Wybrany fragment pracy laureata drugiej edycji konkursu szefa ABW
na najlepszą pracę licencjacką/magisterską
z dziedziny bezpieczeństwa wewnętrznego
2011/2012

Maciej Musiejko

Zjawisko cyberterroryzmu w polskim prawie karnym

Od najdawniejszych czasów rozwój techniczny wpływał na sposób życia człowieka. Obecnie, gdy nabrał on niespotykanego dotąd tempa, zmiany dokonują się niemal na naszych oczach. Postęp jest szczególnie dobrze widoczny w krajach, które wychodzą z technologicznego zapóźnienia. Jeszcze dwadzieścia lat temu komputer osobisty był urządzeniem nieosiągalnym dla większości polskiego społeczeństwa, a dostęp do internetu miały jedynie niektóre ośrodki naukowe. Obecnie komputer jest powszechnie stosowanym narzędziem pracy i rozrywki, a dostęp do szerokopasmowego internetu jest prawie tak naturalny, jak dostęp do bieżącej wody. Co więcej, z ogólnoświatowej sieci można korzystać już nie tylko siedząc przy biurku, ale też za pomocą komputerów przenośnych, a nawet telefonów komórkowych.

W ślad za postępem technicznym podąża nieustannie rozszerzające się spektrum możliwości wykorzystania istniejącej infrastruktury sieciowej. W swoich „młodzieńczych" latach internet był jedynie zbiorem statycznych stron www, w niektórych przypadkach zawierających niskiej jakości grafikę. Jego zawartość była skierowana bardziej do wąskiego grona odbiorców, niż do użytkowników masowych. Stopniowe upowszechnienie dostępu do sieci dało jednak impuls do zmian i przeistoczenia militarno-naukowego tworu (bo taki charakter miał z założenia ARPANET – protoplasta internetu) w globalną sieć wykorzystywaną do celów komercyjnych i rozrywkowych. Zaczęły powstawać sklepy internetowe (np. Amazon.com) umożliwiające dokonywanie zakupów bez zrobienia choćby kroku w stronę drzwi mieszkania. Pojawiła się możliwość nawiązywania kontaktów z ludźmi z całego świata za pośrednictwem czatów i forów dyskusyjnych. Zwykli użytkownicy dzięki temu mogą opowiedzieć o sobie lub o tym, co ich interesuje. W tym celu mogą również zaprojektować własne strony www. Papierowe wydania prasy codziennej, tygodników i innych gazet zaczęły być częściowo dostępne także w wersji elektronicznej. Banki zaoferowały swoim klientom dostęp do kont przy wykorzystaniu internetu, administracja publiczna zaś przedstawiła w tenże sposób informacje na temat swojej działalności.

Obecnie wykorzystanie internetu do celów komercyjnych poszło o krok dalej. Sklepy internetowe i serwisy aukcyjne pozwalają kupić wszystko, czego można zapragnąć – nawet produkty spożywcze. Istnieje możliwość zapłacenia rachunków (otrzymywanych e-mailem) przy korzystaniu z usług banku internetowego. Sam bank nie musi posiadać oddziałów, w których można wypłacić pieniądze, a konto można założyć on-line, wypełniając stosowny formularz. Wpływy na ów wirtualny rachunek zapewnia na przykład telepraca, w pełni dopuszczalna w świetle zapisów kodeksu pracy[1]. Zeznanie podatkowe można złożyć w postaci elektronicznej, do czego zresztą

[1] Rozdział IIb *Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy* (Dz.U. z 1998 r Nr 21, poz. 94 z późn. zm.).

zachęca samo Ministerstwo Finansów. Wdrażane są również inne programy oferujące załatwianie spraw urzędowych przez internet. Także wymiar sprawiedliwości korzysta z sieci, umożliwiając złożenie pozwu w tzw. e-Sądzie[2] działającym przy Sądzie Rejonowym Lublin-Zachód w Lublinie. Niektóre uczelnie uruchamiają tzw. studia e-learningowe, proponując kształcenie się przy użyciu komputera. Rozrywkę natomiast zapewniają między innymi możliwość oglądania telewizji przez internet czy dostępna w sieci ogromna liczba gier, w tym z opcją gry wieloosobowej. Nawiązywaniu i podtrzymywaniu kontaktów towarzyskich służą portale społecznościowe, takie jak np. Facebook, na którym konto posiada ponad pół miliarda osób. Komunikatory, m.in. Skype, pozwalają w czasie rzeczywistym widzieć i rozmawiać z osobą na innym kontynencie. Rozwój sieci internet sprawił, że człowiek XXI wieku nie musi już praktycznie wychodzić z domu.

Oczywiście globalna sieć komputerowa nie jest tworem idealnym, pozbawionym zagrożeń. W równie wysokim stopniu jak działalności legalnej, internet służy czynom zakazanym przez prawo – m.in. dystrybucji pornografii dziecięcej, sprzedaży niedostępnych w kraju środków farmakologicznych, szpiegostwu, hackingowi, oszustwom internetowym. Przestępczość w sieci nie ogranicza się tylko do dokonywania „tradycyjnych" czynów zabronionych przez prawo przy pomocy nowego narzędzia (np. oszustw na aukcjach internetowych), ale zdołała wykształcić nowe, mające wyłącznie wirtualny charakter, przestępstwa, jak choćby hackerstwo. Co więcej, przestrzeń wirtualna stała się polem rywalizacji międzynarodowej – światowe mocarstwa starają się rozszerzyć swoją strefę wpływów na cyberprzestrzeń i wykorzystywać ją do uzyskania przewagi nad swoimi rywalami. Coraz częstsze są akcje grup hackerów kierowane przeciwko stronom i serwerom państwowym. Oficjalnie sprawcy tych czynów są potępiani i piętnowani, nieoficjalnie zaś uzyskują wsparcie rodzimych agend rządowych. Niektórzy badacze i wojskowi wskazują nawet, że cyberprzestrzeń jest nowym rodzajem pola walki zbrojnej.

W takiej sytuacji nie powinna dziwić wzmożona aktywność państw i organizacji międzynarodowych w sferze szeroko rozumianego cyberbezpieczeństwa. W dziedzinie wojskowości na przykład normą staje się powoływanie do życia oddziałów wojskowych specjalizujących się w zabezpieczaniu działań armii oraz prowadzeniu walki w cyberprzestrzeni. Prym w tej kwestii wiodą Stany Zjednoczone, dysponujące takimi oddziałami w niemal każdym rodzaju sił zbrojnych oraz wspólnym dla nich dowództwem (USCYBERCOM[3]). Podobne inicjatywy podjęły już między innymi armia brytyjska, niemiecka, chińska, a także polska – ta ostatnia pod postacią Centrum Bezpieczeństwa Cybernetycznego w Białobrzegach. W strukturach polskich sił zbrojnych planowane jest utworzenie „batalionów cyfrowych", których zadaniem będzie zapewnienie bezpieczeństwa armii[4]. Oprócz tego typu inicjatyw podejmowane są również działania w ramach międzynarodowej współpracy militarnej. Pamiętając o wydarzeniach z przełomu kwietnia i maja 2007 r. w Estonii, powołano do życia Centrum Doskonalenia Obrony Cybernetycznej[5], które w październiku 2008 r. uzyskało akredytację NATO i stało się międzynarodową organizacją wojskową. Wagę problemu zauważył nie tylko

[2] www.e-sad.gov.pl [dostęp: 17 III 2012].

[3] Z ang. *United States Cyber Command*.

[4] „Tygodnik BBN" 14–20 stycznia 2011 r., nr 16, s. 6, www.bbn.gov.pl/portal/pl/561/2446/ tygodnik_ BBN.html [dostęp: 4 II 2011].

[5] Z ang. *Cooperative Cyber Defence Centre of Excellence* (CCD COE).

sektor wojskowy – coraz częściej jest ona dostrzegana przez najważniejsze organizacje międzynarodowe[6]. Zarówno ONZ, jak i Unia Europejska stworzyły ośrodki, które mają zajmować się bezpieczeństwem cyberprzestrzeni – odpowiednio Światową Agencję ds. Cyberbezpieczeństwa (GCA)[7] oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). Swoje strategie cyberbezpieczeństwa przygotowały już między innymi Stany Zjednoczone, Kanada, Francja, Niemcy, a nawet Estonia. W Polsce natomiast tworzony jest Rządowy Program Ochrony Cyberprzestrzeni (RPOC), którego realizacja ma zwiększyć zdolność zapobiegania niebezpieczeństwom płynącym ze strony cyberprzestrzeni oraz ich zwalczania. Wyraźnie więc widać, że zagrożenia, jakie mogą się wiązać z cyberprzestrzenią, zostały dostrzeżone i poważnie potraktowane przez społeczność międzynarodową.

Do największych zagrożeń XXI wieku można zaliczyć także terroryzm. Zamachy w Nowym Yorku, Madrycie i Londynie pokazały, że nikt nie może czuć się w pełni bezpiecznym. Nawet obywatele najbardziej rozwiniętych i najpotężniejszych światowych mocarstw muszą być przygotowani na akty przemocy skierowane przeciwko nim. Choć do tej pory przemoc ta przybierała formę zamachów bombowych, porwań i egzekucji niewinnych osób, to naiwnością byłoby wierzyć, że terroryści nie będą korzystać z nowych technologii. Rozwój i wzrost znaczenia cyberprzestrzeni otwiera przed nimi nowe możliwości – zarówno organizowania zamachów, jak i ich przeprowadzania. Cyberterroryzm jest więc połączeniem obu wymienionych powyżej zagrożeń.

Z uwagi na poruszone kwestie potrzebne wydaje się przeanalizowanie polskich regulacji prawnych odnoszących się do cyberterroryzmu. Przemawia za tym również fakt, iż w skład Rządowego Programu Ochrony Cyberprzestrzeni będzie wchodzić wiele działań legislacyjnych, które mają stanowić pierwszy etap w procesie zapewnienia bezpieczeństwa cyberprzestrzeni. Niniejsza praca stanowi próbę przeanalizowania tych regulacji w zakresie dotyczącym prawa karnego materialnego. Autor będzie starał się znaleźć odpowiedź na pytanie, czy polskie prawo karne odnosi się do zjawiska cyberterroryzmu, a jeśli tak, to w jaki sposób. Niezbędne będzie wyjaśnienie, czym jest cyberterroryzm. Ponadto celem publikacji jest wskazanie ewentualnych luk w prawie i wysunięcie postulatów *de lege ferenda*. Posłuży do tego analiza dogmatyczna treści aktów prawnych oraz krytyka i analiza literatury.

Istnieje stosunkowo niewiele opracowań na temat cyberterroryzmu w kontekście prawnym, toteż konieczne jest odwołanie się do literatury spoza dziedziny prawa, głównie dotyczącej bezpieczeństwa państwa, ale również do źródeł o charakterze technicznym czy odnoszących się do kwestii lingwistycznych. Z tego powodu część pracy traktuje o kwestiach pozaprawnych, co jest zabiegiem niezbędnym, by w sposób możliwie jak najbardziej kompleksowy oddać problematykę dotyczącą cyberterroryzmu. Mała liczba źródeł implikowała również badawczy charakter pracy, stąd znaczna część twierdzeń w niej zawartych stanowi pogląd autora.

---

[6] Szerzej: K. Liedel, *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej,* w: *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Warszawa 2011, Difin.

[7] *Global Cybersecurity Agenda* – wchodzi ona w skład Międzynarodowego Związku Telekomunikacyjnego.

Przepisy penalizujące ataki w cyberprzestrzeni

Poszukiwanie przepisów odnoszących się do cyberterroryzmu należy rozpocząć w rozdziale XXXIII kodeksu karnego, w którym wymienione są przestępstwa przeciwko ochronie informacji. W jego skład wchodzą zarówno przepisy chroniące informację w szerokim tego słowa rozumieniu, jak i bezpieczeństwo danych, systemów oraz sieci.

Artykuły 265 i 266 kk penalizują ujawnienie oraz wykorzystanie informacji niejawnych w sposób naruszający zapisy ustawy o ochronie informacji niejawnych[8]. Choć ze względu na górną granicę zagrożenia karnego przestępstwo z art. 265 kk można by w niektórych przypadkach uznać za przestępstwo o charakterze terrorystycznym[9], to jednak wziąwszy pod uwagę czynność sprawczą (ujawnienie lub wykorzystanie wbrew przepisom ustawy informacji niejawnych o klauzuli „tajne" lub „ściśle tajne") trudno jest uznać je za akt cyberterroryzmu. Artykuł 266 kk natomiast nie spełnia nawet wymogu zagrożenia karą pięciu lat pozbawienia wolności. W związku z tym dalsza analiza tych artykułów jest bezcelowa.

Kolejnym przepisem dotyczącym przedmiotowej tematyki jest artykuł 267 kk, który stanowi:

> „Art. 267 § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
>
> § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
>
> § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
>
> § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.
>
> § 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego".

Przepis ten chroni poufność informacji w szerokim zakresie – dotyczy informacji zapisanej zarówno w tradycyjny sposób (*otwierając zamknięte pismo*), przekazywanej na odległość (*podłączając się do sieci telekomunikacyjnej*) czy też zawartej na nośnikach nowoczesnego typu (*przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie*). W literaturze zwraca się uwagę na to, że przepis ten jest także środkiem mogącym służyć do walki z hackingiem[10].

---

[8] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r. Nr 182, poz. 1228).

[9] „Art. 115 § 20 Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:
1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej
– a także groźba popełnienia takiego czynu".

[10] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Warszawa 2010, Wolters Kluwer Business, s. 211.

W kontekście cyberterroryzmu szczególnie interesujący wydaje się § 2 tego przepisu. Został on wprowadzony ustawą[11], która miała za zadanie m.in. implementację *Decyzji ramowej Rady 2005/222/WSiSW* w sprawie ataków na systemy informatyczne i dostosowanie polskich przepisów do *Konwencji o cyberprzestępczości*. Prócz zmiany dość archaicznych zapisów art. 267 § 1 kk (we wcześniejszej wersji była mowa o podłączaniu się *do przewodu służącego do przekazywania informacji*), za przestępstwo zostało uznane samo uzyskanie dostępu do całości lub części systemu informatycznego. Jak wskazano w projekcie ustawy, *czyn taki może polegać np. na wprowadzeniu do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem, w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe. Sprawca w takim przypadku nie działa w celu uzyskania informacji znajdującej się w zasobach przejętego systemu lub dostępu do niej, lecz w celu przejęcia kontroli nad systemem jako narzędziem do bezprawnego wykorzystywania*[12]. Mowa zatem o tworzeniu Botnetu[13], który mógłby służyć przeprowadzeniu ataku typu DDoS, a stąd już tylko krok do cyberataków. Niemniej jednak uzyskanie dostępu do informacji lub systemu nie spełnia kryteriów z art. 115 § 20, toteż nie może ono stanowić przestępstwa o charakterze terrorystycznym.

Konieczne wydaje się wyjaśnienie pojęcia „system informatyczny", które pojawiło się w art. 267 kk i występuje także w innych przepisach. Pomimo ujednolicenia terminologii informatycznej i wprowadzenia do ustaw terminu „system teleinformatyczny" ustawodawca posłużył się innym określeniem, nie zdefiniowanym ustawowo. Definicję „system informatyczny" można natomiast znaleźć w art. 1 *Konwencji o cyberprzestępczości*. Zgodnie z nią jest to *każde urządzenie lub grupa wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych*. Ta definicja zasadniczo zgadza się z definicją „systemu teleinformatycznego"[14], z tą różnicą, że nie obejmuje funkcji wysyłania i odbierania danych. Podobnego zdania jest A. Baworowski, który twierdzi, że pojęcie „system teleinformatyczny" jest szersze od pojęcia „system informatyczny", gdyż system teleinformatyczny oprócz przetwarzania i przechowywania danych będzie służył także do ich przesyłania i odbierania. Jak zauważa, *każdy system teleinformatyczny jest systemem informatycznym, lecz nie każdy system informatyczny jest systemem teleinformatycznym*[15].

---

[11] *Ustawa z dnia 24 października 2008 r. o zmianie ustawy Kodeks karny oraz niektórych innych ustaw* (Dz.U. z 2008 r. Nr 214, poz. 1344).

[12] *Uzasadnienie projektu ustawy z dnia 24 października 2008 r. o zmianie ustawy Kodeks karny oraz niektórych innych ustaw.*

[13] *Botnet – sieć zawirusowanych i przejętych komputerów, które raportują swojemu właścicielowi i są zarządzane w czasie rzeczywistym przez serwer kontrolujący. Botnety najczęściej są wykorzystywane do przeprowadzania zmasowanych ataków typu DDoS, rozsyłania spamu itp.* Źródło: http://www.orange.pl/kid,4002354750,id,4002365117,title,slownikB,article.html [dostęp: 12 V 2012].

[14] W rozumieniu przepisów *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* system teleinformatyczny jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą telekomunikacyjnego urządzenia końcowego właściwego dla danego rodzaju sieci.

[15] A. Baworowski, *Problemy wykładni przepisów art. 268 § 2, 269 § 2, 267 i 269a kk po nowelizacjach z 2008 r.,* „Diariusz Prawniczy" 2009, nr 10/11.

Następnym przepisem służącym ochronie informacji jest art. 268 kk:

„Art. 268 § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego".

Nie chodzi tu jednak o każdą informację, lecz o taką, która jest w pewien sposób istotna. Jak zauważa M. Kalitkowski, kwestia wagi informacji zależy od jej znaczenia dla jej dysponenta oraz celu, któremu służyła lub miała służyć[16]. Karalne jest zatem działanie, które udaremnia lub utrudnia zapoznanie się z zapisem istotnej informacji, w szczególności poprzez zniszczenie, uszkodzenie, usunięcie lub zmianę tego zapisu. Poprzez udaremnienie zapoznania się z informacją należy rozumieć *całkowite uniemożliwienie* (...) *zrozumienia sensu zapisu tej informacji*. O znacznym utrudnieniu można mówić natomiast wtedy, gdy do odczytania informacji jest niezbędny znaczny nakład czasu lub wysiłku, a także, gdy informacja jest niekompletna lub znacznie zniekształcona[17]. Typ kwalifikowany tego przestępstwa został zawarty w paragrafie drugim art. 268, który odnosi się do zapisu istotnej informacji na informatycznym nośniku danych. Zgodnie z ustawą o informatyzacji „informatyczny nośnik danych" to *materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej*. Jako przykładowe informatyczne nośniki danych można wskazać dyskietki, płyty CD, DVD, Blu-ray, dyski twarde, pamięci flash, taśmy oraz dyski magnetyczne. Udaremnienie lub utrudnienie zapoznania się z informacjami przechowywanymi na nośniku informatycznym może zostać dokonane w taki sam sposób, jak w przypadku informacji zawartych na nośniku nieinformatycznym (np. poprzez ich uszkodzenie lub choćby schowanie), ale również w sposób charakterystyczny tylko dla nich. W. Wróbel jako przykład podaje wprowadzenie do komputera programu blokującego możliwość zapoznania się z treścią poczty elektronicznej czy korzystania z bazy danych[18]. Także M. Kalitkowski zauważa możliwość wprowadzenia do systemu wirusa komputerowego w celu uniemożliwienia dostępu do informacji. W przypadku, gdy taki czyn wywoła znaczną szkodę majątkową[19], zagrożenie karne wzrasta do pięciu lat pozbawienia wolności, co wiąże się z możliwością uznania go za przestępstwo o charakterze terrorystycznym. Tym samym art. 268 kk może w odpowiednich okolicznościach (np. w przypadku utrudnienia lub uniemożliwienia zapoznania się z istotną informacją, gdy została ona zapisana na informatycznym nośniku danych lub w przypadku spowodowania znacznej szkody majątkowej) służyć karaniu aktów cyberterroryzmu.

---

[16] *Kodeks karny. Komentarz*, M. Filar (red.), Warszawa 2010, LexisNexis, s. 1146.

[17] *Kodeks karny. Część szczególna,* t. 2, A. Zoll (red.), Warszawa 2008, Wolters Kluwer Polska, s. 1300.

[18] Tamże, s. 1301.

[19] Zgodnie z art. 115 § 5 i § 7 o znacznej szkodzie majątkowej można mówić wtedy, gdy jej wartość przekroczy 200 000 złotych.

Jednym z przepisów dodanych w celu dostosowania regulacji kodeksu karnego do postanowień *Konwencji o cyberprzestępczości* jest art. 268a kk. Jak wskazuje B. Kunicka-Michalska, stanowi on o jednej z postaci sabotażu komputerowego. Przestępstwo to jest w jej opinii ujęte w kilku odrębnych przepisach kodeksu karnego, jego postaci zaś są opisane także w artykułach 269 kk oraz 269a kk[20].

W obecnym brzmieniu przepis ten stanowi, że:

„Art. 268a § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego".

Dobrem chronionym przez ten przepis są dane informatyczne, ale można tu zauważyć pewne podobieństwo do art. 268 kk. Podobnie jak zapis informacji, tak i dane są tu chronione przed zniszczeniem, uszkodzeniem, usunięciem lub zmianą, a także utrudnieniem dostępu do nich. W istocie informacje zapisane na informatycznym nośniku danych można utożsamiać z danymi informatycznymi, co zdaje się potwierdzać takie samo zagrożenie karne w art. 268 § 2 i 268a § 1 kk. Wobec braku definicji legalnej „danych informatycznych" wyjaśnienia tego terminu należy szukać u źródła jego powstania. Konwencja o cyberprzestępczości rozumie pod tym pojęciem *dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny.* Oprócz działań przeciwko danym informatycznym wspomnianych w pierwszej części przepisu, art. 268a kk przewiduje również karalność zakłóceń w istotnym stopniu lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania danych. Przetwarzaniem danych informatycznych według M. Dąbrowskiej-Kardas i P. Kardasa jest *opracowywanie za pomocą maszyn cyfrowych dużych ilości danych*[21]. Jak zauważa P. Kozłowska-Kalisz, o automatycznym charakterze przetwarzania można mówić wtedy, gdy odbywa się ono za pomocą urządzeń sterujących, bez niczyjej ingerencji, bądź z ograniczonym udziałem czynnika ludzkiego[22]. „Gromadzenie" to sposób koncentracji danych informatycznych, ich archiwizacja, umieszczanie w jednym pliku, „przekazywanie" zaś jest właściwie tożsame z „przesyłaniem", którym to terminem posługiwano się w poprzedniej wersji przepisu[23]. Opis działania sprawcy, w kontekście cech systemów informatycznych i teleinformatycznych, zdaje się sugerować, że karze podlegają także działania skierowane przeciwko systemom i sieciom. Artykuł 268a kk nie zawiera wskazania, w jaki sposób miałoby dojść do zakłócenia lub uniemożliwienia automatycznego przetwarzania danych. Stąd wniosek, że chodzi o jakiekolwiek działanie, np. uszkodzenie urządzeń, odcięcie

[20] *Kodeks karny. Część szczególna. Komentarz do artykułów 222–316,* A. Wąsek, R. Zawłocki (red.), Warszawa 2010, C.H. Beck, s. 720.

[21] *Kodeks karny. Część szczególna*, t. 3, A. Zoll (red.), Warszawa 2008, Wolters Kluwer Polska, s. 327.

[22] *Kodeks Karny. Praktyczny Komentarz,* M. Mozgawa (red.), Warszawa 2007, Wolters Kluwer Polska, s. 523.

[23] *Kodeks karny*, t. 3, A. Zoll (red.), s. 328.

dopływu prądu czy wprowadzenie wirusa komputerowego[24]. Ważne jest natomiast, aby skutkiem oddziaływania było uniemożliwienie automatycznego przetwarzania danych albo co najmniej zakłócenie go w istotnym stopniu. Zgodnie z definicją słownikową „istotny" oznacza tyle co „duży, znaczny"[25], zatem chodzi o zakłócenie poważne, na dużą skalę, niemal uniemożliwiające prawidłowe działanie. Tym samym karze nie podlega takie działanie sprawcy, które nie wywołuje zbyt dotkliwych skutków. Analogicznie do art. 268 kk, jeśli skutkiem czynu opisanego w paragrafie pierwszym będzie znaczna szkoda majątkowa, to sprawca podlega karze do pięciu lat pozbawienia wolności. Rozwiązanie takie czyni art. 268a kk kolejnym narzędziem z cyberterroryzmem.

Istotnym zagadnieniem jest problem relacji między przepisami zawartymi w artykułach 268 i 268a kk. W kwestii tej doktryna nie jest zgodna i proponuje różne rozwiązania. Z jednej strony art. 268 kk jest uznawany za *lex specialis* wobec art. 268a kk (tego zdania jest m.in. W. Wróbel) w sytuacji, gdy dane będą nośnikiem istotnej informacji. Inne stanowisko prezentuje B. Kunicka-Michalska sugerując, iż art. 268a kk jako *lex consumens* wyłączy stosowanie art. 268 kk. A. Suchorzewska natomiast wskazuje na pojawiające się w literaturze postulaty, aby usunąć art. 268 § 2 kk, gdyż zakres jego penalizacji został pochłonięty przez 268a kk[26].

W kontekście ochrony infrastruktury krytycznej, która jest najprawdopodobniejszym celem ataku cyberterrorystów, wyróżnia się kolejny przepis:

> „Art. 269 § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
>
> § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych".

Łatwo można dostrzec podobieństwa między tym przepisem a przepisem dotyczącym przestępstwa z artykułu 268a kk. W obu przypadkach przedmiotem ochrony są dane informatyczne, a znamiona określające czynność sprawczą są identycznie niemalże ujęte. Podobieństwo to może uzasadniać koncepcję B. Kunickiej-Michalskiej o „rozbiciu" przepisu odnoszącego się do przestępstwa sabotażu komputerowego na kilka przepisów. Niemniej jednak istnieją cechy w znaczący sposób odróżniające art. 269 kk od art. 268a kk. Przede wszystkim art. 269 kk chroni jedynie te dane, które cechują się szczególnym znaczeniem dla:

a) obronności kraju,
b) bezpieczeństwa w komunikacji,

---

[24] Przykłady za: *Kodeks karny*..., A. Wąsek, R. Zawłocki (red.), s. 1177.

[25] Zob. http://sjp.pwn.pl/szukaj/istotny [dostęp: 7 III 2012].

[26] D. Harbat, *Ochrona informacji w kodeksie karnym na tle postanowień „Konwencji o cyberprzestępczości"*, w: *Zmiany w polskim prawie karnym po wejściu w życie kodeksu karnego z 1997 roku*, T. Bojarski, K. Nazar, A. Nowosad (red.), Lublin 2006, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, s. 302.

c) funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego.

W pewnym stopniu wyliczenie to pokrywa się z definicją infrastruktury krytycznej z art. 3 pkt. 2 *Ustawy o zarządzaniu kryzysowym*, art. 269 kk nie chroni jednak wszystkich systemów w niej wymienionych. Choć może się wydawać, że takie dane znajdują się wyłącznie w posiadaniu państwa, to jednak należy zauważyć, że przestępstwo to może dotyczyć danych informatycznych znajdujących się w rękach prywatnych – np. danych zawartych w komputerze pokładowym samolotu pasażerskiego. Ustawodawca przewidział różne formy popełnienia przestępstwa:

a) niszczenie, uszkadzanie, usuwanie, zmienianie danych,
b) zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych,
c) niszczenie lub wymiana informatycznego nośnika danych,
d) niszczenie lub uszkadzanie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych.

Działania wymienione w punkcie „a" są analogiczne do tych wymienionych w art. 268a § 1 kk, z tą jednak różnicą, że brak wśród nich utrudniania dostępu do danych. Węższy zakres kryminalizacji w tym przypadku wydaje się być przeoczeniem ustawodawcy.

Kolejną różnicą jest objęcie karalnością zakłócania automatycznego przetwarzania, gromadzenia lub przekazywania danych, bez względu na to, jak istotne skutki ono wywoła. Stanowi to znaczne rozszerzenie kręgu działań podlegających karze. Paragraf drugi zakłada, że karze podlega sprawca, który popełnił czyn opisany w paragrafie pierwszym, poprzez wskazane działania skierowane przeciwko nośnikowi danych informatycznych lub urządzeniu służącemu do ich automatycznego przetwarzania, gromadzenia lub przekazywania. Nie budzi wątpliwości to, że fizyczne niszczenie i uszkadzanie nośników danych lub urządzeń wchodzi w zakres regulacji art. 269 § 2 kk. Niemniej jednak A. Baworowski zauważa, że również ingerencja w procesy inicjowane przez oprogramowanie może doprowadzić do uszkodzenia czy nawet zniszczenia urządzenia[27]. Właśnie taka niefizyczna destrukcja może być aktem cyberterroryzmu. Zważywszy na to, że górna granica zagrożenia karnego przekracza wymagane pięć lat pozbawienia wolności, artykuł 269 kk należy zaliczyć do grona przepisów penalizujących cyberterroryzm.

Przyjmuje się, że art. 269 kk stanowi *lex specialis* wobec art. 268a kk. Wydaje się, że taka sama relacja zachodzi również między nim a art. 268 kk. Z uwagi na specyficzny charakter danych możliwy jest kumulatywny zbieg przepisów z artykułami 173, 174 oraz 165 kk. W opinii autora także art. 140 kk może pozostawać w zbiegu kumulatywnym z art. 269 kk.

Przepisem, który może budzić problemy interpretacyjne jest art. 269a kk. Celem jego wprowadzenia była pełna realizacja założeń art. 5 *Konwencji o cyberprzestępczości* poprzez wypełnienie pewnej luki w zakresie penalizacji dokonywanej przez art. 269 i 287 kk – ten pierwszy odnosi się wyłącznie do określonych danych, drugi zaś nie dotyczy czynów popełnionych w innym celu, niż tylko z chęci osiągnięcia korzy-

[27] Szerzej zob. A. Baworowski, *Problemy wykładni przepisów*.., s. 75.

ści majątkowej[28]. Wobec takiego stanu rzeczy do kodeksu karnego dodano art. 269a o następującym brzmieniu:

> „Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

Karze podlega sprawca, który w istotny sposób zakłóci pracę systemu komputerowego lub sieci teleinformatycznej. Obok działań wymienionych w poprzednich przepisach pojawia się novum – zakłócanie działania (systemu lub sieci) poprzez transmisję danych. „Transmisja danych" to ich przesyłanie poprzez sieć do oraz z systemu (a także wewnątrz niego). Nadmierna transmisja danych może zakłócić działanie sieci („zapychając" ją) oraz systemu (wykorzystując całe dostępne zasoby pamięci i mocy obliczeniowej), co odpowiada *mail bombingowi* i atakom DDoS. Warto zauważyć, że działanie sprawcy musi dotyczyć danych informatycznych, a nie procesów ich dotyczących. Skutki oddziaływania na te dane muszą natomiast doprowadzić do istotnego zakłócenia pracy systemu lub sieci. Wydaje się zatem, że w art. 269a kk chodzi (za wyjątkiem transmisji) o dane mające szczególne znacznie dla działania systemów i sieci, tj. o pliki systemowe, ustawienia konfiguracyjne sprzętu itd.

Przedmiotem ochrony jest prawidłowe funkcjonowanie sieci teleinformatycznych i systemów komputerowych. Użycie sformułowania „system komputerowy" znacznie komplikuje prawidłowe zrozumienie art. 269a kk. O ile „system teleinformatyczny" posiada definicję legalną w ustawie, a „system informatyczny" w *Konwencji o cyberprzestępczości*, o tyle pojęcie „system komputerowy" nie występuje w polskim prawie karnym. W. Wróbel nie dostrzega dostatecznych racji, aby odróżniać pojęcie „system komputerowy" od terminu „system informatyczny". Podobnego zdania jest B. Kunicka-Michalska wskazująca na jego interpretację w myśl *Konwencji*, której rozwiązania art. 269a kk ma przecież wprowadzać do polskiego systemu prawnego. Trudno w tym przypadku posądzać ustawodawcę o pomyłkę, skoro ustawa ujednolicająca zmieniła treść sąsiednich przepisów, pozostawiła natomiast określenia „system komputerowy" oraz „sieć teleinformatyczna", co oznacza, że wolą ustawodawcy było odróżnienie go od innych systemów. Konieczne jest zatem ustalenie, czym jest system komputerowy i jaka jest różnica między nim a systemem informatycznym i teleinformatycznym. Wyjątkowo trafna jest uwaga B. Kunickiej-Michalskiej, że system komputerowy jest systemem informatycznym, w którym rolę „urządzenia" pełni komputer. Za taką interpretacją przemawia zarówno geneza przepisu, jak i działania, które mogą spowodować zakłócenie funkcjonowania systemu informatycznego. Systemem komputerowym w takim rozumieniu byłby zatem *każdy komputer lub grupa wzajemnie połączonych lub związanych ze sobą komputerów, z których jeden lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych*. Być może zamysłem ustawodawcy było posłużenie się przymiotnikiem „komputerowy" w powszechnym tego słowa rozumieniu. Odróżniałoby to działania przeciwko komputerom osobistym (które prócz przetwarzania danych służą także uzyskiwaniu dostępu do informacji) od tych, podejmowanych przeciw tak złożonym urządzeniom, jak superkomputery, czy rozbudowanym systemom, których zadaniem jest przetwarzanie ogromnych ilości danych.

[28] Uzasadnienie projektu ustawy z dnia 18 marca 2004 r. o zmianie ustawy *Kodeks karny*, ustawy *Kodeks postępowania karnego* oraz ustawy *Kodeks wykroczeń.*

Odchodząc od zagadnień interpretacyjnych, należy zwrócić uwagę na przewidziane zagrożenie karne – podobnie jak w przypadku art. 268 § 3 oraz 268a § 2 kk wynosi ono od trzech miesięcy do pięciu lat pozbawienia wolności. Jednocześnie warto zauważyć, że art. 269a kk jako *lex consumens* wyłącza stosowanie wspomnianych przepisów, ale jednocześnie sam może być wyłączony przez art. 269 kk stanowiący wobec niego *lex specialis*. Skutkiem tego art. 269a kk jawi się jako podstawowy przepis zwalczający akty terrorystyczne w cyberprzestrzeni.

Wspomniany wcześniej artykuł 287 kk jest przepisem umiejscowionym w rozdziale XXXV dotyczącym przestępstw przeciwko mieniu. W doktrynie zyskał on nazwę oszustwa komputerowego, w skutek połączenia określenia, jakim opisuje się to przestępstwo w paragrafie i metod działania sprawcy.

> „Art. 287 § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
>
> § 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
>
> § 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego."

Dobrem chronionym przez ten przepis jest mienie, ale, jak zauważa A. Suchorzewska, wnioskując ze znamion przestępstwa i kontekstu ustawowego, chodzi o *zbiorczą nazwę dla wszelkich praw majątkowych, których potwierdzeniem (dowodem istnienia) jest odpowiedni zapis w systemie gromadzącym, przetwarzającym lub przesyłającym automatycznie dane informatyczne albo mienie, z którym związany jest taki zapis*[29]. Z racji takiego ujęcia przedmiotu przestępstwa art. 287 kk obejmuje swą ochroną przede wszystkim własność oraz inne prawa rzeczowe (również obligacyjne) do mienia, które zostały wyrażone na nośniku informacji[30]. Jako przykład mienia można więc podać zapis stanu konta na rachunku bankowym, skład portfela inwestycyjnego prowadzonego przez dom maklerski, ale również kolekcję plików muzycznych przechowywaną na dysku twardym czy też aktualnie pisaną publikację, tworzoną grafikę albo komponowany utwór. Działanie sprawcy opisane w dyspozycji analizowanego przepisu polega na wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub ingerowaniu (zmienianiu, usuwaniu albo wprowadzaniu nowego zapisu) w dane informatyczne. Wpływanie takie, według M. Dąbrowskiej-Kardas i P. Kardasa, może się przejawiać we wszystkich formach zakłócania procesu, utrudnianiu jego przebiegu, uniemożliwianiu rozpoczęcia, przebiegu i zakończenia go, a także zniekształceniu tego procesu lub jego wyników[31]. Ze względu na znamię celu przestępstwo z art. 287 kk można by podzielić, co często czyni doktryna, na dwie odmiany – oszustwo komputerowe (mające na celu osiągnięcie korzyści majątkowej) oraz na szkodnictwo komputerowe (za cel stawiające sobie wyrządzenie innej osobie szkody). Choć osiągnięcie korzyści majątkowej może nosić cechy czynności przygotowawczej do aktu cyberterroryzmu, to jednak w kontekście popełnienia takiego aktu ważniejsze wydaje się działanie, które ma wyrządzić szkodę innej osobie – zwłaszcza,

[29] A. Suchorzewska, *Ochrona prawa systemów*..., s. 242.

[30] Tamże.

[31] Więcej na ten temat zob. *Kodeks karny*... t. 3, A. Zoll (red.), s. 324 i nast.

że górna granica zagrożenia karnego pozwala kwalifikować czyn stypizowany w art. 287 kk jako przestępstwo o charakterze terrorystycznym. Biorąc pod uwagę fakt, że penalizowane zachowanie bardzo przypomina zachowanie opisane w dyspozycjach wcześniej omawianych przepisów, ważną kwestią staje się określenie ich wzajemnej relacji. Ze względu na majątkowy charakter dóbr, w które godzi zachowanie sprawcy, art. 287 kk stanowi *lex specialis* wobec art. 268, 268a oraz 269a kk. W literaturze wskazano natomiast, że kumulatywny zbieg z art. 269 § 2 kk może mieć miejsce wtedy, gdy modyfikacja danych (usunięcie, zmiana wprowadzenie nowych zapisów) będzie dotyczyła danych odnośnie do mienia i jednocześnie mających szczególne znaczenie[32].

Wszystkie analizowane powyżej przepisy zakładają karalność umyślnego działania sprawcy, co wydaje się być zabiegiem właściwym. Należy pamiętać, że standardowym działaniem administratorów jest zabezpieczanie i ograniczanie dostępu do danych oraz systemów przed ingerencją osób niepowołanych. Trudno więc sobie wyobrazić, by osoba o przeciętnych umiejętnościach obsługi komputera mogła w sposób przypadkowy dopuścić się czynów stypizowanych w powyższych przepisach. Odpowiada to również naturze przestępstwa o charakterze terrorystycznym, które jest popełniane „w celu", a zatem zawsze w zamiarze umyślnym. Niemal wszystkie artykuły (za wyjątkiem art. 269 i 287 kk) przewidują karalność działań osoby, która nie jest uprawniona do ich wykonania. Okolicznością wyłączającą kryminalną bezprawność czynu jest zatem fakt działania osoby upoważnionej, np. administratora systemu czy funkcjonariuszy organów powołanych do ochrony bezpieczeństwa publicznego.

Przepisy penalizujące skutki cyberataków

Skutki popełniania powyższych przestępstw sprowadzają się do powodowania strat w cyberprzestrzeni – głównie niszczenia danych, utrudnienia ich przetwarzania, zakłócenia działania systemów i sieci, a niekiedy także uszkodzenia lub zniszczenia sprzętu. Oczywiście już takie straty mogą spowodować, że cel działania terrorystów zostanie osiągnięty. Przykładowo, uniemożliwienie działania systemów giełdy może spowodować poważne zakłócenia w gospodarce, a zablokowanie dostępu do kont bankowych zastraszyć wiele osób. Niemniej jednak, jak wcześniej wskazano, działania w cyberprzestrzeni mogą być tylko środkiem mającym wywołać straty w świecie rzeczywistym. Wobec tego warto przeanalizować także przestępstwa, które mogą być skutkiem działań dokonywanych w cyberprzestrzeni.

Przepisem najczęściej wymienianym w literaturze, który został wskazany także w założeniach do RPOC[33], jest artykuł 165 kk. Penalizuje on spowodowanie niebezpieczeństwa dla dóbr, jakimi są życie i zdrowie wielu osób oraz mienia w wielkich rozmiarach, przy czym może być ono rozumiane w sposób tożsamy z mieniem wielkiej wartości w rozumieniu art. 115 kk. W rzeczywistości chodzi o fizyczne rozmiary mienia, a nie jego wartość[34]. Zagrożenie to nie musi mieć charakteru bezpośredniego, konieczne jest jednak by było realne, a nie abstrakcyjne[35]. Formy działania prowadzące do wywołania tego zagrożenia zostały opisane w paragrafie pierwszym tego przepisu:

[32] Tamże, s. 335.

[33] http://bip.msw.gov.pl/download/4/4297/program_20ochrony_20cyberprzestrzeni.pdf [dostęp: 25 VI 2011].

[34] R.A. Stefański, *Pojęcie „mienia o wielkich rozmiarach"*, „Prokuratura i Prawo" 1999, nr 1.

[35] *Kodeks karny*..., M. Filar (red.), s. 735.

„Art. 165 § 1. Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach:
1) powodując zagrożenie epidemiologiczne lub szerzenie się choroby zakaźnej albo zarazy zwierzęcej lub roślinnej,
2) wyrabiając lub wprowadzając do obrotu szkodliwe dla zdrowia substancje, środki spożywcze lub inne artykuły powszechnego użytku lub też środki farmaceutyczne nie odpowiadające obowiązującym warunkom jakości,
3) powodując uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności urządzenia dostarczającego wodę, światło, ciepło, gaz, energię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia,
4) zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych,
5) działając w inny sposób w okolicznościach szczególnie niebezpiecznych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

Szczególnie interesujące w kontekście cyberataków są punkty 3 i 4. Punkt trzeci przewiduje karalność uszkodzenia lub unieruchomienia urządzeń użyteczności publicznej i jednocześnie podaje ich przykłady. Wydaje się, że działanie opisane w art. 165 § 1 pkt. 3 kk może dotyczyć większości (a być może nawet wszystkich) systemów składających się na infrastrukturę krytyczną. Ustawodawca wskazuje jedynie na urządzenia użyteczności publicznej, których naruszenie może powodować powstanie niebezpieczeństwa dla ludzi lub mienia, nie określając jednocześnie, w jaki sposób miałyby one zostać uszkodzone lub unieruchomione. Tym samym zakresem penalizacji przepisu jest objęte każde działanie, które może wywołać wspomniany skutek, np. odcięcie źródła zasilania, wymontowanie ważnych elementów, fizyczne zniszczenie, ale też oddziaływanie na układ sterujący czy wprowadzenie fałszywych danych. Tymczasem wymieniany w punkcie czwartym sposób działania sprowadza się do wpływania na automatyczne przetwarzanie, gromadzenie i przekazywanie danych, bez konkretnego wskazania treści czy charakteru tych danych. Zatem przy dokonywaniu kwalifikacji prawnej cyberataku o charakterze terrorystycznym czyn ten będzie, co do zasady, jednocześnie wypełniał znamiona opisane w obu wspomnianych punktach. Karą, jaką ustawodawca przewidział za popełnienie tego przestępstwa w typie podstawowym, jest pozbawienie wolności od sześciu miesięcy do ośmiu lat. Jeśli następstwem czynu będzie śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, to granice wymiaru kary będą wynosiły od dwóch do dwunastu lat pozbawienia wolności. Wydaje się, że możliwy jest kumulatywny zbieg przestępstw wymienionych w artykułach 268a i 269 kk. Ze względu na wartość mienia chronionego przez art. 165 kk będzie on stanowił *lex consumens* wobec art. 287 kk. Nie da się też wykluczyć możliwości zbiegu art. 165 § 1 pkt. 3 z art. 269a kk.

Artykuł 163 kk przewiduje karę za spowodowanie zdarzenia, które zagraża życiu lub zdrowiu wielu osób albo mieniu w wielkich rozmiarach. Aby można było je za takie uznać, powinno ono przyjąć jedną z form wymienionych w § 1, czyli formę:
- pożaru,
- zawalenia się budowli, jej zalania albo obsunięcia się na nią ziemi, skał lub śniegu,
- eksplozji materiałów wybuchowych lub łatwopalnych albo innego gwałtownego wyzwolenia energii, rozprzestrzenienia się substancji trujących, duszących lub parzących,
- gwałtownego wyzwolenia energii jądrowej lub wyzwolenia promieniowania jonizującego.

Można sobie wyobrazić, że w niektórych przypadkach działania w cyberprzestrzeni mogą wywołać zdarzenie, które będzie miało jedną z wyżej wymienionych form, np. będzie to pożar w fabryce wywołany przez awarię spowodowaną wyłączeniem systemu chłodzenia albo zalanie dużych obszarów poprzez jednoczesne, całkowite otwarcie wszystkich śluz w tamie. W takim przypadku przewidywana kara wynosi od roku do dziesięciu lat pozbawienia wolności, w typie kwalifikowanym zaś (gdy następstwem jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób) od dwóch do dwunastu lat pozbawienia wolności. Samo sprowadzenie bezpośredniego niebezpieczeństwa takiego zdarzenia podlega natomiast, w myśl art. 164 kk, karze pozbawienia wolności od sześciu miesięcy do ośmiu lat.

Sektorem szczególnie narażonym na ataki terrorystyczne jest transport i komunikacja. To właśnie środki transportu zbiorowego były celem zamachów w Madrycie (2004 r.) i Londynie (2005 r.). Także działania terrorystów w cyberprzestrzeni, polegające na przejęciu kontroli nad systemami zarządzającymi transportem i komunikacją, mogą wywołać tragiczne skutki. Stąd też wobec sprawców takich ataków może mieć zastosowanie art. 173 kk:

> „Art. 173 § 1. Kto sprowadza katastrofę w ruchu lądowym, wodnym lub powietrznym zagrażającą życiu lub zdrowiu wielu osób albo mieniu w wielkich rozmiarach, podlega karze pozbawienia wolności od roku do lat 10".

Karalnością jest objęte każde działanie, które doprowadza do katastrofy wszelkiego rodzaju środków transportu, zagrażające ludzkiemu życiu, zdrowiu lub mieniu w wielkich rozmiarach. Wydaje się, że, podobnie jak niebezpieczeństwa wymienione w art. 165 kk, zagrożenie to może być realne. Przykładem działania cyberterrorystycznego wypełniajacego znamiona art. 173 kk byłoby spowodowanie karambolu samochodowego poprzez ingerencję w działanie sygnalizacji świetlnej albo wprowadzenie statku na mieliznę poprzez modyfikację danych systemu GPS na temat jego położenia. Zagrożenie karne za popełnienie tego czynu jest analogiczne jak w przypadku art. 163 kk – od roku do dziesięciu lat pozbawienia wolności w typie podstawowym, od dwóch do dwunastu lat, jeśli doprowadzi do śmierci człowieka lub ciężkiego uszczerbku na zdrowiu wielu osób (art. 173 § 3 kk), i od sześciu miesięcy do ośmiu lat pozbawienia wolności za sprowadzenie bezpośredniego niebezpieczeństwa katastrofy (art. 174 § 1 kk).

Powyższe wyliczenie nie stanowi zamkniętego katalogu czynów karalnych, które mogą być skutkiem cyberataków. W istocie ma ono jedynie charakter przykładowy, wskazujący na najbardziej prawdopodobne przestępstwa. Trudno przewidzieć sposób działania cyberterrorystów i dobra prawne, które będą naruszać, wskutek czego niemożliwe jest wskazanie dokładnej kwalifikacji prawnej czynu. Wydaje się jednak, że nie będą oni poprzestawać na powodowaniu strat w cyberprzestrzeni i że będą dążyć do wywołania szkód w świecie rzeczywistym, przedkładając efektowność działań nad ich efektywność.