 Please cite as: BiTP Vol. 38 Issue 2, 2015, pp. 105–111

DOI:10.12845/bitp.38.2.2015.9

dr **Joanna Stojer-Polańska**[1]
inż. **Artur Luzar**[2]

Przyjęty/Accepted/Принята: 14.10.2014;
Zrecenzowany/Reviewed/Рецензирована: 23.05.2015;
Opublikowany/Published/Опубликована: 30.06.2015;

Współczesne zagrożenia teleinformatyczne w aspekcie działań służb ratowniczych

Contemporary Threats to Information Technology (IT) Security in Context of Fire and Rescue Services Activities

Современные информационно-коммуникационные угрозы в контексте действий спасательных служб

ABSTRAKT

Cel: Celem artykułu jest rozpoznanie i identyfikacja współczesnych zagrożeń, których źródłem jest działalność człowieka w cyberprzestrzeni oraz analiza potencjalnych zagrożeń, które wynikają z szybkiego rozwoju sieci teleinformatycznych. W artykule wskazane zostały czynniki ryzyka oraz opisano potencjalne zachowania sprawców czynów z zakresu cyberprzestępczości i cyberterroryzmu, które mogą być źródłem zagrożenia wobec działań służb ratowniczych oraz systemów powiadamiania ratunkowego. Celem artykułu jest więc identyfikacja czynników ryzyka, która jest pomocna w stworzeniu odpowiednich strategii prewencyjnych wobec cyberprzestępczości i cyberterroryzmu.
Wprowadzenie: Obserwowany współcześnie szybki rozwój technologii wyprzedza rozwój badań z dziedziny nauk społecznych dotyczących zachowania człowieka w cyberprzestrzeni i człowieka w obliczu rozwoju nowych technologii. Rozwój technologiczny wyprzedza również regulacje prawne, dlatego często brakuje norm prawnych, które wskazują, jak działać w nowej sytuacji. Stąd też tworzy się spekulacje na temat możliwego zachowania człowieka w związku z rozwojem sieci teleinformatycznych oraz buduje scenariusze działań na wypadek konieczności prowadzenia akcji ratowniczych w skomplikowanych warunkach, zarówno prawnych, jak i faktycznych. Przećwiczenie takich działań może być pomocne podczas rzeczywistych akcji ratunkowych.
Metodologia: Analizą objęto dostępne sprawozdania (Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013, Raport o stanie bezpieczeństwa RP w 2013) oraz dostępną literaturę z zakresu zagrożenia cyberterroryzmem i cyberprzestępczością. W pracy wskazane zostały główne źródła zagrożeń oraz hipotetyczne scenariusze na podstawie już dokonanych ataków na sieci teleinformatyczne, ze szczególnym uwzględnieniem aspektów związanych ze skuteczną działalnością służb ratowniczych.
Wnioski: Autorzy postulują prowadzenie badań nad rozwojem technologii w kontekście zachowania jednostek oraz opracowanie strategii prewencyjnych wobec nowych zagrożeń, których źródłem może być cyberprzestrzeń. Podkreślają także wagę przeprowadzenia w systemie ustawicznym szkoleń dotyczących współczesnych zagrożeń wynikających z rozwoju technologii, a także prowadzenie edukacji na temat skutków rozwoju technologii. Należy wykorzystać szanse, jakie daje rozwój naukowy, a jednocześnie minimalizować ryzyko potencjalnych nowych zagrożeń. Konieczne jest także promowanie badań i współpracy interdyscyplinarnej pomiędzy służbami odpowiedzialnymi za akcje ratunkowe i bezpieczeństwo.

Słowa kluczowe: cyberterroryzm, cyberprzestępczość, zagrożenie teleinformatyczne, służby ratunkowe
Typ artykułu: artykuł przeglądowy

ABSTRACT

Aim: The purpose of this article is the identification of contemporary challenges, the source of which is human activity in the cyberspace, as well as provision of an analysis of potential risks following the rapid development of IT networks. The article identifies risk factors and describes potential behaviour of cybercrime perpetrators, and cyber terrorists, which pose risks to the operation of emergency services

[1] Uniwersytet Dzieci, Kraków / The Children's University, Poland; wkład merytoryczny w powstanie artykułu / percentage contribution – 50%;
[2] Szkoła Aspirantów Państwowej Straży Pożarnej w Krakowie / The Fire Service College of the State Fire Service in Krakow; wkład merytoryczny w powstanie artykułu / percentage contribution – 50%; artur.luzar@gmail.com;

DOI:10.12845/bitp.38.2.2015.10

and proper functioning of the emergency notification system. Therefore, the article intends to identify risks, which should be considered and utilised in the design of appropriate preventive strategies against cybercrime and cyber terrorism.
Introduction: Current developments in IT surpass the development of social sciences concerning human behaviour in cyberspace and response to development of new technology. Technological developments precede the creation of laws and consequently we frequently encounter an absence of legal norms, which specify appropriate action to evolving situations. Consequently, there is some speculation about potential behaviour of humans in relation to developments of IT networks and scenarios are developed in response to needs associated with the conduct of operations in complex circumstances, both legal as well as practical. Training, which incorporates such elements, may be useful for real life rescue operations.
Methodology: Available reports were analysed (Report concerning cyberspace safety in the Republic of Poland 2013, Poland 2013 Crime and Safety Report) as well as available literature about cyber terrorism and cybercrime risks. Research has identified main sources of threats as well as hypothetical scenarios based on IT network attacks identified to date, with a particular focus on aspects associated with successful operation of rescue services.
Conclusions: The authors recommend further research about technological developments, in the context of human behaviour and creation of preventive strategies against emerging threats, the source of which may be cyberspace activity. The importance of a continuous training system, to deal with current threats, which emerge from technological progress is emphasised, as well as the need for education about the consequences of future technological developments. Opportunities arising from technological developments should be grasped, but potential risks from emerging threats should be minimized. It is also necessary to promote research and interdisciplinary cooperation between the uniformed services responsible for safety and rescue operations.

Keywords: cyber terrorism, cybercrime, IT threat, rescue services
Type of article: review article

АННОТАЦИЯ

Цель: Целью статьи является распознание и идентификация современных угроз, источником которых является деятельность человека в киберпространстве, а также анализ потенциальных угроз, которые являются результатом быстрого развития информационно-коммуникационных сетей. В статье были указаны факторы риска и описаны потенциальные поведения виновных в сфере киберпреступности и кибертерроризма, которые могут быть источником опасности для действий спасательных служб и систем аварийного оповещения. Целью данной статьи является идентификация факторов риска, которая необходима при разработке соответствующих предупредительных стратегий по борьбе с киберпреступностью и кибертерроризмом.
Введение: В настоящее время наблюдается быстрое развитие технологии, которое опережает развитие исследований в области общественных наук, касающихся поведения человека в киберпространстве и человека в условиях развития новых технологий. Технологическое развитие опережает также правовое регулирование, поэтому часто отсутствуют правовые нормы, которые указывали бы, как действовать в новой ситуации. Поэтому возникают спекуляции о возможном поведении человека в связи с развитием информационно-коммуникационных сетей и разрабатываются сценарии поведения на случай необходимости проведения спасательных действий в сложных условиях, как правовых, так и фактических. Практика проведения таких мероприятий может помочь при проведении реальных спасательных работ.
Методология: Анализ включал доступные отчёты (отчёт о состоянии безопасности киберпространства Республики Польша в 2013, отчёт о состоянии безопасности в Республике Польша в 2013) и имеющуюся литературу об угрозе кибертерроризма и киберпреступности. В работе были указаны главные источники угроз и гипотетические сценарии, на основе совершенных атак на информационно-коммуникационные сети, с особым акцентом на аспекты, связанные с эффективной деятельностью спасательных служб.
Выводы: Авторы предлагают проводить исследования развития технологий относительно поведения отдельных лиц и развивать предупредительные стратегии предотвращения новых угроз, источником которых может быть киберпространство. Мы также подчёркиваем значение проведения в рамках системы образования обучения, касающегося современных угроз, обусловленных развитием технологии, а также проведение обучения по последствиям технологического развития. Следует использовать возможности, которые предоставляет развитие науки, и одновременно минимизовать риск новых потенциальных угроз. Необходимо также продвигать исследования и междисциплинарное сотрудничество между службами, отвечающими за спасательные работы и безопасность.

Ключевые слова: кибертерроризм, киберпреступность, информационно-коммуникационная угроза, спасательные службы
Вид статьи: обзорная статья

1. Wprowadzenie

Obecność systemów komputerowych w niemal wszystkich gałęziach przemysłu i administracji przyczyniła się do zwiększenia komfortu pracy i jej wydajności. Zastosowanie innowacyjnych rozwiązań i systemu wspomagania decyzji w Państwowej Straży Pożarnej zaowocowało znacznym wzrostem efektywności działań ratowniczych. Kierunkiem rozwoju jest więc łączenie tradycyjnego podejścia do ratownictwa z wykorzystaniem najnowszych technologii. W nieodległej przyszłości nieodzownym atrybutem dowódców kierujących akcją ratowniczą będzie tablet lub laptop, które umożliwią śledzenie na bieżąco rozwoju sytuacji na miejscu akcji, prowadzenie korespondencji radiowej z ratownikami, a także konsultacje z ekspertami z różnych dziedzin ratownictwa.

Wielkie nadzieje pokładane są również w bezzałogowych systemach latających (tzw. dronach). Ich zastosowanie może być bardzo szerokie – od lotów zwiadowczych monitorujących zagrożenie pożarowe w lasach do bardziej zaawansowanych

takich jak szybkie dostarczenie defibrylatora na miejsce wypadku komunikacyjnego lub ocena zagrożenia pożarowego poprzez analizę widma dymu. W ramach programów *smart city* takie rozwiązania są już testowane na świecie, a służby mundurowe i zarządzający miastami dokonują zakupów dronów. Pisząc o nowych technologiach, trzeba docenić rodzime produkcje oraz aplikacje wspomagające pracę ratowników. Wśród nich należy wspomnieć o takich przedsięwzięciach jak bezpłatna aplikacja Ratownik wspomagająca edukację z zakresu kwalifikowanej pierwszej pomocy, czy też zaangażowanie kół naukowych inżynierii technicznych w rozwój bezzałogowych systemów latających wspierających straż pożarną. Z drugiej jednak strony pojawiają się nowe zagrożenia dla bezpieczeństwa związane z rozwojem technologii, mogące w konsekwencji doprowadzić do paraliżu wielu obszarów życia publicznego, w tym do wyłączenia działania służb ratowniczych i systemu powiadamiania ratunkowego. To właśnie systemy komputerowe zarządzają wieloma obszarami infrastruktury krytycznej w branżach takich jak: energetyka, transport, bankowość, służba zdrowia oraz w krytycznej z punktu widzenia systemu ratownictwa telekomunikacji. Celem artykułu jest wskazanie współczesnych zagrożeń związanych z rozwojem sieci komputerowych i infrastruktury teleinformatycznej. W przekonaniu autorów zagrożenie cyberterroryzmem wydaje się obecnie bardzo realne.

2. Zjawisko cyberterroryzmu

Terroryzm jako zagrożenie dla bezpieczeństwa jest terminem wieloznacznym. Autorzy publikacji z zakresu bezpieczeństwa, zarządzania kryzysowego i dziedzin pokrewnych posługują się różnymi definicjami zjawiska terroryzmu [1–4]. Zjawisko cyberterroryzmu jest trudne do zdefiniowania [5–7]. Pierwsze incydenty związane z bezpieczeństwem teleinformatycznym miały miejsce na przełomie lat 70. i 80. ubiegłego wieku. W 1983 roku w Stanach Zjednoczonych kilka komputerów należących do instytucji rządowych padło ofiarą ataku kilku nastoletnich hackerów z tzw. grupy „414's". Zdarzenie to wywołało szeroką dyskusję w kongresie USA [8]. Jednak zdecydowaną intensyfikację występowania zagrożeń terrorystycznych obserwuje się od 2001 roku, kiedy to nastąpił atak muzułmańskich ekstremistów na World Trade Center w Nowym Jorku. Od tego właśnie momentu rządy poszczególnych państw świata zachodniego zaczęły traktować zagrożenie terroryzmem, w tym także cybernetycznym, jako realne i mogące spowodować ogromne straty, porównywalne z konwencjonalnymi atakami terrorystycznymi. W związku z tym faktem zaczęto stosować coraz bardziej zaawansowane metody prewencji i obrony przed cyberterrorystami. Z obserwacji praktyki wynika, że najczęstszą formą ataków stają się strony internetowe instytucji publicznych[3]. W historii można znaleźć przykłady zdecydowanie bardziej niebezpiecznych działań takich jak cyberataki na infrastrukturę krytyczną oraz systemy bankowe. Najbardziej spektakularny atak przy użyciu wirusa komputerowego Stuxnet nastąpił na irański system komputerowy kontrolujący pracę elektrowni atomowych. Stuxnet dzięki wykorzystaniu luk w systemie Windows może przejąć całkowitą kontrolę nad systemem odpowiedzialnym za zarządzanie instalacjami przemysłowymi, co w konsekwencji może doprowadzić nawet do fizycznego samozniszczenia tej instalacji. W Europie Środkowo-Wschodniej głównymi ofiarami hackerów stały się instytucje państwowe w Estonii (2007), na Litwie (2008) oraz w Gruzji (2008).

Jak już wspomniano, nie istnieje ogólnie przyjęta definicja cyberterroryzmu. Pojęcia tego nie definiuje również polskie prawo. W art. 115 § 20 Kodeksu Karnego[4] zdefiniowano przestępstwo o charakterze terrorystycznym. Definicja ta jednak poddawana jest krytyce w literaturze przedmiotu [9]. Konsekwencją niejednolitej wykładni jest utrudniona praca w tworzeniu strategii prewencyjnych, a także problemy dla organów ścigania i wymiaru sprawiedliwości. Niezwykle trudno jest pociągnąć do odpowiedzialności sprawców tego typu przestępstw, ponieważ samo ich wykrycie sprawia wiele problemów. Teoretycznie możliwe byłoby również odwołanie się do art. 269, art. 269a lub 269b Kodeksu Karnego[5]. Autorzy niniejszego artykułu

[3] Zob. Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013, Cert.gov.pl, Warszawa 2014, s. 5 i nast.: „W sumie, w 2013 roku zarejestrowanych zostało aż 8817 zgłoszeń, z których 5670 zakwalifikowano, jako incydenty".

[4] Ustawa Kodeks Karny Dz. U. z 1997 r. Nr 88, poz. 553 ze zm. Treść przepisu: 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.

[5] Ustawa Kodeks Karny Dz. U. z 1997 r. Nr 88, poz. 553 ze zm. Treść przepisów: 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.
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.
Art. 269b. § 1. Kto wytwarza, pozyskuje, zbywa lub udostępnia innym osobom urządzenia lub programy komputerowe przystosowane do popełnienia przestępstwa określonego w art. 165 § 1 pkt 4, art. 267 § 3, art. 268a § 1 albo § 2 w związku z § 1, art. 269 § 2 albo art. 269a, a także hasła komputerowe, kody dostępu lub inne dane umożliwiające dostęp do informacji przechowywanych w systemie komputerowym lub sieci teleinformatycznej, podlega karze pozbawienia wolności do lat 3. § 2. W razie skazania za przestępstwo określone w § 1, sąd orzeka przepadek określonych w nim przedmiotów, a może orzec ich przepadek, jeżeli nie stanowiły własności sprawcy.

DOI:10.12845/bitp.38.2.2015.10

podzielają stanowisko wyrażone przez K. Lidela, który za zjawisko cyberterroryzmu uznaje „politycznie umotywowany atak lub groźbę ataku na komputery, sieci lub systemy informatyczne w celu zniszczenia infrastruktury oraz zastraszenia lub wymuszenia na rządzie i ludziach daleko idących politycznych i społecznych celów" [10]. Przy czym należy dodać, że zdarzenia o charakterze cyberterrorystycznym mogą być również powodowane motywacją tzw. *for fun and fame* (dla zabawy i sławy) lub wynikać z motywów wyłącznie finansowych.

Ryzyko zagrożenia cyberprzestępczością z roku na rok jest coraz większe. Duża jest też z pewnością ciemna liczba tego rodzaju zachowań w Internecie. Słusznie wskazują autorzy *Raportu o stanie bezpieczeństwa RP w 2013 roku*, że „w większości przypadków cyberprzestrzeń nie stwarza nowego rodzaju przestępstwa, a jedynie dostarcza nowych metod i środków do jego popełnienia lub stanowi jedynie nowe miejsce popełnienia przestępstw, jej rzeczywista skala jest trudna do oszacowania" [26]. Nie dotyczy to jednak ataków na systemy teleinformatyczne [26, s. 291], które należy postrzegać jako odrębny czyn zabroniony. Nie jest do końca jasne, czy czyn potencjalnego sprawcy wypełni znamiona określonego przepisu ustawy karnej, bowiem działania z zakresu cyberterroryzmu są wysoce nieprecyzyjne w literaturze przedmiotu. Nie można zarzucić osobie, że popełniła przestępstwo, jeśli nie wypełniła znamion określonych w przepisach prawa. Może jednak dojść do sytuacji, w której sprawca dopuszcza się czynu zasługującego na karę, ale nieujętego w przepisach prawa. Prawo bardzo często nie nadąża za rozwojem technologii [11]. Ponadto wiele tego typu zdarzeń może pozostawać we wspomnianej ciemnej liczbie zdarzeń kryminalnych, bowiem nikt nie zawiadomił odpowiednich organów o możliwości popełnienia przestępstwa, a służbom odpowiedzialnym za bezpieczeństwo nie udało się samodzielnie uzyskać informacji o takim wydarzeniu.

Ryc. 1. Bezzałogowy statek latający
Fig. 1. Unmanned flying craft
Źródło/Source: fot. Grzegorz Mazur

3. Kim są cyberterroryści [12]?

P. Sienkiewicz i H. Świeboda zaproponowali podział cyberterryzmu na dwa główne źródła: zagrożenia ustrukturalizowane oraz nieustrukturalizowane. Jeśli chodzi o pierwsze, powołani autorzy zwracają uwagę na niebezpieczeństwa wynikające z działalności służb obcych państw, w szczególności wyspecjalizowanych instytucji państwowych zatrudniających ekspertów z dziedziny bezpieczeństwa sieci teleinformatycznych. Równie niebezpieczne są lokalne bądź ponadpaństwowe zorganizowane grupy przestępcze, a w szczególności podmioty o charakterze zbrojnym i terrorystycznym. Istnieją silne przesłanki świadczące o tym, że do tej grupy należałoby zaliczyć także międzynarodowe korporacje dysponujące wiedzą, technologią oraz sprzętem, dzięki którym mogą przechwytywać poufne informacje gospodarcze.

Źródła zagrożeń nieustrukturalizowanych tworzą pojedyncze osoby, względnie niewielka grupa osób. Są to przede wszystkim amatorscy hackerzy, haktywiści, cybernetyczni wandale i frustraci. Szkodliwość ich działalności jest różnie oceniana, nie zawsze jest też znana motywacja do popełniania czynów zagrażających bezpieczeństwu sieci teleinformatycznych. Dostęp do specjalistycznej wiedzy oraz bardzo kosztowego sprzętu powoduje, iż poważniejszych konsekwencji można się spodziewać ze strony dużych, strukturalnych grup, aniżeli pojedynczych osób. Nie można jednak wykluczyć, że jednostka może spowodować bardzo duże zagrożenie dla bezpieczeństwa powszechnego. Największym wyzwaniem dla organów ścigania są tzw. samotne wilki, bowiem trudno prowadzić wobec nich działania wykrywcze [13]. Bardzo niepokojąca wydaje się też możliwość manipulowania w sieci grupą podobnie jak w sekcie, tak więc jedna osoba mogłaby korzystać z działań i sprzętu komputerowego innych osób, niekoniecznie świadomych celu tych działań.

Niestety raz na jakiś czas dochodzi do trudnych do przewidzenia zdarzeń takich jak masakra dokonana przez A. Breivika, w wyniku której życie straciło kilkadziesiąt osób. A. Breivik przed zamachem opublikował w Internecie informację, co zamierza uczynić. Takie wydarzenia nazywane bywają „czarnymi łabędziami", bowiem nie są spotykane szczególnie często [14]. Z tego też powodu przy opracowaniu działań na wypadek zagrożeń należy również rozpatrywać ewentualność wersji zdarzeń mało prawdopodobnych lub nawet nieprawdopodobnych. Pozwoliłoby to na sprawniejsze reagowanie w sytuacji zagrożenia.

Autorzy pragną podkreślić, że czasami czynniki ryzyka związane z określoną jednostką, takie jak skłonność do agresji lub autoagresji, mogą wpływać na bezpieczeństwo innych osób i wymuszać konieczność zaktywizowania służb ratunkowych. Przykładem są zachowania suicydalne występujące również w cyberprzestrzeni – na forach, na których dyskutuje się o tym, jak popełnić samobójstwo [15]. Rola informatyków może polegać na zlokalizowaniu osoby deklarującej chęć popełnienia samobójstwa [16], natomiast to służby ratunkowe i policja będą następnie uczestniczyć w zdarzeniu [17]. Jednak funkcja prewencyjna, a także operacyjna i wykrywcza w cyberprzestrzeni nie może być pomijana przez właściwe służby.

4. Zagrożenie dla podmiotów ratowniczych

Podmioty ratownicze, takie jak Państwowa Straż Pożarna, Ochotnicza Straż Pożarna, czy Państwowe Ratownictwo Medyczne oraz inne służby pomocnicze, nie powinny traktować zjawiska cyberterroryzmu jako zjawiska nierealnego lub mało prawdopodobnego. Atak przeprowadzony na infrastrukturę teleinformatyczną może spowodować skutki bardziej dotkliwe od tradycyjnie przeprowadzonego ataku terrorystycznego.

Z punktu widzenia działalności służb ratowniczych obszarami zagrożenia są:

- funkcjonowanie numerów alarmowych (112, 998),
- system sterowania ruchem miejskim,
- system alarmowania osób funkcyjnych,
- ciągłość funkcjonowania oprogramowania dyspozytorskiego,
- ograniczenie lub wyłączenie zasilania sieci hydrantowych,
- ataki mieszane.

5. Funkcjonowanie numerów alarmowych

Sieci telekomunikacyjne stanowią potencjalny cel ataku cyberterrorystów. Szczególnie niebezpieczny, a zarazem z technicznego punktu widzenia stosunkowo niezbyt trudny do przeprowadzenia, wydaje się atak polegający na przeciążeniu sieci telefonicznej poprzez zmasowaną próbę połączeń w jednym czasie np. za pomocą wykorzystania technologii VOIP. Dodatkowym zagrożeniem może być nagły wzrost fałszywych zgłoszeń. W przypadku ataków mieszanych zdarzenie to w konsekwencji doprowadzi do obniżenia potencjału ratowniczego na miejscu faktycznego zamachu.

6. System sterowania ruchem miejskim

Atak na serwery oraz infrastrukturę obsługującą sygnalizację świetlą na skrzyżowaniach miast może doprowadzić do wydłużenia czasu dojazdu wozów bojowych Państwowej Straży Pożarnej, zespołów ratownictwa medycznego i innych jednostek oraz służb. Wirus komputerowy może przykładowo spowodować włączenie na wszystkich skrzyżowaniach czerwonego światła dla wszystkich ulic dochodzących do danego skrzyżowania, lub co gorsza światła zielonego, co z pewnością spowodowałoby liczne kolizje i wypadki samochodowe[6]. Awarie tego typu zdarzają się, powodując paraliż ruchu ulicznego. W Krakowie w październiku 2013 roku na skutek wady fabrycznej światłowodu łączącego serwer obsługujący sygnalizację świetlą spowodował kilkudziesięciominutowe opóźnienie komunikacji miejskiej.

7. System alarmowania osób funkcyjnych

W momencie wystąpienia faktycznego zagrożenia, dyżurny stanowiska kierowania zobligowany jest do powiadomienia o zaistniałej sytuacji właściwego komendanta/dowódcę komendy/jednostki ratowniczo-gaśniczej. Niestety jest to łączność w dużej mierze oparta na sieci GSM, a alarmowanie osób funkcyjnych często odbywa się poprzez wysyłanie wiadomości SMS. W tym celu dyżurni wykorzystują moduł alarmowania Systemu Wspomagania Decyzji ST. Dla cyberterrorystów zablokowanie kilku lub kilkunastu numerów telefonicznych GSM nie stanowi żadnego problemu, dlatego ważne jest, aby w każdej jednostce organizacyjnej PSP istniała procedura na wypadek wystąpienia takiego incydentu.

8. Ciągłość funkcjonowania oprogramowania dyspozytorskiego

Monitoring użycia sił i środków odbywa się za pomocą Systemu Wspomagania Decyzji ST. Oparta na systemie

[6] Motyw taki został przedstawiony w filmie *Szklana pułapka IV*, reż. L. Wiseman, 2007.

DOI:10.12845/bitp.38.2.2015.10

teleinformatycznym aplikacja dostarcza niezbędnych informacji o dostępnych w danej chwili strażakach, specjalistach z różnych dziedzin ratownictwa, środkach gaśniczych oraz samochodach gaśniczych i specjalnych. Nagły brak tych informacji w sytuacji wzmożonego zapotrzebowania na dysponowanie sił i środków byłby sporym utrudnieniem dla dyżurnych stanowisk kierowania poszczególnych szczebli. O ile do tej pory oprogramowanie dyspozytorskie PSP nie padło ofiarą poważnych awarii, to nie można tego samego powiedzieć o systemach informatycznych innych służb. Krajowy System Informacyjny Policji, umożliwiający szybką kontrolę praw jazdy kierowców oraz informacji dotyczących skradzionych pojazdów, w październiku 2014 roku po raz kolejny uległ awarii. W efekcie policjanci mieli ograniczony dostęp do niezbędnych danych, co czasowo osłabiło potencjał tej formacji. W opinii autorów niepotrzebnie informacje o tego typu awariach zamieszczane są na portalach ogólnodostępnych [27].

9. Ograniczenie lub wyłączenie zasilania sieci hydrantowych

Obecnie niechętnie podchodzi się do automatyki zasilania miejskiej sieci hydrantowej, tym niemniej prawdopodobne jest, iż w przyszłości będą one w całości zarządzane przez sieć komputerową. Sytuacja taka występuje już dziś m.in. w niektórych stanach USA. Cyberatak na tego typu infrastrukturę wymagałby podawania wody na dużą odległość metodą dowożenia lub korzystania z alternatywnych źródeł – sztucznych lub naturalnych zbiorników wody.

10. Ataki mieszane – szczególny rodzaj zagrożenia

Połączenie tradycyjnego ataku terrorystycznego, w którym napastnicy używają np. ładunków wybuchowych oraz ataku cybernetycznego, to tzw. atak mieszany (ang. *blended attack*) [18]. Jest to szczególnie niebezpieczna sytuacja, bowiem opóźnienie o kilkanaście lub kilkadziesiąt minut przyjazdu służb ratowniczych na miejsce faktycznego zamachu bombowego mogłoby doprowadzić do zwiększenia liczby ofiar śmiertelnych.

Z jednej strony rozwój techniki i technologii umożliwia prowadzenie bardziej efektywnych działań służb ratunkowych, z drugiej zaś naraża ich akcje na nieoszacowane ryzyko. Przykładowo – drony, które planuje zakupić Państwowa Straż Pożarna, postrzegane są jako narzędzie do zwiększenia efektywności działań w stosunku do tradycyjnie prowadzonych akcji ratunkowych [19]. Dron może zostać wykorzystany zarówno do poszukiwań zaginionej osoby, jak i do zdobywania informacji z powietrza o miejscu zagrożenia pożarem czy powodzią [20]. Nie można jednak wykluczyć, że możliwe jest zdalne sterowanie urządzeniem przez osoby do tego nieuprawnione. Istnieją techniczne możliwości pozwalające na przejęcie komunikacji pomiędzy dronem i operatorem poprzez podanie sfałszowanego sygnału GPS (spoofing GPS). Cyberterrorysta może w ten sposób wydać dronowi zmodyfikowane dyspozycje np. zaprogramować dowolny, inny kurs, zmusić go do lądowania lub przejąć całe urządzenie. Warto tu wspomnieć o wrogim przejęciu wojskowego drona Lockheed Martin RQ-170 w 2011 roku na terenie Iranu [21]. Z perspektywy służb ratunkowych takie incydenty mogą spowodować opóźnienie akcji ratunkowej lub też wysłanie niewłaściwych jednostek do działań w niewłaściwym miejscu, a taki przypadek należy rozpatrywać w kontekście działań cyberterrorystycznych.

11. Edukacja ma znaczenie

Kolejną sprawą, niezwykle istotną z punktu widzenia prewencji, jest właściwa edukacja na temat zagrożeń oraz czynników ryzyka. Powinna ona przebiegać dwutorowo: jako element nauczania w szkołach pożarniczych oraz poprzez samodoskonalenie zawodowe dyspozytorów oraz kadry w ramach kształcenia ustawicznego. Negatywne skutki braku szkoleń z zakresu bezpieczeństwa teleinformatycznego są widoczne w wielu jednostkach organizacyjnych PSP, gdzie w pojedynczych przypadkach zdarza się, że wydrukowane dane niezbędne do logowania wiszą na tablicach korkowych stosunkowo łatwo dostępnych także dla osób trzecich. Takie nieostrożne zachowania często wynikają z niewiedzy oraz niefrasobliwości [22].

Szczególnym obszarem wiedzy o przeciwdziałaniu współczesnym zagrożeniom, na jaki należy zwrócić uwagę podczas szkoleń, to inżynieria społeczna. Choć termin ten może się kojarzyć z naukami społecznymi, to wedle definicji jest to „zestaw metod mających na celu uzyskanie niejawnych informacji przez cyberprzestępcę" [23] poprzez wykorzystanie łatwowierności i nieświadomości użytkowników systemów informatycznych celem pokonania zabezpieczeń odpornych na techniczne formy ataku. Cyberprzestępcy, podając się np. za administratora systemu lub pracownika producenta oprogramowania, mogą próbować wyłudzić dane niezbędne do wprowadzania niepożądanych zmian w systemach wykorzystywanych przez Państwową Straż Pożarną.

W programach kształcenia strażaków różnego szczebla nie znajdują się żadne treści kształcenia traktujące o bezpieczeństwie informatycznym, co w dobie wzrostu zagrożenia atakami terrorystycznymi wydaje się być dużym niedopatrzeniem i może spowodować wzrost zagrożenia.

12. Podsumowanie

Walka z zagrożeniami terrorytycznymi i przeciwdziałanie im stały się obecnie jednymi z największych wyzwań, przed którymi stoją służby mundurowe wszystkich państw. Szczególnym rodzajem zagrożeń jest terroryzm cybernetyczny, zwany cyberterrotyzmem, oraz terroryzm mieszany i/lub kombinowany, w którym wraz z tradycyjnymi formami ataków terrorystycznych przeprowadzane są jednocześnie ataki na sieci teleinformatyczne. Odpowiednia edukacja i przygotowanie się na sytuację zagrożenia bezpieczeństwa sieci teleinformatycznej może zabezpieczyć przed tego typu incydentami, a w chwili ich wystąpienia poprawi efektywność prowadzenia akcji ratowniczych.

Literatura

[1] Indecki K., *W sprawie definicji normatywnej terroryzmu*, w: *Przestępczość zorganizowana: świadek koronny, terroryzm w ujęciu praktycznym*, E. Pływaczewski (red.), Zakamycze, Kraków 2005.

[2] Wiak K., *Prawnokarne środki przeciwdziałania terroryzmowi*, Wydawnictwo KUL, Lublin 2009.

[3] Aleksandrowicz T.R., *Medialność jako konstruktywne znamię aktu terrorystycznego,* w: *Terroryzm w medialnym obrazie świata*, K. Liedel, S. Mocek (red.), Wydawnictwo TRIO, Warszawa 2010.

[4] Horgan J., *Psychologia terroryzmu*, PWN, Warszawa 2008.

[5] Serwiak S., *Cyberprzestrzeń jako źródło zagrożenia terroryzmem*, w: *Przestępczość zorganizowana: świadek koronny, terroryzm w ujęciu praktycznym*, E. Pływaczewski (red.), Zakamycze, Kraków 2005.

[6] Aleksandrowicz R. T., *Nowy terroryzm*, w: *Współczesne zagrożenia terroryzmem oraz metody działań antyterrorystycznych*, J. Szafrański (red.), Wyższa Szkoła Policji w Szczytnie, Szczytno 2007.

[7] Bolechów B., *Terroryzm w świecie podwubiegunowym. Przewartościowania i kontynuacje*, Wydawnictwo Adam Marszałek, Toruń 2003.

[8] Compiled by washingtonpost.com, Timeline: The U.S. Government and Cybersecurity, The Washington Post, 16 maja 2003, [dok. elektr.] http://www.washingtonpost.com/wp-dyn/articles/A50606-2002Jun26.html, [dostęp: 02.10.2014].

[9] Górniok O., *Przestępstwo o charakterze terrorystycznym w art. 115 § 20 k.k.*, „Przegląd Sądowy", Issue 10, 2004, pp. 3–11.

[10] Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2005.

[11] Tomaszewski T., *Dowód naukowy przed sądem*, w: *Prawo wobec nowych technologii*, P. Girdwoyń (red.), Liber, Warszawa 2008, 155–164.

[12] Lakomy M., *Zagrożenia dla bezpieczeństwa teleinformatycznego państw – przyczynek do typologii*, „e-Politikon", 2013, 6, s. 100–141 [dok. elektr.], http://oapuw.pl/e-politikon-nr-62013/, [dostęp: 2.10.2014].

[13] Małysa T., *Rozpoznawanie działalności terrorystycznej*, „E-terrroryzm.pl. Internetowy Biuletyn Centrum Studiów nad Terroryzmem i kwartalnika e-Studia nad Bezpieczeństwem i Terroryzmem", Issue 8, 2012.

[14] Taleb N.N., *The Black Swan*, Random House Trade Paperbacks, New York 2008.

[15] Rosa K., Krzywania P., *Ekspozycja zachowań samobójczych w sieci. Analiza treści stron internetowych,* w: *Percepcja zachowań samobójczych. Między opiniami a doświadczeniami*, Uniwersytet Medyczny w Łodzi, Kraków 2014.

[16] Krawczyk P., Maj M., *Informacje o próbach samobójczych w Internecie. Metody identyfikacji źródeł wiadomości,* w: *Samobójstwo. Stare problemy, nowe rozwiązania*, J. Stojer Polańska, A. Biederman-Zaręba (red.), Jak, Kraków 2013.

[17] Kuca P., Luzar A., *Praktyczne aspekty działań prowadzonych przez strażaków Państwowej Straży Pożarnej w Krakowie w przypadku samobójstwa*, w: *Samobójstwo. Stare problemy, nowe rozwiązania*, J. Stojer Polańska, A. Biederman-Zaręba (red.), Jak, Kraków 2013.

[18] Coleman K., *Cyberterrorism preparedness for fire and emergency services*, [dok. elektr.], http://www.fireengineering.com/articles/2013/04/cyberterrorism-preparedness-for-fire-and-emergency-services.html, [dostęp: 02.10.2014].

[19] Kosieliński S., *In statu nascendi*, w: *Roboty w przestrzeni publicznej. In statu nascendi*, A. Gontarz, S. Kosieliński (red.), Instytut MikroMakro, Warszawa 2014.

[20] Sowizdraniuk P., *Wsparcie dla ratowników,* w: *Roboty w przestrzeni publicznej. In statu nascendi*, A. Gontarz, S. Kosieliński (red.), Instytut MikroMakro, Warszawa 2014.

[21] Miszczak A., *Drony* z każdej strony, „Focus", Issue 8, 2014.

[22] Kołodziej M., *Ukrywanie się i podszywanie w Internecie*, w: *Przestępczość teleinformatyczna*, J. Kosiński (red.), Wyższa Szkoła Policji w Szczytnie, Szczytno 2009.

[23] Suchorzewska A., *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem*, Wydawnictwo Wolters Kluwer, Warszawa 2010.

[24] Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2013, Cert.gov.pl, Warszawa 2014.

[25] Ustawa Kodeks Karny Dz. U. z 1997 r. Nr 88, poz. 553 ze zm.

[26] Raport o stanie bezpieczeństwa RP w roku 2013, MSW, Warszawa 2014.

[27] http://wiadomosci.onet.pl/kraj/wielka-awaria-w-policji-nie-dziala-krajowy-system-informacyjny-policji/bjzyb, [dostęp: 4.10.2014].

* * *

dr Joanna Stojer-Polańska – doktor nauk prawnych, kryminalistyk. Absolwentka Uniwersytetu Jagiellońskiego. Autorka artykułów naukowych dotyczących oddziaływania mediów na proces karny, artykułów dotyczących działań sprawców z nietypowym modus operandi i sprawców działających w cyberprzestrzeni, redaktor książki poświęconej samobójstwom. Wykładowca akademicki z kryminalistyki, kryminologii, zwalczania przestępczości. Prowadzi zajęcia z kryminalistyki na Uniwersytecie Dzieci w Krakowie.

inż. Artur Luzar – inżynier bezpieczeństwa cywilnego, absolwent Szkoły Głównej Służby Pożarniczej. Pracownik Wydziału Informatyki i Łączności Szkoły Aspirantów Państwowej Straży Pożarnej w Krakowie. Entuzjasta nowych technologii.