Journal of Cyber Criminology" 2013, vol. 7/11, s. 1–17.

W związku z tym pojawiają się trudności w prowadzeniu dochodzeń, gdy występują nowe zdarzenia[15].

W wielu przypadkach służby policyjne – podobnie jak inne agencje wymiaru sprawiedliwości w sprawach karnych – to instytucje o charakterze konserwatywnym, które zostały ukształtowane w tradycyjnym modelu biurokratycznym. Dlatego też instytucje państwowe, w tym policja, nie reagują szybko na gwałtowne zmiany. Zatem jednym ze sposobów, w jaki siły policyjne odnoszą się do nowych kwestii, jest powstanie w ich szeregach wyspecjalizowanych jednostek, do których są zaliczani oficerowie z odpowiednimi specjalizacjami. Chociaż te zjawiska stanowią rzeczywistą i widoczną odpowiedź, to jednak nie wolno zapominać, że zbyt duża profesjonalizacja może grozić marginalizacją problemu i zapobiegać szerszemu gromadzeniu i wymianie wiedzy między instytucjami zajmującymi się rozwiązywaniem bieżących problemów.

***

Internet bez wątpienia zmienił świat i sposób, w jaki współczesny człowiek żyje. Polityka, gospodarka, finanse, siły zbrojne, infrastruktura, służba zdrowia, kultura, a także służby wywiadowcze są silnie uzależnione od komputerów. Miliardy tajemnic i projektów przemysłowych są obecnie przechowywane w systemach, które są nierozłącznie związane z Internetem. Oznacza to, że są one podatne na ataki. Zagrożenia wymuszają również stosowanie na większą skalę szkoleń, które miałyby uświadamiać pracownikom instytucji publicznych zagrożenia związane z funkcjonowaniem w cyberprzestrzeni.

Wymiar wirtualny wzbudza w wielu kręgach rządowych duże zainteresowanie. Towarzyszy temu regularne zwiększanie budżetu państwa oraz tworzenie nowych organizacji koordynujących działania podmiotów publicznych w cyberprzestrzeni. Jednak obecna polityka wielu państw europejskich w zakresie cyberbezpieczeństwa, zarówno na szczeblu lokalnym, jak i międzynarodowym, nie jest na tyle kompleksowa ani spójna, aby skutecznie przeciwdziałać zagrożeniom wynikającym z powszechnego stosowania technologii informatycznej. Unikalne cechy cyberprzestrzeni stanowią wyzwanie dla obecnych struktur krajowych, pierwotnie stworzonych z myślą o przeciwdziałaniu konwencjonalnym zagrożeniom. Realizacja ta prowadzi rządy wielu państw do poszukiwania odpowiednich struktur i procesów, które mogłyby optymalnie przeciwdziałać nowemu zagrożeniu cybernetycznemu, chroniąc jednocześnie podstawowe prawa obywatelskie.

Internet stanowi nowe narzędzie do popełniania przestępstw. Ważne jest badanie jego wpływu na społeczeństwo, aby lepiej zrozumieć naturę cyberprzestępczości. Szczególnie zauważalny jest wpływ dynamicznej ekspansji cyberprzestrzeni, która przyczyniła się do przyspieszenia tendencji do zachowań przestępczych.

[15] D.S. Wall, *Policing Cybercrimes: Situating the Public Police in Networks of Security within Cyberspace*, „Police Practice and Research An International Journal" 2007, vol. 8/2, s. 183–205.

Cyberprzestrzeń zmienia także tradycyjne relacje między przestępcami a ofiarami. Wymusza tworzenie nowych regulacji prawnych wobec potencjalnie nowych oraz szkodliwych dla otoczenia zachowań. Zwiększając zasięg możliwości przestępców na skalę globalną, cyberprzestrzeń umożliwia przestępcom angażowanie się w nowe sposoby oraz dostarcza nowych możliwości nielegalnych działań.

Systemy komputerowe w wielu krajach obsługują infrastrukturę krytyczną, na przykład elektrownie jądrowe, wodociągi, dystrybucję i przesył gazu oraz prądu, transport publiczny czy szpitale. Wszystkie te elementy są potencjalnymi celami cyberataków. W kontekście dopasowana polityki, obronności oraz przemysłu do cyberprzestrzeni niezbędne wydaje się stosowanie edukacji dla cyberbezpieczeństwa.

Zachodzące procesy w wymiarze cyberprzestrzeni wciąż inspirują do nowych dyskusji w obszarze polityki państwa. Obecnie, jak udowadniają liczne cyberincydenty, klasyfikacja i zdefiniowanie procesów zachodzących w nowych technologiach jest jednym z kluczowych elementów polityki bezpieczeństwa. Zadaniem państwa oraz służb jemu podległych jest między innymi ochrona infrastruktury krytycznej oraz umożliwienie jej funkcjonowania w bezpiecznym środowisku informatycznym.

Challenges for security policy in the context of cyber threats

Summary

Cybersecurity has become a serious problem for nation states. This article discusses the themes that are present in the public debate on cybersecurity. The purpose of this article is also to reflect on the development of new cyber threats. The problem raised generates the need to analyze the functioning of institutions responsible for cybersecurity. Some new cyber threats are publicly announced by those authorized to do so – through the media – to promote remedies. Cyberthreats are not just a defect, but they can also be positive in some sense. They are an opportunity or impulse forcing public institutions to innovate in cyber security policy. The rise of cybercrime has forced the state to take new and more effective actions. Expansion of cybercrime phenomena can be fully appreciated by exploring this phenomenon in a technocratic but also socio-political context. Cybercrime affects and influences the quality of public space.

Key words: cyber security, cyber attacks, education for cyber security, phishing, security policy