Wstęp

Przeglądając strony internetowe, czytając prasę, a niekiedy nawet fachowe wydawnictwa, można odnieść wrażenie, że grono osób, które mogą powiedzieć wiele na temat cyberprzestępczości, jest bardzo liczne. Niestety, nie można poglądów przez nie przedstawianych uznać za podzielane przez środowisko naukowe, za zestaw uzgodnień o pojmowaniu zagadnienia cyberprzestępczości. Poglądy te są uwarunkowane czasem ich przedstawienia, obowiązującym stanem prawnym, dokumentami, które nie są źródłem prawa, i wykorzystywanymi technologiami. Co więcej, charakterystyczne dla nauk humanistycznych występowanie wielu paradygmatów naraz jest obecne w cyberprzestępczości.

Książka, którą Państwo macie przed sobą, ma charakter przeglądowy i dotyczy aspektów prawnych, kryminologicznych i w niewielkim stopniu technicznych cyberprzestępczości. Nie sposób było nie zawrzeć w niej także tematyki dowodów cyfrowych, wpływu technik teleinformatycznych na przestępczość oraz opisu systemu zwalczania cyberprzestępczości.

Publikacja ma charakter interdyscyplinarny, gdyż taka jest cyberprzestępczość. W poszczególnych rozdziałach zawarte są kryminologiczne i socjologiczne, prawne i techniczne spojrzenia na cyberprzestępczość. Jeśli chce się przedstawić opisywane pojęcia w sposób zrozumiały dla Czytelnika, te spojrzenia często mieszają się ze sobą. Autor dołożył starań, aby żadne z tych spojrzeń zbytnio nie dominowało nad pozostałymi. Cyberprzestępczość ciągle podlega dynamicznym zmianom, dlatego bardzo ważne jest holistyczne podejście do niej, uwzględniające wszystkie aspekty pozwalające zrozumieć zachodzące procesy. Wspomniana dynamika dotyczy wszystkich nowych technologii, ale najsilniej obserwowana jest w internecie, który spowodował, niekiedy rewolucyjne, zmiany w komunikowaniu się, handlu, edukacji i wielu innych dziedzinach, w tym, niestety, i przestępczości.

Konstrukcja niniejszej książki tworzona była na schemacie zakładającym gruntowną analizę przypadków cyberprzestępstw, na podstawie wielu różnych

źródeł, począwszy od informacji internetowych, a skończywszy na aktach sądowych i analizach specjalistycznych. Wykorzystane analizy specjalistyczne również były weryfikowane w wielu źródłach, gdyż trzeba było z nich odrzucić partykularne interesy ich autorów (np. wywodzących się z reprezentujących firmy komercyjne lub organizacje zainteresowane propagowaniem określonych tez). Jeżeli istniała tylko taka możliwość, to analizy były weryfikowane na podstawie aktów spraw i danych organów ścigania. Bardzo istotnym materiałem wykorzystanym w książce były publikowane wyniki badań naukowych oraz raporty organizacji międzynarodowych odrzucające czysto sensacyjny opis zdarzeń, a koncentrujące się na zjawisku. Dzięki takiemu podejściu, w swojej istocie, publikacja stanowi zbiór poglądów na temat cyberprzestępczości, identyfikujący opisywany obszar. Prezentowany paradygmat cyberprzestępczości nie musi być podzielany przez innych naukowców, z pewnością jednak będzie stanowił punkt odniesienia pozwalający na ocenę, krytykę, ale głównie na porozumienie prowadzące do bliższego prawdy zrozumienia tego zjawiska.

Potrzeba stworzenia takiej publikacji wyniknęła z braku dostępnych kompleksowych analiz cyberprzestępczości pod kątem jej zagrożenia dla bezpieczeństwa indywidualnej osoby, firmy lub organizacji, państwa czy regionu. Dostępne na polskim rynku publikacje nt. cyberprzestępczości mają charakter dziedzinowy. Historycznie za pierwszą pozycję z tego obszaru należy uznać książkę Ryszarda Czechowskiego i Piotra Sienkiewicza *Przestępcze oblicza komputerów* z 1993 roku[1], w której autorzy poruszyli tematykę bezpieczeństwa i przestępczości komputerowej na tle ówczesnych systemów komputerowych. Najlepsza publikacja, podejmująca ten temat od strony prawnej, to pochodząca z 2000 roku książka Andrzeja Adamskiego pt. *Prawo karne komputerowe*[2]. Zaletą tej pozycji jest wnikliwa analiza prawna oparta na poprawnym opisie technicznym opisywanych pojęć. Pomimo upływu lat i zmian w prawie karnym analizy przestępstw spotykanych w cyberprzestrzeni są prawidłowe i mogą służyć jako wzorzec podejścia do penalizacji czynów zapisanych w Kodeksie karnym po jego licznych nowelizacjach. Uzupełnieniem tej książki jest *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy* tego samego autora z 2001 roku[3], będąca analizą zapisów Konwencji Rady Europy o cyberprzestępczości. Z tego samego okresu pochodzi, również często cytowana, monografia Bogdana Fischera *Przestępstwa komputerowe i ochrona informacji*[4], która wyraźnie się zdezaktualizowała. Kolejna książka, mimo ciekawego tytułu

[1] R. Czechowski, P. Sienkiewicz, *Przestępcze oblicza komputerów*, Warszawa 1993.

[2] A. Adamski, *Prawo karne komputerowe*, Warszawa 2000.

[3] A. Adamski, *Przestępczość w cyberprzestrzeni. Prawne środki przeciwdziałania zjawisku w Polsce na tle projektu konwencji Rady Europy*, Toruń 2001.

[4] B. Fischer, *Przestępstwa komputerowe i ochrona informacji*, Zakamycze 2000.

– *Prawo w sieci. Zarys regulacji Internetu* Piotra Waglowskiego z 2005 roku[5], ma raczej charakter publicystyczny niż naukowy. Pozycja Dariusza Dorozińskiego *Hakerzy. Technoanarchiści cyberprzestrzeni* z roku 2001[6] jest już częściowo nieaktualna, a *Cyberprzestępczość* Macieja Siwickiego z 2013 roku[7] stanowi powielenie innych pozycji z jednoczesnym spłyceniem zagadnienia. Dosyć wąskie, ale jednocześnie ciekawe jest prawnicze spojrzenie na zagrożenie cyberterroryzmem zaprezentowane w *Ochronie prawna systemów informatycznych wobec zagrożenia cyberterroryzmem* Aleksandry Suchorzewskiej z 2010[8]. Z punktu widzenia prawniczego, ale bardzo ważnego dla informatyków pozyskujących i zabezpieczających ślady cyberprzestępstwa, należy także wspomnieć o publikacji Arkadiusza Lacha pt. *Dowody elektroniczne w procesie karnym* z 2004 roku[9], która jest doskonałym kompendium wiedzy o uzyskiwaniu, zabezpieczaniu i możliwościach wykorzystania dowodów elektronicznych w procesie karnym. Z punktu widzenia technicznego warto zwrócić uwagę na książki: *Szkoła hakerów. Podręcznik* z 2006 roku[10], *Metody inwigilacji i elementy informatyki śledczej* z 2011 roku[11] oraz *Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7* z 2013 roku[12], które w sposób szczegółowy przedstawiają metody, techniki i narzędzia wykorzystywane do popełniania wybranych cyberprzestępstw, ale także wskazują miejsca, w których należy poszukiwać śladów wskazujących na ich wykorzystanie, oraz narzędzia, jakich można użyć, aby te ślady ujawnić i zabezpieczyć. Zaletą tych pozycji jest prezentacja technicznego punktu widzenia na podstawie typowych, standardowych dla systemów operacyjnych rozwiązań, co sprawia, że wolniej ulegają procesowi starzenia się. Do pozycji technicznych, jednak o dużej porcji wiedzy z zakresów formalnych bezpieczeństwa informacji, które dotyczą cyberprzestępczości, zaliczyć trzeba publikacje: Krzysztofa Lidermana pt. *Analiza ryzyka i ochrona informacji w systemach komputerowych* z 2008 roku[13] oraz *Bezpieczeństwo informacyjne* z 2013 roku[14]. Inny zakres dotyczący technicznych aspektów zwalczania cyberprzestępczości zawiera

[5] P. Waglowski, *Prawo w sieci. Zarys regulacji Internetu*, Gliwice 2005.

[6] D. Dorozińskiego, *Hakerzy. Technoanarchiści cyberprzestrzeni*, Gliwice 2001.

[7] M. Siwicki, *Cyberprzestępczość*, Warszawa 2013.

[8] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Warszawa 2010.

[9] A. Lach, *Dowody elektroniczne w procesie karnym*, Toruń 2004.

[10] D. Put, W. Adamczyk, A. Wróbel, P. Bylina, *Szkoła hakerów. Podręcznik*, Kwidzyn 2006.

[11] A.M. Kalinowski, *Metody inwigilacji i elementy informatyki śledczej*, Kwidzyn 2011.

[12] H. Carvey, *Analiza śledcza i powłamaniowa. Zaawansowane techniki prowadzenia analizy w systemie Windows 7*, Gliwice 2013.

[13] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, Warszawa 2008.

[14] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2013.

monografia pod redakcją Edwarda Nawareckiego, Grzegorza Dobrowolskiego i Marka Kisiel-Dorohickiego pt. *Metody sztucznej inteligencji w działaniach na rzecz bezpieczeństwa publicznego* z 2009 roku[15]. Książką, w której autor próbuje połączyć spojrzenie prawnicze i techniczne w zakresie dowodów cyfrowych, jest publikacja Macieja Szmita z 2014 roku pt. *Wybrane zagadnienia opiniowania sądowo-informatycznego*[16]. Wymienione pozycje można uzupełnić o wiele książek, głównie publikowanych przez wydawnictwo Helion, będących tłumaczeniami pozycji zagranicznych, często ukazujących się na naszym rynku z dużym opóźnieniem, co sprawia, że z technicznego punktu widzenia są już przestarzałe[17]. Obszaru cyberprzestępczości w zakresie socjologicznym i kryminologicznym dotyczą także książki popularne, np. Wojciecha Orlińskiego *Internet. Czas się bać* z 2013 roku[18] i Kevina Mitnicka *Sztuka podstępu* z 2003 roku[19]. Żadna z wymienionych książek nie obejmuje wszystkich aspektów przedstawionych w tej publikacji.

Niniejsza publikacja nie jest także podręcznikiem uczącym, jak dokonywać cyberprzestępstwa ani jak je zwalczać, chociaż jedną z docelowych grup czytelników są funkcjonariusze organów ścigania zajmujący się zwalczaniem cyberprzestępczości. Książka ma w sposób krytyczny pokazać zagrożenia wynikające z wykorzystania nowoczesnych technologii przetwarzania informacji dla ich użytkowników. Ma także zwrócić uwagę, że cyberprzestępczość nie jest zwykłym przestępstwem, do którego wykrycia i ścigania wystarczają tradycyjne metody pracy organów ścigania i wymiaru sprawiedliwości. Ze względu na to, że cyberprzestępczość wykorzystuje nowoczesne technologie przetwarzania informacji, ale jednocześnie często korzysta z socjotechniki, dynamicznie reaguje na wymagania gospodarcze i ekonomiczne wyszukując luki prawne, trudno opracować proste i jednoznaczne metodyki jej zwalczania. Tym istotniejsze jest poznanie i zrozumienie pojęć i zależności związanych z działaniami przestępczymi w cyberprzestrzeni[20].

---

[15] E. Nawarecki, G. Dobrowolski, M. Kisiel-Dorohicki (red.), *Metody sztucznej inteligencji w działaniach na rzecz bezpieczeństwa publicznego*, Kraków 2009.

[16] M. Szmit, *Wybrane zagadnienia opiniowania sądowo-informatycznego*, Kraków 2014.

[17] Np. L. Klander, *Hacker proof, czyli jak bronić się przed intruzami*, Warszawa 1998; E. Amoroso, *Wykrywanie intruzów*, 1999; T.J. Klevinsky, S. Laliberte, A. Gupta, I.T. Hack, *Testy bezpieczeństwa danych*, Gliwice 2003; M. Horton, C. Mugge, *Notes antyhakera. Bezpieczeństwo sieci*, Warszawa 2004; D.L. Shinder, *Cyberprzestępczość. Jak walczyć z łamaniem prawa w sieci*, Gliwice 2004.

[18] W. Orliński, *Internet. Czas się bać*, Warszawa 2013.

[19] K. Mitnick, *Sztuka podstępu*, Gliwice 2003.

[20] Na tym etapie można przyjąć za T. Szubrychtem, że cyberprzestrzeń to przestrzeń komunikacyjna tworzona przez system powiązań internetowych. Ułatwia ona użytkownikowi sieci kontakty w czasie rzeczywistym. Obejmuje wszystkie systemy komunikacji elektronicznej, które przesyłają informacje pochodzące ze źródeł numerycznych. T. Szubrycht, *Cyberterroryzm jako nowa forma zagrożenia terrorystycznego*, Zeszyty Naukowe Akademii Marynarki Wojennej, nr 1/2005.

Ochrona cyberprzestrzeni stanowi obecnie jedno z podstawowych zadań strategicznych w obszarze bezpieczeństwa praktycznie każdego państwa[21]. Budowie społeczeństwa informacyjnego wykorzystującego nowe technologie teleinformatyczne towarzyszą zagrożenia dotyczące bezpieczeństwa zarówno samych systemów, jak i przetwarzanych z ich wykorzystaniem informacji.

W niniejszej pracy autor wykorzystał wyniki wieloletnich badań, z których wnioskami zapoznawał w przeszłości zainteresowanych problematyką cyberprzestępczości na łamach czasopism i w publikacjach specjalistycznych. Jeśli prezentowane w książce treści były już wcześniej publikowane przez autora, to zostały one powtórnie zweryfikowane i uzupełnione.

1. Cel publikacji

Głównym celem tej publikacji jest przedstawienie zbioru poglądów dotyczących pojęcia „cyberprzestępczość" i zagrożeń istniejących w cyberprzestrzeni, co powinno pozwolić na bliższe poznanie i zrozumienie problemu cyberprzestępczości. Rekapitulacja dotychczasowych poglądów jest podstawą dokonania syntezy cyberprzestępczości i w konsekwencji określenia jej paradygmatów. Można dyskutować, czy należy tworzyć nowe kategorie przestępstw w zależności od narzędzi, sprzętu lub mechanizmu, za pomocą których zostały one popełnione. Nie tworzy się kategorii przestępstw samochodowych lub pistoletowych. Jednakże ze względu na charakter i różnorodność metod, technik i narzędzi popełniania cyberprzestępstw, które odróżniają je od klasycznych przestępstw, należy taką kategorię wprowadzić. Cyberprzestępczość może być rozumiana w wąskim znaczeniu (przestępczość komputerowa) obejmującym każde nielegalne zachowania realizowane za pomocą działań elektronicznych nakierowanych na bezpieczeństwo systemów komputerowych i danych w nich przetwarzanych. Można także cyberprzestępczość rozumieć w szerokim znaczeniu (przestępczość związana z komputerami) – jako wszelkie nielegalne zachowania popełnione za pomocą lub względem systemu komputerowego czy sieci, w tym takie przestępstwa jak nielegalne posiadanie, oferowanie lub rozpowszechnianie informacji za pomocą systemu komputerowego lub sieci[22]. Tak rozumiana cyberprzestępczość mieści się w obszarze od przestępstw gospodarczych, takich jak: oszustwa, fałszerstwa, szpiegostwo przemysłowe, sabotaż i wymuszenia, poprzez piractwo komputerowe

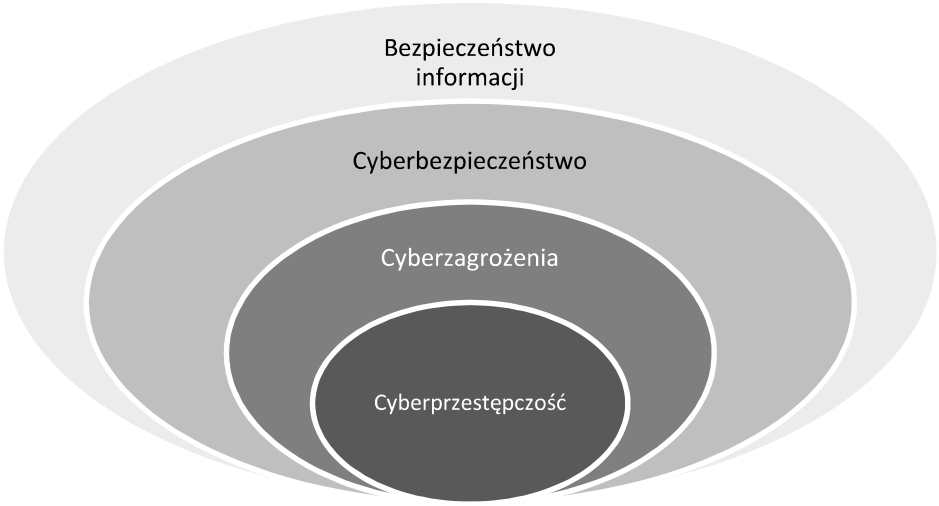
[21] *Biała Księga Bezpieczeństwa Narodowego*, BBN, Warszawa 2013, s. 63.

[22] Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders. Crimes related to computer networks, UN, Vienna 2000, s. 4. http://www.uncjin.org/Documents/congr10/10e.pdf, dostęp: 16.07.2013.

i inne przestępstwa przeciwko własności intelektualnej oraz przypadki naruszenia prywatności, propagację nielegalnych i szkodliwych treści, ułatwianie prostytucji i inne przestępstwa przeciwko moralności, aż do przestępczości zorganizowanej. Tę drugą granicę wyznacza także cyberterroryzm obejmujący ataki na bezpieczeństwo publiczne, życie i walkę elektroniczną skierowaną przeciwko infrastrukturze krytycznej. W pojęciu cyberterroryzmu, tak jak w cyberprzestępczości, przedrostek „cyber" odnosi się do popełnienia przestępstwa związanego z nowymi technologiami informacyjnymi lub wykorzystania cyberprzestrzeni do tradycyjnych działań (np. planowania, komunikacji, prowadzenia wywiadu, działań logistycznych i finansowych).

Omawiając cyberprzestępczość, nie można uciec od kontekstu, w którym ona występuje (rys. 1.).

Rysunek 1. Cyberprzestępczość w kontekście bezpieczeństwa informacji



Źródło: opracowanie własne.

Zwykle przyjęło się mówić, że cyberprzestępczość jest jednym z cyberzagrożeń, które obejmują nieuprawnione zachowania skierowane na uzyskanie dostępu, pozyskanie, manipulowanie lub utratę integralności, poufności i dostępności danych, aplikacji czy systemu komputerowego. W obszarze cyberzagrożeń znajdują się ponadto m.in.: cyberterroryzm, cyberszpiegostwo i wojna elektroniczna. Cyberzagrożenia rozpatrywane są w kontekście cyberbezpieczeństwa rozumianego jako bezpieczeństwo połączonych globalnie systemów informacyjnych (np. infrastruktura internetu), sieci telekomunikacyjnych, systemów kompu-

terowych i systemów sterowania przemysłowego. Naruszenie cyberbezpieczeństwa jest wykorzystywane do wielu działań przestępczych, które powodują znaczące straty materialne i niematerialne organizacji, firm i osób prywatnych. Nie można nie zauważać, że jest to istotny problem także w kontekście bezpieczeństwa wewnętrznego, a tym samym również bezpieczeństwa państwa.

W 2003 roku Dan Verton napisał, że w krajach wysoko rozwiniętych niezakłócone działanie cyberprzestrzeni jest podstawą nie tylko prawidłowego funkcjonowania gospodarki, ale także bezpieczeństwa kraju[23]. To stwierdzenie, dotyczące zarówno bezpieczeństwa zewnętrznego, jak i wewnętrznego, a wraz z rozwojem technologii teleinformatycznych jest jeszcze bardziej prawdziwe.

Terminowi „bezpieczeństwo" nadawanych jest wiele znaczeń. *Słownik języka polskiego* definiuje bezpieczeństwo jako stan niezagrożenia, spokoju, pewności[24].

Ocena stanu i poczucia bezpieczeństwa może być przeprowadzana z wykorzystaniem pentagonalnego modelu. Pentagonalny model bezpieczeństwa rozpatruje bezpieczeństwo danego podmiotu w pięciu sektorach, a w każdym sektorze wskazywany jest jeden konkretny czynnik, za pomocą którego określa się poziom oraz poczucie bezpieczeństwa. Są to sektory:

1) militarny – zagrożenie terroryzmem,
2) polityczny – zagrożenie przestępczością. Poziom bezpieczeństwa oceniany jest poprzez wzrost lub spadek liczby odnotowanych oficjalnie przestępstw, a poczucie bezpieczeństwa badane na podstawie badań opinii publicznej,
3) gospodarczy – problem bezrobocia,
4) ekologiczny – ocena środowiska naturalnego,
5) społeczny – ocena ubóstwa[25].

Według Janusza Stefanowicza etymologia słowa „bezpieczeństwo" uwydatnia pierwotność poczucia zagrożenia w stosunku do poczucia pewności swego zabezpieczenia[26]. Za Stanisławem Koziejem można powiedzieć, że zagrożenie to pośrednie lub bezpośrednie destrukcyjne oddziaływania na podmiot[27]. Zagrożenia można rozpatrywać ze względu na różne kryteria (rys. 2.).

Zagrożenie asymetryczne to każda forma zagrożenia, na które to zagrożenie struktury (państwowe, koalicyjne, sojusznicze) nie są przygotowane kulturowo, strukturalnie, intelektualnie ani też z punktu widzenia legislacyjnego, administra-

---

[23] D. Verton, *Black Ice: niewidzialna groźba cyberterroryzmu*, Warszawa 2004, s. 76.

[24] *Słownik języka polskiego*, PWN, Warszawa 1996.

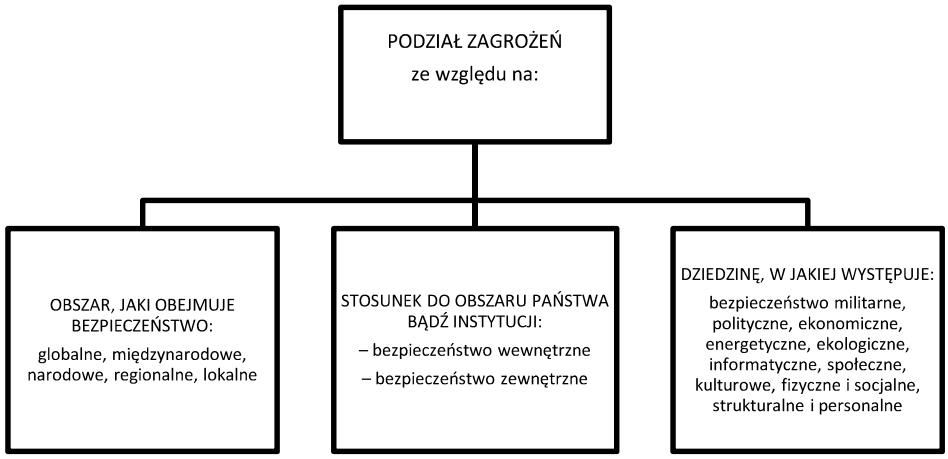
[25] S. Wojciechowski, *Stan i poczucie bezpieczeństwa w Polsce. Pentagonalny model bezpieczeństwa,* [w:] Wojciechowski S., Wejkszner A. (red.), *Kluczowe determinanty bezpieczeństwa Polski na początku XXI wieku*, Difin, Warszawa 2013, s. 13.

[26] J. Stefanowicz, *Współczesne pojmowanie bezpieczeństwa*, Warszawa 1996, s. 15.

[27] S. Koziej, *Strategiczne środowisko bezpieczeństwa międzynarodowego i narodowego w okresie pozimnowojennym*, Warszawa 2010, s. 4.

cyjnego lub regulaminowego, tak aby móc zareagować natychmiast, skutecznie i ostro[28]. W sensie przedmiotowym współczesne zagrożenia asymetryczne związane są z istnieniem terroryzmu międzynarodowego, niekontrolowanym rozprzestrzenianiem broni masowego rażenia i zorganizowaną przestępczością międzynarodową[29]. Wydaje się, że do tych trzech zagrożeń należy dodać zagrożenie związane z wykorzystaniem nowoczesnych technologii przetwarzania informacji. Warto zwrócić uwagę na zagrożenia dotyczące użycia przez podmioty niepaństwowe nowych technik informatycznych. Wśród najczęściej przywoływanych zjawisk w związku z tymi zagrożeniami wymieniane są: „walka informacyjna", „cyberterroryzm" czy „infoterroryzm". John Arquilla i David Ronfeldt zwrócili uwagę na dwa rodzaje konfliktów: „cyberwojnę" (*cyberwar*) i „wojnę sieciową" (*netwar*). Pierwszego z powyższych pojęć użyli w odniesieniu do konfliktów o wysokiej i średniej intensywności. Drugiego natomiast w odniesieniu do konfliktów o niskiej intensywności i operacji innych niż wojna[30].

Rysunek 2. Podział zagrożeń ze względu na wybrane kryteria



Źródło: R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka" nr 4/2010, s. 39.

[28] T. Szubrycht, *Analiza podobieństw operacji militarnych innych niż wojna oraz działań pozwalających zminimalizować zagrożenia asymetryczne*, Zeszyty Naukowe AMW, nr 1/2006, s. 145–146.

[29] A. Wejkszner, *Zagrożenia asymetryczne a bezpieczeństwo Polski*, [w:] Wojciechowski S., Wejkszner A. (red.), *Kluczowe determinanty bezpieczeństwa Polski na początku XXI wieku*, Difin, Warszawa 2013, s. 139.

[30] Za: A. Wejkszner, *Zagrożenia asymetryczne a bezpieczeństwo Polski*..., s. 149–150.

W każdym z tych terminów kluczowe znaczenie ma informacja. Carl von Clausewitz użył pojęcia „środek ciężkości" do wyróżnienia elementów, które w danym czasie nadają narodowi zasadniczą siłę. W swoich czasach dostrzegał sześć strategicznych elementów składających się na środek ciężkości i zaliczał do nich: armię, stolicę, sojusze, wspólnotę interesów, opinię publiczną, osobowość dowódców. Informacja stała się nowym środkiem ciężkości[31].

Szybki rozwój techniki obserwowany przez ostatnie lata, a w szczególności rozwój technik telekomunikacyjnych i lawinowa komputeryzacja niemal każdej dziedziny życia, sprawia, że obecnie najcenniejszym zasobem jest informacja. Jest ona kluczem do sukcesu zarówno w polityce i biznesie, jak i w planowaniu oraz prowadzeniu działań militarnych. Nie mniej istotne jest jednak to, że odpowiedni przepływ i dostępność informacji warunkują możliwość zapewnienia właściwego funkcjonowania gospodarki, administracji oraz wyspecjalizowanych służb każdego państwa[32].

Nie ma elementów narodowej siły wolnych od zależności od informacji. Wojsko, policja, system finansowy, gospodarka, system transportowy, energetyka, służba zdrowia, media są przykładami obszarów, w których zastosowanie informatyki spowodowało, że są one uzależnione od funkcjonowania systemów teleinformatycznych. Informację zawartą i przetwarzaną w tych systemach należy chronić jak każde dobro materialne. Informacja stała się przedmiotem walki, której narzędziami są wszelkie środki dostosowane do jej zdobywania, zakłócania i obrony. Walka informacyjna ukierunkowana jest na zdobywanie i wykorzystywanie zasobów informacyjnych – tajnych, poufnych i niedostępnych informacji. Prowadzona jest w celu zdobywania danych osobowych, ale również między konkurującymi firmami i korporacjami. Walka informacyjna prowadzona jest także w wymiarze państwowym i regionalnym[33].

Wojnę informacyjną można rozpatrywać poprzez analizę jej głównych elementów: zasobów informacyjnych, walczących podmiotów, operacji ofensywnych i defensywnych[34]. Jedną z dziedzin wojny informacyjnej jest przestępczość[35], którą zwykle się wykorzystuje, wraz z wywiadem z otwartych źródeł (OSINT – *Open Source Intelligence*) i wywiadem konkurencyjnym (*competitive intelligence*), do działań ofensywnych. Zwalczanie cyberprzestępczości jest jednym z ważniejszych zadań rządu w obszarze działań defensywnych.

---

[31] Za: L. Ciborowski, *Walka informacyjna*, Toruń 2001, s. 7. W skali mikro można powiedzieć za Sapkowskim, że „informacja nosi metkę z ceną", A. Sapkowski, *Sezon burz. Wiedźmin*, Warszawa 2013.

[32] *Biała Księga Bezpieczeństwa Narodowego*, BBN, Warszawa 2013, s. 63.

[33] Za: L. Ciborowski, *Walka informacyjna*, Toruń 2001, s. 9.

[34] Szerzej na ten temat można znaleźć w: D.E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*, Warszawa 2002, rozdz. 2. *Teoria wojny informacyjnej*, s. 23–48.

[35] Ibidem, s. 59.

Na początku roku 2013 sensacją była publikacja raportu firmy Mandiant na temat chińskich ataków APT[36] (*Advanced Persistent Threats*). Firma Mandiant, zajmująca się analizą ruchu internetowego i cyberbezpieczeństwem, w raporcie opisała włamania obywateli i firm z Chińskiej Republiki Ludowej do baz danych organizacji działających głównie w USA, Kanadzie i Wielkiej Brytanii oraz wykradzenie z nich setek terabajtów danych. W raporcie opisano systematyczne kradzieże danych z co najmniej 141 firm skupionych w branżach uważanych przez Chińczyków za strategiczne – zbrojeniowej, energetycznej i medialnej. Trudno nazwać opisane w raporcie działania chińskie inaczej jak „ofensywna wojna informacyjna".

Specyfiką zagrożeń pojawiających się wraz z wykorzystaniem technologii teleinformatycznych jest brak fizycznego kontaktu z przestępcą. Brak wyraźnie zdefiniowanego przeciwnika rozmywa ostrość i realizm dostrzegania zagrożeń, a tym samym potrzebę tworzenia i utrzymywania stosownego systemu bezpieczeństwa. Brak w tym zakresie ogólnospołecznego zrozumienia jest również objawem zagrożenia. Utrudnia bowiem podejmowanie racjonalnych wysiłków prowadzących do kształtowania przestrzeni bezpieczeństwa wielowymiarowo, jednocześnie i spójnie merytorycznie[37].

Warto pamiętać, że z technicznego punktu widzenia zbudowanie absolutnie bezpiecznego systemu teleinformatycznego jest praktycznie niemożliwe. Źródłem zagrożenia systemu teleinformatycznego może być technika albo ludzie. Zagrożenia, których źródłem jest technika, np. awaria dysku twardego komputera, są przewidywane i odpowiednio neutralizowane (np. poprzez zdublowanie krytycznych elementów systemu) lub stosownie do analizy ryzyka zapewniany jest zaplanowany poziom bezpieczeństwa (np. poprzez realizację sekwencyjnych kopii bezpieczeństwa). Znacznie trudniej przewidzieć zagrożenia, których źródłem są ludzie. Przykładowe zagrożenia przedstawiono w tabeli 1.

Z tabeli 1. można odczytać, że atakującym może być osoba z zewnątrz naruszająca bezpieczeństwo albo osoba z wewnątrz organizacji, której zachowanie powoduje zagrożenia. Mimo że medialnie znacznie częściej nagłaśniane są ataki z zewnątrz, to badania i analizy wskazują, że niebezpieczniejsi i powodujący więcej strat są atakujący z wewnątrz (obecni lub byli pracownicy, kontrahenci lub inni partnerzy biznesowi)[38]. Ich dostęp do sieci biznesowych i serwerów wykorzysty-

[36] APT1. Exposing One of China's Cyber Espionage Units. Mandiant 2013. http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf, dostęp: 15.04.2013.

[37] L. Ciborowski, *Walka informacyjna*, Toruń 2001, s. 178–179.

[38] Increase in Insider Threat Cases Highlight Significant Risks to Business Networks and Proprietary Information, http://www.ic3.gov/media/2014/140923.aspx, Survey: More Attacks Coming From Outsiders, Insider Attacks More Costly, http://www.securityweek.com/survey-more-attacks-coming-outsiders-insider-attacks-more-costly, dostęp: 25.09.2014 oraz D.M. Lynch, *Securing Against Insider Attacks*, „Information Security And Risk Management", 11/2006.

wany jest do niszczenia danych, kradzieży oprogramowania, uzyskiwania informacji o klientach, aby uzyskać przewagę konkurencyjną w nowej firmie, pozyskiwania towarów i usług dzięki nieautoryzowanemu użyciu kont klientów, a także do wyłudzania pieniędzy od swojego pracodawcy poprzez modyfikowanie i ograniczanie dostępu do firmowych stron internetowych, wyłączanie funkcji systemu zarządzania treścią oraz blokowanie funkcjonowania usług.

Tabela 1. Przykładowe motywacje osób stwarzających zagrożenie w cyberprzestrzeni

Atakujący	Zamierzenie
Uczeń	Testowanie możliwości (zamiast czytania instrukcji obsługi)
Student	Odczytywanie cudzych listów dla zabawy
Kraker	Przełamanie zabezpieczeń systemu komputerowego dziekanatu
Haker	Testowanie bezpieczeństwa obcych systemów
Przedstawiciel handlowy	Chęć poprawy własnego wizerunku i prestiżu
Biznesmen	Poznanie strategicznych tajemnic konkurentów
Pracownik	Nieświadome zawirusowanie komputera firmowego
Były pracownik	Zemsta za zwolnienie z pracy
Księgowy	Defraudacja pieniędzy firmowych
Makler giełdowy	Wycofanie się z obietnicy złożonej klientowi drogą elektroniczną
Oszust	Przechwycenie numerów kart kredytowych, fikcyjna sprzedaż
Szpieg	Zapoznanie się z wojskowymi i przemysłowymi tajemnicami
Terrorysta	Dokonanie zniszczeń, które zastraszą zaatakowanego
Pedofil	Podszywanie się pod dziecko przy korzystaniu z komunikatora

Źródło: opracowanie własne na podstawie: R. Tadeusiewicz, *Zagrożenia w cyberprzestrzeni*, „Nauka" nr 4/2010, s. 39.

O bezpieczeństwie w cyberprzestrzeni niewiele mówi Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 roku. Strategia wskazuje jedynie na nowe zagrożenia, które mogą wynikać z postępującej informatyzacji kluczowych obszarów funkcjonowania państwa.

W Strategii Bezpieczeństwa Narodowego RP w rozdziale *Bezpieczeństwo informacyjne i telekomunikacyjne* zapisane jest, że:

„78. Należy skutecznie zapobiegać próbom destrukcyjnego oddziaływania na infrastrukturę telekomunikacyjną państwa poprzez redukowanie jej podatności na to oddziaływanie, minimalizowanie skutków ewentualnych ataków oraz przywrócenie w krótkim czasie stanu pełnej jej funkcjonalności.

79. Należy tworzyć i rozwijać długofalowe plany ochrony kluczowych systemów teleinformatycznych przed uzyskiwaniem dostępu do danych przez podmioty do tego niepowołane, zakłócaniem normalnego ich funkcjonowania, kradzieżą tożsamości i sabotażem. Trzeba stale oceniać możliwości wtargnięcia do

systemów teleinformatycznych, przygotować możliwe formy odpowiedzi na ataki oraz rozwijać metody ewaluacji poniesionych strat informacyjnych (…).

80. Zwalczanie zagrożeń rządowych systemów teleinformatycznych i sieci telekomunikacyjnych ma na celu przeciwdziałanie przestępczości komputerowej oraz innym wrogim działaniom wymierzonym w infrastrukturę telekomunikacyjną, w tym zapobieganie atakom na elementy tej infrastruktury. Szczególne znaczenie ma ochrona informacji niejawnych przechowywanych lub przekazywanych w postaci elektronicznej. Ważnym zadaniem jest opracowanie i wdrożenie przejrzystych zasad dostępu uprawnionych organów państwa do treści przesyłanych drogą elektroniczną. Wymaga to ciągłego dostosowywania przepisów prawa telekomunikacyjnego, by – mimo szybkiego postępu technologicznego – stale odpowiadały współczesnym realiom, uwzględniając bezpieczeństwo Polski"[39].

W dokumencie uszczegóławiającym tę strategię – Strategia obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej – z 2009 roku przedrostek „cyber" pojawia się tylko raz – w słowie „cyberterroryzm".

Podobnie jest w ekspertyzie Bezpieczeństwo Wewnętrzne Państwa z 2010 roku przygotowanej na zlecenie Ministerstwa Rozwoju Regionalnego. Również w tej ekspertyzie słowo z przedrostkiem „cyber" autorzy umieścili tylko raz, w kontekście wyzwań w sferze bezpieczeństwa wewnętrznego, postulując „że należy wśród nich umieścić: protesty społeczne, terroryzm, problem bezpieczeństwa informacyjnego ze szczególnym uwzględnieniem cyberprzestrzeni…"[40].

W opracowaniu Biura Bezpieczeństwa Narodowego pt. *Strategiczny Przegląd Bezpieczeństwa Narodowego. Główne wnioski i rekomendacje dla Polski* z 2012 roku przedrostek „cyber" pojawia się dwa razy – w diagnozie zwrócono uwagę, że cyberterroryzm stanowi wyzwanie dla potencjału ochronnego oraz w ocenie i prognozie, w której zauważono, że zagrożenia terrorystyczne przeniosą się do cyberprzestrzeni[41].

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022[42] przyjęta uchwałą Rady Ministrów w 2013 r. sytuuje zagrożenia występujące w cyberprzestrzeni wśród najgroźniejszych zagrożeń asymetrycznych wraz z terroryzmem, proliferacją broni masowego rażenia i środków jej przenoszenia, międzynarodową przestępczością zorganizowaną. W strategii ocenia się, że negatywne oddziaływania w cyberprzestrzeni mogą wynikać z celowe-

[39] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2007, s. 20.

[40] W. Fehler, I.T. Dziubek, *Bezpieczeństwo Wewnętrzne Państwa*, Warszawa 2010, s. 7.

[41] *Strategiczny Przegląd Bezpieczeństwa Narodowego. Główne wnioski i rekomendacje dla Polski*, Warszawa 2012, s. 4 i 6.

[42] http://mon.gov.pl/z/pliki/dokumenty/rozne/2013/09/SRSBN_RP_przyjeta090413.pdf. dostęp: 13.11.2013.

go lub nieumyślnego działania człowieka bądź wywołanych awarią albo nieszczęśliwym wypadkiem zakłóceń funkcjonowania infrastruktury teleinformatycznej. Wśród priorytetów strategii wymienione są: pogłębianie współpracy na rzecz bezpieczeństwa cybernetycznego na forum NATO i UE (priorytet 1.1.5.), podwyższenie stopnia zabezpieczeń zasobów teleinformatycznych administracji publicznej i państwowej, w tym przed zagrożeniami sieci Internet oraz cyberterroryzmem (priorytet 5.3.1.), i rozwijanie Systemu Reagowania na Incydenty Komputerowe (priorytet 5.3.2.). Za główne działania zmierzające do realizacji priorytetu 1.1.5. uznano:

- „wspieranie inicjatyw na rzecz wzmocnienia roli i zdolności NATO i UE w zakresie polityki bezpieczeństwa cybernetycznego oraz wyposażenie obu organizacji w instrumenty udzielania pomocy państwom członkowskim (w szczególności średnim i małym) narażonym na ataki cybernetyczne,
- wspieranie działań na rzecz uwzględnienia obrony cybernetycznej w bieżących pracach planistycznych NATO,
- wzmocnienie współpracy pomiędzy NATO i UE w obszarze bezpieczeństwa cybernetycznego, w tym w szczególności w zakresie ochrony infrastruktury krytycznej sektorów cywilnych (łączność, energetyka, transport, finanse),
- aktywny udział Polski w budowie i funkcjonowaniu unijnych i sojuszniczych elementów struktur obrony cybernetycznej,
- udoskonalenie zasad i mechanizmów współpracy wewnątrz- i międzyresortowej, w tym pomiędzy ABW i MON,
- uwzględnienie w Polityce bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej nowych elementów wynikających z prac NATO i UE nad polityką bezpieczeństwa cybernetycznego”[43].

W przypadku priorytetu 5.3.1. uznano, że główne działania powinny dotyczyć:

- „przyjęcia Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej,
- umocnienia mechanizmów koordynacji i współdziałania na poziomie państwa poprzez działania Komitetu Rady Ministrów ds. Cyfryzacji,
- zwiększenia zasięgu działania systemu ARAKIS.GOV poprzez objęcie wszystkich urzędów i instytucji państwowych systemem,
- prowadzenie prac naukowych w obszarze reagowania na incydenty komputerowe w zakresie Systemu Zarządzania Bezpieczeństwem Informacji”.

Dla priorytetu 5.3.2. głównymi zadaniami są:

- „dalsze rozszerzanie współpracy z innymi zespołami narodowymi i organizacjami konsolidującymi międzynarodowe struktury CERT, w tym nowo powstałym zespołem CERT.UE,

[43] Ibidem, s. 43.

- ustanowienie Krajowego Systemu Reagowania na Incydenty Komputerowe pozwalającego na podjęcie szybkiej reakcji na zagrożenia z sieci Internet,
- posiadanie przez Agencję Bezpieczeństwa Wewnętrznego oraz resort obrony narodowej silnych, wyposażonych w zaawansowane technologie zespołów reagowania (w tym zespołów szybkiego reagowania – Rapid Reaction Team) usprawni realizowanie współpracy międzynarodowej oraz pozwoli osiągnąć nowe zdolności operacyjne w zakresie zadań reagowania na incydenty bezpieczeństwa teleinformatycznego oraz dowodzenia i kierowania w cyberprzestrzeni"[44].

Wprawdzie w diagnozie jest zapisane, że „na szczególną uwagę w aspekcie funkcjonowania służb specjalnych zasługuje również zagrożenie cyberatakami, w których wyniku może dojść do uzyskania dostępu do przechowywanych w formie elektronicznej informacji niejawnych przez nieuprawnione podmioty, w tym obce służby specjalne lub ugrupowania terrorystyczne i przestępcze, a także groźba dezorganizacji najważniejszych systemów informacyjnych instytucji rządowych i publicznych oraz sfer sektora prywatnego o istotnym znaczeniu gospodarczym"[45], to zarówno język, jak i wymienione w strategii zadania kładą nacisk na militarne cyberzagrożenia bezpieczeństwa narodowego oraz zagrożenia systemów teleinformatycznych administracji, marginalnie traktując cyberprzestępczość o charakterze kryminalnym.

5 listopada 2014 roku prezydent Bronisław Komorowski zatwierdził Strategię Bezpieczeństwa Narodowego RP zastępującą Strategię z 2007 r. Jednym z celów strategicznych w dziedzinie bezpieczeństwa wyznaczono zapewnienie bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni[46]. Sam przedrostek „cyber" występuje w tym dokumencie 37 razy. W wymiarze globalnym zauważono, że „wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak: cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw"[47]. Jednocześnie zwrócono uwagę na to, że w wymiarze regionalnym znaczenie bezpieczeństwa w cyberprze-

[44] Ibidem, s. 86–87.
[45] Ibidem, s. 24 i 34.
[46] Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2014, s. 12.
[47] Ibidem, s. 19.

strzeni będzie rosło podobnie jak odpowiedzialność państw za jej ochronę i obronę, a w wymiarze krajowym bezpieczne funkcjonowanie systemu teleinformatycznego RP jest warunkiem niezakłóconego działania całego państwa. Wyzwaniem pozostaje zapewnienie dostępności, integralności i poufności danych przetwarzanych w systemach teleinformatycznych administracji publicznej oraz brak jednolitych zabezpieczeń teleinformatycznych. Istotne znaczenie z punktu widzenia bezpieczeństwa ma niewystarczająca wiedza użytkowników o zagrożeniach w cyberprzestrzeni oraz konieczność rozwiązania dylematu pomiędzy wolnością osobistą i ochroną praw jednostki a stosowaniem środków służących zachowaniu bezpieczeństwa państwa. Za szczególnie ważne uznano:

- współpracę i koordynację działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej,
- prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni,
- wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie,
- rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców,
- prowadzenie walki informacyjnej w cyberprzestrzeni,
- współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych[48].

Uznano, że rozwijane muszą być podsystemy ochronne, w tym instytucje właściwe do spraw cyberbezpieczeństwa. Do najważniejszych zadań przygotowawczych w obszarze cyberbezpieczeństwa należy wdrożenie i rozwijanie systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym. Konieczne jest określenie zasad prowadzenia aktywnej obrony oraz budowa narodowego systemu obrony cybernetycznej, w tym rozwijanie Krajowego Systemu Reagowania na Incydenty Komputerowe w Cyberprzestrzeni RP, kompatybilnego z systemami państw sojuszniczych[49].

Zwrócono także uwagę, że istotne jest również zwiększanie świadomości użytkowników o zagrożeniach w cyberprzestrzeni poprzez intensyfikację działań edukacyjnych na wszystkich poziomach nauczania, a także w formie szkoleń i kampanii społecznych[50].

---

[48] Ibidem, s. 35.
[49] Ibidem, s. 49.
[50] Ibidem, s. 49.

Cechą charakterystyczną podejścia do cyberbezpieczeństwa i cyberzagrożeń przedstawionego w strategii jest podejście militarne kładące nacisk na cyberwojnę, a nie na cyberprzestępczość.

Rada Bezpieczeństwa Narodowego przyjęła główne założenia zmierzające do przygotowania projektu doktryny cyberbezpieczeństwa, która będzie sektorowym dokumentem wykonawczym do Strategii Bezpieczeństwa Narodowego RP. Stworzy ona warunki do zespolenia wysiłków i nakreśli strategiczne kierunki i ramy budowania zintegrowanego, spójnego systemu cyberbezpieczeństwa Rzeczypospolitej Polskiej[51].

O tym, jak istotnym zjawiskiem jest cyberprzestępczość, świadczą wyniki badań prowadzonych przez różne organizacje. Jednymi z ciekawszych i prowadzonych przez dłuższy czas były badania cyberprzestępczości wykonane przez Computer Security Institute (CSI) i Computer Intrusion Squad FBI z San Francisco. W ostatnim, sporządzonym w 2011 roku raporcie[52] stwierdzono, że bezpieczeństwo informacji stopniowo się poprawia. Coraz mniej ataków jest zauważanych przez respondentów. Niestety, rośnie liczba wysoce wyrafinowanych ataków. Są one bardziej złośliwe i jeżeli się powiodą, to powodują większe straty. Sprzyjają temu zmiany infrastruktury internetu. Wirtualizacja zaciera granice między serwerami i tworzy topologię sieci często bez wyraźnych granic, na których tradycyjnie mogły czuwać zapory (*firewalle*). Cloud computing zaciera lokalizację danych i procesów. Następuje ogromna ekspansja urządzeń, które mają adresy IP, mogą być widoczne w internecie i wykorzystane do cyberprzestępstw.

Rada Unii Europejskiej w konkluzjach z 2013 roku w sprawie ustalania priorytetów UE w zakresie walki z poważną i zorganizowaną przestępczością między 2014 a 2017 rokiem[53] jednym z priorytetów uczyniła zwalczanie cyberprzestępstw popełnianych przez zorganizowane grupy przestępcze, generujących duże profity, takich jak oszustwa online i z wykorzystaniem kart płatniczych, cyberprzestępstw, które powodują poważne szkody ich ofiarom, np. wykorzystywanie seksualne dzieci online oraz cyberataków, które wpływają na infrastrukturę krytyczną i systemy informacyjne w UE. A pamiętać należy, że już wcześniej została przyjęta Strategia bezpieczeństwa cybernetycznego Unii Europejskiej[54], w której

---

[51] Wystąpienie szefa BBN ministra Stanisława Kozieja na międzynarodowej konferencji nt. *Zagrożenia w cyberprzestrzeni – bezpieczeństwo ponad granicami* w dniu 6 listopada 2014 r.

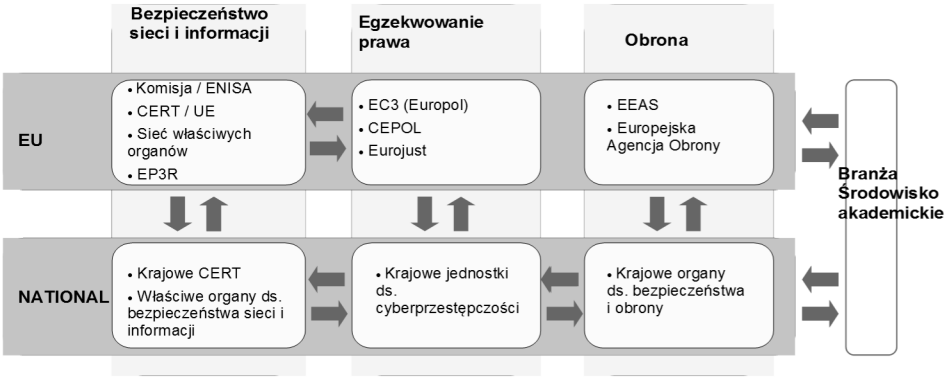
[52] http://www.ncxgroup.com/wp-content/uploads/2012/02/CSIsurvey2010.pdf, dostęp: 12.05.2012.

[53] Council conclusions on setting the EU's priorities for the fight against serious and organised crime between 2014 and 2017. Doc 137401/13. http://www.consilium.europa.eu/uedocs/cms_Data/docs/pressdata/en/jha/137401.pdf, dostęp: 12.11.2013.

[54] Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów z dnia 7 lutego 2013 r. pt. „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń", doc. JOIN (2013)1.

jest mowa o konieczności zwiększenia zdolności operacyjnej w celu zwalczania cyberprzestępczości i zwiększenia odporności infrastruktury informatycznej. Według tego samego dokumentu rozwiązanie problemu cyberbezpieczeństwa w kompleksowy sposób powinno obejmować trzy filary – bezpieczeństwo sieci i informacji, egzekwowanie przepisów i obronę – które również funkcjonują na podstawie różnych ram prawnych (rys. 3.).

Rysunek 3. Trzy filary cyberbezpieczeństwa



Źródło: „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń".

Strategia zwraca także uwagę na fakt, że poważne incydenty lub cyberataki mogą mieć wpływ na rządy, przedsiębiorstwa i osoby fizyczne w UE. Tym samym znaczącą rolę w zapewnieniu wolnej i bezpiecznej cyberprzestrzeni muszą odgrywać administracje rządowe. Mają one wiele zadań: zapewnienie dostępu i otwartości, poszanowanie i ochronę praw podstawowych w internecie oraz utrzymanie niezawodności i interoperacyjności Internetu. Znaczne części cyberprzestrzeni są jednak w posiadaniu i użytkowaniu sektora prywatnego. Dlatego wszelkie inicjatywy w tej dziedzinie, jeśli mają prowadzić do sukcesów, muszą uwzględniać jego wiodącą rolę[55].

Badania przeprowadzone przez Symantec[56] na podstawie informacji uzyskanych od ponad 13 tys. dorosłych respondentów z 24 krajów, w tym z Polski, wskazują, że w okresie lipiec 2011 – czerwiec 2012 roku koszty bezpośrednie[57]

[55] Ibidem, s. 2.

[56] Norton Cybercrime Report 2012. http://www.norton.com/2012cybercrimereport, dostęp: 16.11.2013.

[57] Bezpośrednie koszty i straty finansowe określono na podstawie informacji pochodzących od ofiar cyberprzestępstw, biorąc pod uwagę koszty poniesione w wyniku takich incydentów, jak: oszustwa, kradzieże i koszty naprawy systemów.

związane z globalną cyberprzestępczością wymierzoną w konsumentów wyniosły na całym świecie 110 mld dolarów, a w Polsce – 4,8 mld zł (1,4 mld dol.). W każdej sekundzie ofiarą cyberprzestępstw pada 18 dorosłych osób. W skali globalnej oznacza to ponad półtora miliona ofiar dziennie. Bezpośrednio pokrzywdzeni tracą średnio 197 dolarów rocznie. W Polsce kwota ta wynosi aż 672 zł. To badanie wskazuje na rozwój „nowych" form cyberprzestępczości, ukierunkowanych na sieci społecznościowe i urządzenia mobilne. Według badania aż 39% użytkowników sieci społecznościowych było już ofiarami przestępstw w tych sieciach (w Polsce 42%). Tylko w ciągu ostatniego roku co piąta dorosła osoba na świecie korzystająca z internetu (21%) padła ofiarą przestępstwa w sieci społecznościowej lub mobilnej (w Polsce 16%).

Raport z badania uwypukla kilka niepokojących faktów na świecie i w Polsce:

- 15% użytkowników sieci społecznościowych podaje, że ktoś włamał się na ich profil i podszywał się pod nich (w Polsce 9%),
- co dziesiąty użytkownik sieci społecznościowej przyznaje, że stał się ofiarą oszustwa typu „scam" lub fałszywego łącza w sieci społecznościowej (w Polsce 8%),
- 75% użytkowników internetu ma świadomość, że cyberprzestępcy działają w sieciach społecznościowych, ale tylko 44% (40% w Polsce) używa rozwiązania chroniącego przed zagrożeniami w sieci społecznościowej,
- prawie jedna trzecia użytkowników mobilnych (31% na świecie, 34% w Polsce) otrzymała wiadomość tekstową od nieznanego nadawcy z propozycją kliknięcia podanego łącza lub wybrania nieznanego sobie numeru w celu odebrania „poczty głosowej".

Kolejna edycja badania przeprowadzonego przez Symantec w 2013 roku[58] potwierdziła wcześniejsze spostrzeżenia, jednocześnie zauważając 50% wzrost kosztów cyberprzestępstwa przypadający na jedną ofiarę (do kwoty 298 dol.). Jednocześnie niepokojąca jest skala cyberprzestępczości – 378 mln ofiar rocznie, czyli 12 ofiar cyberprzestępców w każdej sekundzie.

Zeznając przed Kongresem Stanów Zjednoczonych 20 marca 2009 roku szef ds. bezpieczeństwa AT&T Edward Amoroso oszacował, że roczny zysk cyberprzestępców przekracza 1 bilion (10^{12}) dol., czyli więcej niż przychód całej branży IT, a około 7% PKB Stanów Zjednoczonych[59]. Podana wartość jest prawdopodobnie przeszacowana, gdyż była podawana w kontekście starania się o pomoc finansową.

---

[58] Norton Cybercrime Report 2013. http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=norton-report-2013.

[59] National Research Council. Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy. Washington, DC: The National Academies Press, 2010, s. 8, http://www.nap.edu/download.php?record_id=12997, dostęp: 07.04.2013.

Z badania przeprowadzonego przez brytyjski Departament ds. Biznesu, Innowacji i Umiejętności przy współpracy z PwC wynika, że wartość kosztów ponoszonych przez brytyjskich przedsiębiorców w wyniku naruszenia cyberbezpieczeństwa sięga miliardów funtów rocznie i potroiła się w ciągu 2012 roku[60]. To samo badanie informuje, że w 87% małych firm i 93% dużych organizacji odnotowano przynajmniej jeden rodzaj naruszenia bezpieczeństwa w 2012 roku. Najgorsze naruszenia cyberbezpieczeństwa kosztowały małe firmy średnio 50 000 funtów, a duże przedsiębiorstwa (więcej niż 250 pracowników) około 650 000 funtów. Do tego należy doliczyć koszt związany z utrzymaniem cyberbezpieczeństwa w firmach – ok. 10% ich budżetu IT. Z powyższych powodów rząd brytyjski utworzył w 2013 roku specjalną platformę CISP[61], składającą się z funkcjonariuszy z Komendy Głównej Łączności Rządowej (GCHQ)[62], Narodowej Agencji Kryminalnej (NCA)[63], MI5, UK CERT oraz przedstawicieli biznesu (w pierwszej fazie z obszaru infrastruktury krytycznej – obrony, energii, finansów, farmaceutyków i telekomunikacji), do ochrony firm przed rosnącym zagrożeniem atakami cybernetycznymi pochodzącymi z Chin, Rosji i Iranu.

Chociaż większość cyberataków była spowodowana przez outsiderów, takich jak przestępcy, hakerzy i konkurenci, to we wspomnianym raporcie zwrócono uwagę na zagrożenia pochodzące od wewnątrz. 36% najgorszych naruszeń bezpieczeństwa było spowodowanych przypadkowymi ludzkimi zachowaniami, a kolejne 10% zostało spowodowane celowym nadużyciem systemów przez pracowników.

Szef Interpolu Khoo Boon Hui na 41. Regionalnej Europejskiej Konferencji Interpolu zacytował[64] opracowanie London Metropolitan University informujące, że „80% przestępstw popełnianych w internecie jest powiązanych z międzynarodowymi gangami". Stwierdził również, że „zyski z cyberprzestępczości są większe niż łączne zyski z handlu kokainą, marihuaną i heroiną. W Europie koszt cyberprzestępczości osiągnął 750 mld euro rocznie. W 2011 roku straty amerykańskich banków z powodu przestępstw tradycyjnych wyniosły 900 mln dol., natomiast z powodu cyberprzestępczości 12 mld dol.". Być może nie jest to odkrywcze stwierdzenie, gdyż już w 2005 roku Valerie McNevin, doradca amerykańskiego Departamentu Skarbu ds. cyberprzestępczości, szacowała, że światowe dochody z e-przestępczości w 2004 roku przekroczyły 105 mld dol. i przewyższyły wpły-

[60] http://www.ft.com/intl/cms/s/0/bb3fcc90-ab4a-11e2-ac71-00144feabdc0.html#axzz2ROfLvggZ, dostęp: 17.07.2013.

[61] Cyber Security Information Sharing Partnership, https://www.gov.uk/government/news/government-launches-information-sharing-partnership-on-cyber-security, dostęp: 17.07.2013.

[62] Government Communications Headquarters.

[63] National Crime Agency.

[64] http://www.interpol.int/content/download/14086/99246/version/1/file/41ER-Khoo-Opening-Speech.pdf, dostęp: 19.10.2013.

wy z handlu narkotykami[65], lecz za to dobrze udokumentowane. Federalne Biuro Śledcze (FBI) w 2012 r. odnotowało spadek „przestępstw fizycznych", takich jak napady na banki, w przeciwieństwie do cyberprzestępczości, która wzrosła w zastraszającym tempie[66].

Gen. Keith Alexander, dyrektor Agencji Bezpieczeństwa Narodowego USA nadzorujący US Cyber Command, w lipcu 2012 roku ostrzegł, że cyberataki są przyczyną „największego transferu bogactwa w historii"[67]. Raport UNODC z 2010 roku podaje, że roczne dochody przestępców z kradzieży tożsamości (najbardziej dochodowe cyberprzestępstwo) wyniosły 1 mld dol., a z pornografii dziecięcej 250 mln dol.[68]. Badania McAfee z 2012 roku szacują, że globalny koszt cyberprzestępczości wynosi 1 bln dol.[69]. Oczywiście do wszelkich badań, a w szczególności zjawisk trudno mierzalnych, jak koszt cyberprzestępczości, należy podchodzić z rezerwą[70], ale nawet wartość o 50% mniejsza jest wartością olbrzymią. W raporcie z 2014 roku analitycy McAfee twierdzą, że internet rocznie generuje między 2 a 3 bln dol. przychodu w gospodarce światowej (ze stałą tendencją wzrostową), ale cyberprzestępczość pochłania między 15% a 20% tej wartości[71].

Coraz częściej cyberprzestępczość można traktować jako specyficzny rodzaj usługi świadczonej przez przestępców. W uproszczeniu wyróżniamy cztery kategorie usług świadczonych przez podziemie internetowe:

– badania (*Research-as-a-Service*) – istnieją grupy, które zapewniają sprzedaż podatności, która pojawia się na czarnym rynku przed publikacją poprawki naprawiającej tę podatność przez producenta (*zero-day vulnerabili-*

---

[65] http://news.techworld.com/security/4881/cybercrime-more-profitable-than-drugs, dostęp: 19.10.2013. To stwierdzenie było wielokrotnie podważane, np. http://www.informationweek.com/experts-debate-whether-cybercrime-profits-surpass-drug-trafficking/d/d-id/1038656?, dostęp: 19.10.2013.

[66] http://www.wmbfnews.com/story/20972727/robberies-decrease-as-cyber-crime-increases-fbi-says, dostęp: 20.10.2013.

[67] http://www.ibtimes.com/americas-top-cyberwarrior-says-cyberattacks-cost-250-billion-year--722559, dostęp: 03.03.2012.

[68] Raport TOCTA 2010, UNODC, s. 205, 211, https://www.unodc.org/documents/data-and-analysis/tocta/10.Cybercrime.pdf, dostęp: 04.03.2013.

[69] http://truth-out.org/news/item/10700-does-cybercrime-really-cost-1-trillion, dostęp: 05.08.2012. Wartość ta jest często kwestionowana. W jaki sposób została otrzymana, można zobaczyć w raporcie The Economic Impact of Cybercrime and Cyber Espionage, McAfee 2013, http://www.mcafee.com/sg/resources/reports/rp-economic-impact-cybercrime.pdf, dostęp: 03.06.2013.

[70] Analizę metod szacowania kosztów cyberprzestępczości można znaleźć w D. Florencio, C. Herley, Sex, Lies and Cyber-crime Surveys, MSR-TR-2011-75, June 2011, http://research.microsoft.com/pubs/149886/sexliesandcybercrimesurveys.pdf, dostęp: 03.06.2013.

[71] Net Losses: Estimating the Global Cost of Cybercrime Economic impact of cybercrime II, McAfee 2014. http://csis.org/files/attachments/140609_rp_economic_impact_cybercrime_report.pdf, dostęp: 13.09.2014.

ties). Istnieją także ludzie, którzy działają jako pośrednicy sprzedający tę specyficzną własność intelektualną. W przeciwieństwie do innych kategorii badania jako usługa nie muszą pochodzić z nielegalnych źródeł;

- tworzenie narzędzi do popełniania przestępstw (*Crimeware-as-a-Service*) – w tej kategorii zawiera się usługa tworzenia i rozwoju programów mających na celu wykorzystanie błędów w programowaniu używanych następnie do konkretnych działań przestępczych. Kategoria ta może obejmować również opracowanie programów pomocniczych do wsparcia ataku (np. downloadery, keyloggery, boty i inne), narzędzia służące do ukrywania złośliwego oprogramowania z mechanizmami zapewnienia bezpieczeństwa (szyfratory, obfuskatory, narzędzia do zmian polimorficznych itp.) i narzędzia spamerskie. Dodatkowo do kategorii można zaliczyć tworzenie sprzętu, który może być wykorzystywany do pozyskiwania danych (np. skimmerów do kart magnetycznych), lub urządzenia wykorzystywane do włamań (np. anteny, urządzenia podsłuchowe);
- infrastruktura cyberprzestępcza (*Cybercrime Infrastructure-as-a-Service*) – po opracowaniu zestawu narzędzi inni cyberprzestępcy wykorzystują je wobec zaplanowanych ofiar. Przykładem może być wynajęcie sieci komputerów do przeprowadzenie ataku. Innymi przykładami może być udostępnienie platformy internetowej do samodzielnego skonfigurowania narzędzi cyberprzestępczych lub utrzymywanie platformy pozwalającej na uzyskanie lub wymianę narzędzi niezbędnych do przestępstwa;
- cyberprzestępstwo (*Hacking-as-a-Service*) – usługa, która polega na całkowitym outsourcingu ataku. W tym wypadku zlecający usługę nie musi mieć żadnej wiedzy technicznej. Ta usługa może kosztować więcej niż nabycie poszczególnych narzędzi i samodzielne przeprowadzenie ataku. Kategoria ta obejmuje również dostarczenie informacji, która może być wykorzystana do kradzieży tożsamości, pozyskanie danych kart kredytowych oraz szczegółowych informacji nt. logowania do określonych stron internetowych[72].

Dodatkowy problem rodzi niedocenianie przez polityków, organy ścigania i wymiar sprawiedliwości rozmiarów zagrożeń przestępczością komputerową oraz jej związków z biznesem. Często nie bierze się pod uwagę kosztów społecznych cyberprzestępczości, lecz jedynie jej wymiar materialny. Rzeczywiste rozmiary cyberprzestępczości są trudne do określenia. Jest to w dużej mierze wynikiem faktu, że przestępstwa tego typu często ujawniane są przypadkowo, głównie z powodu błędów popełnianych przez sprawców. Statystyki policyjne przedsta-

[72] Porównaj z raportem Cybercrime Exposed. Cybercrime-as-a-Service, McAfee 2013, s. 3, http://www.mcafee.com/uk/resources/white-papers/wp-cybercrime-exposed.pdf, dostęp: 13.06.2014.

wiają zwykle tylko przestępstwa, które zostały stwierdzone. Wśród nich policje z dumą wskazują dużą liczbę przestępstw wykrytych, ale przy okazji zapominają dodać, że ok. 70% tych wykrytych przestępstw stanowią przestępstwa, w których sprawca był już znany w momencie stwierdzenia przestępstwa[73] (np. został wykryty przez pokrzywdzonego lub jego służby).

[73] Badania własne dotyczące oszustw komputerowych popełnionych w Polsce (A. Adamski, J. Kosiński, *Oszustwa internetowe w ocenie polskich i amerykańskich policjantów*, [w:] *Archiwum kryminologii. Tom XXVIII*, Warszawa 2007, s. 131–149), ale w innych krajach wyniki badań są podobne.