ZESZYTY NAUKOWE POLITECHNIKI RZESZOWSKIEJ **Nr 260**
Zarządzanie i Marketing z. 16 (3/09) **2009**

Jacek LIPSKI*
Wyższa Szkoła Informatyki, Zarządzania i Administracji

SPRAWOZDANIE Z KONFERENCJI NAUKOWEJ „CYBERTERRORYZM – NOWE WYZWANIE XXI WIEKU”

W artykule przedstawiono sprawozdanie z konferencji, której celem było omówienie problemów związanych z cyberterroryzmem, jako największym zagrożeniem dla współczesnego społeczeństwa informacyjnego. Dokonano także oceny obowiązujących przepisów prawnych, służących ściganiu przestępstw tego typu i zapobieganiu im.

Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie wspólnie z Wydziałem Prawa i Administracji, a także Wydziałem Zarządzania Uniwersytetu Warszawskiego oraz Wyższą Szkołą Policji, Akademią Obrony Narodowej i Agencją Bezpieczeństwa Wewnętrznego zorganizowała w dniu 18 maja 2009 r. I Konferencję Naukową „Cyberterroryzm – nowe wyzwania xxi wieku”.

Konferencja odbyła się pod patronatem Wicemarszałka Sejmu RP VI kadencji, posła **Stefana Niesiołowskiego**, a w komitecie honorowym uczestniczyli: **Grzegorz Schetyna** – Wicepremier, Minister Spraw Wewnętrznych i Administracji, **Bogdan Klich** – Minister Obrony Narodowej, **Barbara Kudrycka** – Minister Nauki i Szkolnictwa Wyższego, **Krzysztof Bondaryk** – Szef Agencji Bezpieczeństwa Wewnętrznego, **Andrzej Matejuk** – Komendant Główny Policji, **Marek Witczak** – Komendant Główny Żandarmerii Wojskowej, **Zdzisław Nowakowski** – Rektor Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, **Arkadiusz Letkiewicz** – Komendant-Rektor Wyższej Szkoły Policji w Szczytnie oraz prof. zw. dr hab. **Tadeusz Tomaszewski** – Prorektor ds. Nauczania i Polityki Kadrowej Uniwersytetu Warszawskiego.

Przewodniczącym Komitetu Programowego konferencji był prof. zw. dr hab. **Jerzy Kisielnicki** z Wydziału Zarządzania Uniwersytetu Warszawskiego, zastępca przewodniczącego Rady Informatyki przy Ministrze Spraw Wewnętrznych i Administracji.

Otwarcia konferencji na uroczystej sesji plenarnej i przywitania wszystkich obecnych dokonał prof. dr inż. Zdzisław Nowakowski – Rektor Wyższej Szkoły Informatyki Zarządzania i Administracji w Warszawie, a wprowadzenia do dyskusji w ramach referatu pt.: **Cyberterroryzm jako element zagrożenia współczesnej cywilizacji**[1] dokonał prof. zw. dr hab. Jerzy Kisielnicki. Autor interesująco omówił zagadnienie rewolucji informacyjnej i jej

* Dr Jacek Lipski, Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie.

[1] T. Jemioło, J. Kisielnicki, K. Rajchel (red.), *Cyberterroryzm – nowe wyzwania XXI wieku*. Materiały konferencji naukowej zorganizowanej w dniu 18 maja 2009 r., WSIZiA w Warszawie, WSP w Szczytnie, AON, Warszawa 2009, s. 17-27.

społeczne reperkusje, a także związane z tym zagrożenia cyberterroryzmem w trakcie budowy społeczeństwa informacyjnego. Uznał w nim budowę społeczeństwa informacyjnego za fakt. Również Polska winna dążyć do takiego właśnie ukształtowania się jej infrastruktury, gwarantującej państwo demokratyczne i zarazem nowoczesne. Jednocześnie zwrócił on uwagę na związane z tym pojawiające się nowe zagrożenia. Zakwalifikował do nich cyberterroryzm w różnych postaciach, uznając go za najistotniejsze niebezpieczeństwo dla społeczeństwa informacyjnego. Podkreślił, że winny znaleźć się odpowiednie środki na działania o charakterze antycyberterrorystycznym.

Realizacja programu konferencji odbywała się w części plenarnej i dwóch panelach o tematyce: **Zagrożenia cyberterroryzmem w XXI wieku** oraz **Cyberterroryzm zagrożeniem bezpieczeństwa państwa**.

Pierwszy panel poświęcony został zagadnieniom zagrożeń cyberterroryzmem w XXI wieku. W panelu tym zaprezentowano pięć referatów. Prof. P. Sienkiewicz przedstawił referat noszący tytuł: **Terroryzm w cybernetycznej przestrzeni**. Podkreślił, że oczywistą konsekwencją rozwoju sieciowych technologii informacyjnych jest zagrożenie bezpieczeństwa narodowego (międzynarodowego). Jak wskazał, już I wojnę w Zatoce Perskiej określano mianem *The First Information War*. Następnie zaczęto posługiwać się pojęciami *Cyberwar*, *Netwar* czy też *Network Centric Warfare*. P. Sienkiewicz zasygnalizował, że równolegle do koncepcji walki zbrojnej postępował proces coraz silniejszego uzależnienia od technologii teleinformatycznych wszystkich niemal sfer życia społecznego. Wraz z pojawieniem się nowych zagrożeń w postaci przestępstw komputerowych, istotnym problemem stał się wzrost podatności na zagrożenia informacyjne poszczególnych podsystemów krytycznej infrastruktury państwa. Wspomniał również o nowym wymiarze wojny – przestrzeni cybernetycznej, która stała się nową sferą zagrożeń dla bezpieczeństwa wewnętrznego, także w czasie pokoju – polem działań terrorystycznych cyberterroryzmu.

A. Gniadek zaprezentował referat pt. **Cyberprzestępczość i cyberterroryzm – zjawiska szczególnie niebezpieczne**, w którym zwrócił uwagę na fakt, że cyberatak może wkrótce stać się głównym narzędziem walki grup ekstremistycznych. Zaznaczył jednak, że nieprędko zastąpi on działania konwencjonalne, które dają natychmiastowy rozgłos i efekt, ale należy już spodziewać się transformacji w działaniach terrorystycznych, których przywódcy są coraz lepiej wykształceni oraz bardziej otwarci na korzystanie ze zdobyczy techniki. Wskazał również na kluczową rolę służb w zakresie przeciwdziałania i likwidacji ewentualnych skutków zaistnienia zjawiska cyberprzestępczości i cyberterroryzmu, uwypuklając rolę wzajemnej ich współpracy.

Profesor J.W. Wójcik omówił zagadnienie **Zagrożenie w cyberprzestrzeni a przestępstwa ekonomiczne**. Na wstępie zaznaczył, że sieć internetowa stała się wymarzonym narzędziem dla przestępców, obecnie przede wszystkim dla fałszerzy i oszustów. Jednocześnie zwrócił uwagę na współczesne wydarzenia, które miały miejsce w wielu regionach świata, kiedy to przez specjalistyczne działania doprowadzano do kradzieży cennych danych czy do zablokowania stron internetowych wielu instytucji strategicznych. Prof. Wójcik uznał je za dowód na istnienie cyberterroryzmu jako realnego zagrożenia dla bezpieczeństwa państwa. W sieci toczy się wojna nazywana cyberwojną, w którą angażowane są duże pieniądze, a więc światowa finansjera, media, politycy oraz zorganizowani przestępcy. Mówca zdefiniował również pojęcie cyberprzestępczości oraz cyberterroryzmu. Nadto dokonał analizy poszczególnych kategorii terrorystów (nuklearnych, ekonomicznych, finasowych), a także wybranych zagrożeń cyberterrorystycznych.

Doktor T.R. Aleksandrowicz przedstawił referat pt. **Sieć jako forma organizacji terrorystycznej**. Udowadniał w nim, że powstanie społeczeństwa informacyjnego wpłynęło na ukształtowanie się tzw. nowego terroryzmu. Koncepcja ta zakłada pojawienie się nowych, nieznanych wcześniej lub występujących jedynie sporadycznie cech organizacji terrorystycznych, stwarzających znacznie większe zagrożenia dla społeczności międzynarodowych. Akcentował tutaj sieciowy charakter organizacji, oznaczający odejście od klasycznej struktury hierarchicznej oraz jednoznacznej, stałej lokalizacji, bezterytorialność. Uznał za oczywiste, że powstanie sieciowych organizacji terrorystycznych powoduje konieczność zmiany strategii antyterrorystycznej. Zwalczanie organizacji sieciowej za pomocą metod stosowanych przez klasyczne struktury hierarchiczne ocenił jako zadanie niezwykle skomplikowane, mogące być nawet niewykonalne. Na zakończenie podkreślił, że konflikt pomiędzy mobilnymi sieciami globalnymi a państwem narodowym to w swojej istocie konflikt asymetryczny – sieci mają w nim przewagę. Skuteczna walka z zagrożeniami sieciowymi wymaga zarówno zmiany sposobu myślenia i właściwego postrzegania zagrożeń w kontekście ich sieciowego charakteru, jak też tworzenia struktur o podobnym od strony organizacji i funkcjonalności charakterze.

R. Szpyra w swym wystąpieniu skoncentrował się na problemie, który można określić jako **Cyberterroryzm – poszukiwanie istoty i charakterystyki**. Omówił w nim genezę proponowanego ujęcia cyberterroryzmu, dostrzegając ją przede wszystkim w instytucji walki. Dokonał również analizy pojęć „cyberprzestrzeń", „cyberwalka", „cyberterroryzm". Podkreślił, iż cyberterroryzm może przybrać formę ataku informatycznego, ataku psychologicznego, jednocześnie przybliżył znaczenie tych form.

Autorzy kolejnych referatów wiele miejsca poświęcali zagadnieniom związanym z określeniem pojęć. Węzłowym pojęciem w tym zakresie jest definicja cyberprzestępczości. Według Soumyo d. Moitra, profesora zarządzania i polityki społecznej z Indian Institute of Management Calcutta, obecnie za cyberprzestępstwo uważa się każde negatywne zachowanie, w które zaangażowane są trzy czynniki: komputer hakera, sieć i komputer ofiary, a *modus operandi* sprawcy dotyczy popełnienia przestępstwa wyłącznie przy użyciu Internetu[2].

Panel drugi dotyczył cyberterroryzmu jako zagrożenia bezpieczeństwa państwa. W tej części zaprezentowanych zostało sześć referatów. K. Liedel przedstawił opracowanie **Bezpieczeństwo informacyjne państwa w dobie zagrożeń terrorystycznych**. Zaznaczył w nim, że bezpieczeństwo informacyjne w dobie rosnącego znaczenia zasobów informacyjnych jako zasobów strategicznych państwa staje się jednym z najbardziej kluczowych obszarów. Jednocześnie podkreślił konieczność skupienia na nim aktywności służb i instytucji odpowiedzialnych za bezpieczeństwo państwa. W referacie poddał również analizie współczesne zagrożenia terroryzmem, zagrożenia dla bezpieczeństwa informacyjnego państwa, w szczególności cyberterroryzmem. Ponadto podkreślił, że cyberterroryzm zagrażać może państwu na co najmniej trzech poziomach, na których atak może zagrozić bezpieczeństwu tego państwa, porządkowi publicznemu oraz pozycji państwa na arenie międzynarodowej. Dostrzegł potrzebę wypracowania przez państwo algorytmu postępowania w obszarze zapewnienia bezpieczeństwa informacji, inwestowania w systemy bezpieczeństwa informacyjnego, które pozwolą chronić jego

[2] M. Rydel, *Jak się bronić przed cyberprzestępczością*, [w:] http://www.rp.pl/artykul/61229,307131.

zasoby, jak również prowadzić walkę informacyjną ze wszystkimi podmiotami, zagrażającymi temu bezpieczeństwu.

Z. Bekier zaprezentował **Wybrane aspekty zwalczania cyberterroryzmu**. Zdefiniował on termin „cyberterroryzm" jako atak na system lub informację plus strach oraz żądanie. Dodatkowo zaznaczył, że zwalczanie cyberterroryzmu jest procesem złożonym, przybierającym różne formy i wykorzystującym różne środki w zależności od chronionego dobra, podjętego działania, nauk wspierających zwalczanie cyberterroryzmu, podmiotów zwalczających cyberterroryzm. Zwrócił uwagę, że zapobieganie jest najlepszym sposobem zwalczania każdego zagrożenia, a ewentualne ataki cyberterrorystyczne wykorzystywać będą błędy w systemach zabezpieczeń czy też czynnik ludzki. Za antidotum uznał właściwą politykę bezpieczeństwa, technologie oraz szeroko rozumianą współpracę międzynarodową. Ponadto wskazał na rolę odpowiedniego ustawodawstwa, dającego podstawę prawną do ścigania nowych niebezpiecznych zjawisk w Internecie. Zauważył, że istnieje ścisły związek pomiędzy efektywnym zwalczaniem przestępczości teleinformatycznej a zwalczaniem cyberterroryzmu.

Adwokat Adam Baworowski w swym referacie pt. **Cyberterroryzm w prawie karnym materialnym – przyczynek do dyskusji na gruncie analizy dogmatycznej**[3] zasygnalizował niezmiernie interesujące zagadnienie dotyczące stosowanej terminologii w polskim ustawodawstwie. Prelegent poddał także krytyce niektóre regulacje prawne. Autor w profesjonalny sposób zwrócił uwagę na fakt konieczności przestrzegania obowiązującego prawa i dążności do jego doskonalenia na bazie rozpoznanych zagrożeń. Istotnym elementem przeciwdziałania cyberprzestępczości, wynikającym z jej transgraniczności, jest dostosowanie polskiego prawa karnego i procesowego do wymagań UE. Obwiązujący stan prawny nie jest wystarczającym czynnikiem do skutecznych działań zapobiegawczych. Również stosowana terminologia w obowiązującym ustawodawstwie jest niejednolita, a niekiedy niewłaściwa, jak np.: „informatyczny nośnik danych", „dokument elektroniczny", „system teleinformatyczny" oraz „środki komunikacji elektronicznej". A. Baworowski trafnie zauważył, że ilustracją tego stanu rzeczy będzie wprowadzenie przez ustawę ujednolicającą do porządku prawnego (oprócz kodeksu karnego) pojęcia „system teleinformatyczny" i jednoczesne pozostawienie w kodeksie karnym przez ustawodawcę określeń: „system komputerowy", „sieć teleinformatyczna", „system informatyczny". Dalej autor na podstawie analizy dogmatycznej wyprowadza następujący wniosek, dotyczący zasadności stosowania terminu „system teleinformatyczny", który zgodny jest z definicją legalną ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną,[4] który obejmuje zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie i przechowywanie, a także wysyłanie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego w rozumieniu ustawy z dnia 21 lipca 2000 r. – Prawo telekomunikacyjne[5].

E. Lichocki przedstawił referat zatytułowany **Bezpieczeństwo teleinformatyczne Sił Zbrojnych Rzeczypospolitej Polskiej w dobie zagrożeń cybernetycznych**. Zaznaczył w nim, że problem bezpieczeństwa teleinformatycznego w Siłach Zbrojnych RP jest

[3] *Ibidem*, s. 396-412.

[4] Dz.U. Nr 144, poz. 1204 ze zm.

[5] Dz.U. Nr 73, poz. 852, z 2001 r. Nr 122, poz. 1321 i Nr 154, poz. 1800 i 1802 oraz z 2002 r. Nr 25, poz. 253 i Nr 74, poz. 676.

postrzegany przez instytucje Ministerstwa Obrony Narodowej jako jeden z bardzo ważnych obszarów prawidłowego funkcjonowania wojska. Na zmianę poglądów w tym względzie wpłynęły wydarzenia w Estonii w kwietniu 2007 r., gdzie w wyniku cyberataku zostały zablokowane strony organów władzy Estonii, uszkodzone łącza teleinformatyczne z Unią Europejską i NATO. E. Lichocki wskazał, że kwestie bezpieczeństwa teleinformatycznego Sił Zbrojnych obecnie są przedmiotem zainteresowania nie tylko w Polsce, ale również koncentrują na niej uwagę wojskowe organizacje międzynarodowe. W 2008 r. w Tallinie powstało natowskie centrum ostrzegania przed cyberatakami *(NATO Cooperative Center of Exelence in Cyber Defence* – Centrum Doskonalenia Obrony przed Cyberatakami), zakładające niesienie pomocy państwom członkowskim NATO w przypadku wystąpienia cyberataków na ich sieci komputerowe. Lichocki podkreślił konieczność uświadomienia sobie realnego niebezpieczeństwa, wynikającego z niedostatecznych zabezpieczeń teleinformatycznych sieci bezprzewodowych jednostek organizacyjnych MON, oraz potrzebę przygotowania odpowiedniej kadry służb, do których kompetencji należy zapewnienie bezpieczeństwa w państwie, jak również właściwą współpracę między nimi. Akcentował także wysokie prawdopodobieństwo zaistnienia cyberataku na instytucje rządowe w kraju, podyktowane m.in. zaangażowaniem militarnym i dyplomatycznym Polski.

R. Bałdys i T. Leszczyński byli autorami referatu **Cyberterroryzm zagrożeniem bezpieczeństwa energetycznego społeczeństwa informacyjnego**, w którym wychodząc od określenia bezpieczeństwa społeczeństwa informacyjnego, omówili zagrożenia bezpieczeństwa energetycznego. Zwrócili uwagę na zasadniczą rolę bezpieczeństwa energetycznego państwa i ocenili, że z tego powodu dostarczanie społeczeństwu paliwa, ciepła, energii elektrycznej może w pierwszej kolejności (obok systemów informatycznych czy też za ich pośrednictwem) stać się obiektem cyberataku. Ponadto uznali rozmiar organizacji jako istotny czynnik decydujący o rodzaju oraz sposobie rozmieszczenia stosowanych rozwiązań ochronnych. Mimo że cyberatakami zagrożone są głównie obiekty infrastruktury krytycznej na szczeblu państwa, to najbardziej podatne na nie są małe i średnie przedsiębiorstwa oraz instytucje samorządowe.

Kryminalistycznym śladom elektronicznym i metodyce zbierania tego rodzaju dowodów poświęcony został referat **Dowody elektroniczne – problematyka zabezpieczenia i dobre praktyki**, opracowany przez doktoranta Wydziału Prawa i Administracji UW mgr. P. Królikowskiego, który zwrócił uwagę na niezmiernie ważną kwestię, jaką jest zabezpieczanie elektronicznego materiału dowodowego dla potrzeb procesu karnego. Wymaga to profesjonalnego przygotowania biegłych posiadających wiadomości specjalne. Należy uznać, że zabezpieczanie oraz analiza materiału dowodowego w postaci elektronicznej, ze względu na jego cechy, wymagają szczególnej uwagi. Specjaliści, a w szczególności biegli z zakresu informatyki nie zawsze postępują zgodnie z zasadą dobrej praktyki, co sprawia, że na etapie postępowania sądowego możliwe jest podważenie jego wartości. Jednym z powodów takiego stanu rzeczy może być brak wyczerpujących polskich regulacji i ogólnodostępnych wytycznych. W związku z tym autor postuluje:

1) wprowadzenie nauczania prawa informatycznego do programu studiów prawniczych oraz informatycznych,
2) objęcie edukacją wszystkich tych, którzy ze względu na specyfikę pracy będą coraz częściej mieć do czynienia z zagadnieniem zabezpieczania dowodów elektronicznych

(a w szczególności studentów wydziałów prawa i informatyki, policjantów, prokuratorów, sędziów, a także obrońców),
3) opracowanie ogólnodostępnego zbioru procedur, ewentualnie wytycznych, którymi mogą kierować się specjaliści oraz biegli, posiadający wiadomości specjalne niezbędne w realizacji zabezpieczania dowodów elektronicznych,
4) przygotowanie i ujednolicenie mechanizmów przydatnych do weryfikacji kompetencji biegłych sądowych[6].

Spośród 49 opublikowanych w ramach Konferencji referatów należy zwrócić uwagę na tak istotne zagadnienia, jak chociażby:

- ochrona infrastruktury krytycznej, co było przedmiotem rozważań Pawła Witkowskiego: **Infrastruktura krytyczna państwa – idealny cel dla cyberterrorystów**[7], a także
- nielegalne wykorzystywanie cyberprzestrzeni w referacie gen. bryg. pil. dr. Jana Rajchela: **Wykorzystywanie cyberprzestrzeni przez organizacje terrorystyczne**[8].

Ostatni wygłoszony w trakcie obrad referat K. Lidermana nosił tytuł: **Połączone sieci teleinformatyczne i sieci przemysłowe jako elementy infrastruktury krytycznej – zagrożenia i podstawowe standardy ochrony**. Prelegent zdefiniował w nim istotne dla prezentowanego wystąpienia terminy: „bezpieczeństwo na zewnętrz", „bezpieczeństwo do wewnątrz", „bezpieczeństwo informacji". Poddał analizie wpływ informacji na bezpieczeństwo infrastruktury krytycznej, istniejące zagrożenia w tym zakresie, jak również zdefiniował pojęcia: „bezpieczeństwo infrastruktury krytycznej", „atak na system teleinformatyczny oraz na informację w nim przetwarzaną". Zwrócił także uwagę na nową jakość w dziedzinie bezpieczeństwa – łączenie sieci przemysłowych i teleinformatycznych.

Konferencję zakończyło przyjęcie **Stanowiska** uczestników obrad, którego treść odpowiadała prezentowanym w ramach spotkania poglądom.

STANOWISKO UCZESTNIKÓW I KONFERENCJI „CYBERTERRORYZM – NOWE WYZWANIA XXI WIEKU"

Wyższa Szkoła Informatyki, Zarządzania i Administracji w Warszawie wspólnie z Uniwersytetem Warszawskim, Wyższą Szkołą Policji, Akademią Obrony Narodowej i Agencją Bezpieczeństwa Wewnętrznego zorganizowała w dniu 18 maja 2009 r. I Konferencję CYBERTERRORYZM – NOWE WYZWANIA XXI WIEKU.

Uczestnicy Konferencji reprezentowali środowiska naukowe, administrację rządową, samorządową oraz praktyków z organów ścigania i wymiaru sprawiedliwości. Prezentowane przez nich referaty i ożywiona dyskusja stały się podstawą do stwierdzenia, że cyberterroryzm jest nowym, bardzo dynamicznie rozwijającym się w świecie zjawiskiem, które ma doniosłe następstwa społeczne i wywołuje liczne nieznane wcześniej problemy, wymagające skutecznego przeciwdziałania. Powszechna komputeryzacja, tak jak wiele innych zjawisk i procesów związanych z postępem technicznym, oprócz wartości pozytywnych niesie

[6] *Ibidem*, s. 371-395.
[7] *Ibidem*, s. 592-603.
[8] *Ibidem*, s. 604-614.

ze sobą dysfunkcjonalne skutki uboczne, do których należy zaliczyć różnorodne nadużycia popełniane z wykorzystaniem nowoczesnych technologii przetwarzania informacji.

Cel konferencji został osiągnięty, gdyż ukazano istotę tych problemów oraz dokonano oceny obowiązujących przepisów prawnych, służących ich ściganiu i zapobieganiu. Natomiast przedstawione dalej wnioski i spostrzeżenia wynikają z prezentowanych na Konferencji referatów, jak i wywołanej nimi dyskusji.

Zasadne jest stanowisko, że potencjalne zagrożenia stwarzane przez cyberterroryzm wywołały potrzebę sprawnego działania nie tylko ekspertów ds. bezpieczeństwa, lecz wszystkich użytkowników systemów teleinformatycznych. Istniejący rodzaj działalności przestępczej wskazuje na realne możliwości zaatakowania nie tylko rządowych, lecz również prywatnych systemów teleinformatycznych, a co za tym idzie, wskazuje na niebezpieczeństwo, jakim jest atak na infrastrukturę krytyczną państwa.

Dotkliwy jest brak kryminologicznej diagnozy i prognozy zjawiska, co niezwykle utrudnia zapobieganie, a prezentowane referaty i wyniki badań wskazują na szczególnie duże rozpowszechnienie różnorodnych zagrożeń. Niezbędne są działania w formie systematycznie dokonywanego profesjonalnego rozpoznania, mającego na celu wypracowanie kryminologicznej diagnozy, prognozy i profilaktyki.

Niezwykle ważne jest dokonanie diagnozy możliwości oraz potrzeb służb odpowiedzialnych za bezpieczeństwo państwa w obszarach przeciwdziałania cyberterroryzmowi. Pozwoli to wyposażyć służby w narzędzia i środki służące również do przeciwdziałania cyberprzestępczości na miarę aktualnych zagrożeń.

Wzrost zagrożeń ze strony terrorystów, działających w sieciach publicznych, od których całkowita separacja jest niemożliwa, a także fakt rozproszonej odpowiedzialności za bezpieczeństwo teleinformatyczne wskazuje, że niezbędne jest wprowadzenie systemowych rozwiązań w zakresie przeciwdziałania cyberterroryzmowi. Umożliwią one szybkie ujawnienie wszelkich zagrożeń oraz efektywne reagowanie na zagrożenia i ataki wymierzone przeciwko krytycznym systemom, a systemowi teleinformatycznemu przede wszystkim, a ponadto w przypadkach, gdy zostaną wykorzystane przez terrorystów do prowadzenia oddziaływania socjotechnicznego w cyberprzestrzeni w formie radykalizacji, rekrutacji, szkoleń lub propagandy ideologicznej, a także manipulacji informacją.

Systemowe przeciwdziałanie cyberterroryzmowi wymaga jednak podjęcia stosownych przedsięwzięć umożliwiających właściwym służbom realizację zadań na rzecz ochrony cyberprzestrzeni, a przede wszystkim ochrony społeczeństwa przed jego skutkami. Należy się bowiem spodziewać dalszego wzrostu zainteresowania cyberprzestępczością ze strony zorganizowanych grup przestępczych, w tym o charakterze międzynarodowym.

Prewencja antyterrorystyczna w cyberprzestrzeni ma ogromne znaczenie dla bezpieczeństwa państwa nie tylko w świecie wirtualnym, ale przede wszystkim rzeczywistym. Podnoszenie bezpieczeństwa w sieci zwiększy poziom bezpieczeństwa infrastruktury krytycznej państwa oraz odporności państwa na ataki cyberterrorystyczne.

Kluczowe znaczenie w kontekście budowy systemu przeciwdziałania cyberterroryzmowi ma zdefiniowanie pojęcia „cyberterroryzm" oraz działań wyczerpujących znamiona tego przestępstwa. Brak precyzyjnej definicji cyberterroryzmu powoduje trudności w kwalifikacji prawnej przestępstw o charakterze terrorystycznym, popełnianych w cyberprzestrzeni, a ponadto może powodować trudności w ustaleniu organu właściwego dla ścigania ich sprawców. W tym względzie wyróżnić należy przynajmniej trzy podstawowe potrzeby:

1) *ochrony cyberprzestrzeni przed atakami terrorystycznymi, dokonywanymi zarówno w sposób tradycyjny (np. poprzez fizyczne zniszczenie baz danych), jak i ataki dokonywane wewnątrz sieci, których celem mogą być serwery strategiczne z punktu widzenia działania państwa,*
2) *zwrócenia uwagi na wieloaspektowość zjawiska cyberprzestępczości, obejmującej swym zasięgiem zarówno dziedziny związane z przestępczością ekonomiczną, jak też z przestępczością kryminalną, narkotykową czy z pogranicza cyberterroryzmu,*
3) *ujęcia tematyki związanej z ochroną cyberprzestrzeni w toku prac nad przygotowywaną obecnie strategią zwalczania przestępczości zorganizowanej.*

Niezbędne jest przestrzeganie obowiązującego prawa i dążność do jego doskonalenia na bazie rozpoznanych zagrożeń. Niezmiernie ważnym elementem przeciwdziałania cyberprzestępczości, wynikającym z jej transgraniczności, jest dostosowanie polskiego prawa karnego i procesowego do wymagań UE. Obwiązujący stan prawny nie jest wystarczającym czynnikiem do skutecznych działań zapobiegawczych.

Przyjmujemy z zadowoleniem przyspieszenie prac Rządu nad zagadnieniem cyberterroryzmu, co uwidoczniono w Rządowym Programie Ochrony Cyberprzestrzeni za lata 2008-2011. Jednakże niezmiernie ważne i pilne są również potrzeby:

1) *ratyfikowania przez Polskę konwencji Rady Europy o cyberprzestępczości z 23 listopada 2001 roku, zawartej w Budapeszcie,*
2) *stworzenia ustawowej definicji pojęcia cyberprzestępczości i cyberterroryzmu,*
3) *określenia właściwości poszczególnych służb w odniesieniu do konkretnych zdarzeń w cyberprzestrzeni i ochrony infrastruktury krytycznej zgodnie z ustawą z dnia 26 kwietnia 2007 r. O zarządzaniu kryzysowym (Dz.U. Nr 89, poz. 590),*
4) *powiązania kwestii cyberterroryzmu z tematyką zapobiegania terroryzmowi w ogóle. Okazję do tego stanowią toczące się prace nad projektem ustawy o rozpoznawaniu terroryzmu i przeciwdziałaniu mu. Niezbędny jest postulat przyspieszenia prac nad wspomnianą ustawą,*
5) *realizacji postanowień decyzji ramowej Rady Unii Europejskiej 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.U. L 69/67 z 16.3.2005, s. 1), w której trafnie stwierdza się, że istotne luki i różnice w przepisach prawnych państw członkowskich w tej dziedzinie mogą utrudniać walkę z przestępczością zorganizowaną i terroryzmem oraz mogą komplikować skuteczną współpracę policyjną i sądową w dziedzinie ataków na systemy informatyczne. W związku z tym należy dążyć do uporządkowania i ustanowienia stosowanej w polskim ustawodawstwie terminologii informatycznej, używanej zarówno w kodeksie karnym, jak i w innych ustawach, jak np.: system komputerowy, sieć teleinformatyczna, system informatyczny, system teleinformatyczny. Proponuje się wprowadzenie ujednolicenia terminologii zgodnie z cytowaną decyzją ramową Rady UE oraz ustawą z dnia 4 września 2008 r. O zmianie ustaw w celu ujednolicenia terminologii informatycznej (Dz. U. Nr 171, poz. 1056),*
6) *ujednolicenia definiowania charakteru terrorystycznego czynu zabronionego pomiędzy różnymi ustawami, co jest niezbędnie dla uczynienia zadość zasadzie jednolitości systemu prawnego. Zdefiniowanie aktu terrorystycznego w art. 2 pkt 7 ustawy z dnia 16 listopada 2000 r. O przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych, pochodzących z nielegalnych lub*

nieujawnionych źródeł oraz o przeciwdziałaniu finansowaniu terroryzmu (Dz.U. 2003 Nr 153, poz. 1505 z późn. zm.) ma zupełnie inną budowę normatywną niż definicja przestępstwa o charakterze terrorystycznym ujęta w art. 115 § 20 k.k. Ustawodawca zawęził krąg czynów, mogących mieć charakter aktu terrorystycznego, do wyliczonych we wspomnianym przepisie,

7) *rezygnacji w definicji przestępstwa o charakterze terrorystycznym zapisanej w art. 115 § 20 k.k. z wymogu zagrożenia karą co najmniej pięciu lat pozbawienia wolności,*
8) *wprowadzenia karalności przygotowania do przestępstwa o charakterze terrorystycznym.*

Niezmiernie ważną kwestią jest zabezpieczanie materiału dowodowego dla potrzeb procesu karnego. Wymaga to profesjonalnego przygotowania biegłych, posiadających wiadomości specjalne. Należy uznać, że zabezpieczanie oraz analiza materiału dowodowego w postaci elektronicznej, ze względu na jego cechy, wymaga szczególnej uwagi. Specjaliści, a w szczególności biegli z zakresu informatyki nie zawsze postępują zgodnie z zasadą dobrej praktyki, co sprawia, że na etapie postępowania sądowego możliwe jest podważenie jego wartości. Jednym z powodów takiego stanu rzeczy może być brak wyczerpujących polskich regulacji i ogólnodostępnych wytycznych. W związku z tym uważamy, że koniecznie jest:

1) *wprowadzenie nauczania prawa informatycznego do programu studiów prawniczych oraz informatycznych,*
2) *objęcie edukacją wszystkich tych, którzy ze względu na specyfikę pracy, a w szczególności studentów wydziałów prawa i informatyki, policjantów, prokuratorów, sędziów, a także obrońców, będą coraz częściej mieć do czynienia z zagadnieniem zabezpieczania dowodów elektronicznych,*
3) *opracowanie ogólnodostępnego zbioru procedur ewentualnie wytycznych, którymi mogą kierować się specjaliści oraz biegli posiadający wiadomości specjalne, niezbędne w realizacji zabezpieczania dowodów elektronicznych,*
4) *przygotowanie i ujednolicenie mechanizmów przydatnych do weryfikacji kompetencji biegłych sądowych.*

Uczestnicy I Konferencji apelują do wszystkich użytkowników systemu teleinformatycznego, aby mieli świadomość, że korzystanie z Internetu oprócz korzyści stwarza szereg zagrożeń. Każdy wcześniej czy później zetknie się z nimi, nawet jeśli będą one dla niego niezauważalne. Dlatego ważne jest kształtowanie świadomości istnienia niebezpieczeństw w globalnej sieci oraz wskazywanie konieczności przeciwdziałania cyberzagrożeniom. Świadomość i wiedza na temat sposobów przeciwdziałania i zwalczania zagrożeń stanowią kluczowe elementy przeciwdziałania tym zagrożeniom. Właściwe zachowanie użytkownika sieci może w dużym stopniu zminimalizować ryzyko wynikające z istniejących zagrożeń. Należy podkreślić, że bezpieczeństwo teleinformatyczne nie zależy wyłącznie od działalności wyspecjalizowanych instytucji rządowych, specjalistów do spraw bezpieczeństwa teleinformatycznego, zespołów reagowania na incydenty czy administratorów sieci. Odpowiedzialność za bezpieczeństwo w sieci spoczywa na każdym użytkowniku komputera.

Zagadnienie ochrony infrastruktury przed cyberterroryzmem podjęli również uczestnicy konferencji nt. terroryzmu i cyberterroryzmu, która obyła się w dniach 16 i 17 kwietnia 2009 r. pod egidą Rady Europy. Wyrażamy podobne stanowiska, że działania zapobiegawcze

powinny być bardziej aktywne i wielokierunkowe. Natomiast zadania szczegółowe nałożone ustawowo na organy administracji publicznej, tj. Radę Ministrów, ministrów, wojewodów, starostów, wójtów (burmistrzów, prezydentów miast), zgodnie z przepisami cytowanej ustawy z dnia 26 kwietnia 2007 r. O zarządzaniu kryzysowym mają wykonywać jako ochronę infrastruktury krytycznej. Przedsięwzięcia te winny zostać szczegółowo określone w planach ochrony obiektów tworzonych na poziomie krajowym i wojewódzkim.

W systemowe przeciwdziałania cyberterroryzmowi konieczne wydaje się włączenie do współpracy podmiotów sektora prywatnego. Do grupy tej zaliczyć należy przede wszystkim operatorów i administratorów systemów telekomunikacyjnych i teleinformatycznych. Niezbędne jest jednak precyzyjne określenie obszarów odpowiedzialności oraz sposobów i form współdziałania, w szczególności:

- *współpraca w zakresie zapobiegania i zwalczania wszelkich form przestępczości komputerowej,*
- *wspieranie działań zmierzających do ustalenia sprawców cyberterroryzmu,*
- *przekazywanie istotnych informacji dotyczących poważnych incydentów naruszenia bezpieczeństwa teleinformatycznego, wykrytych we własnych systemach lub sieciach teleinformatycznych, oraz o innych istotnych faktach dla bezpieczeństwa krytycznej infrastruktury teleinformatycznej państwa,*
- *współpraca z organami ścigania w zakresie kontroli użytkowników sieci.*

Z uwagi na fakt, że zagadnienie cyberprzestępczości stanowi novum w systemie prawa oraz wkracza bardzo głęboko w sferę techniczną działania systemów, przetwarzających dane, niezbędne wydaje się wdrożenie kompleksowych zasad edukacji. Prowadzenie systematycznej i profesjonalnej edukacji może istotnie przyczynić się do osiągnięcia pożądanych celów zapobiegawczych.

Równie ważne z punktu widzenia poprawy skuteczności przeciwdziałania cyberterroryzmowi i zwalczania go jest wdrożenie programów badawczych dotyczących wszystkich jego obszarów, uwzględniając symptomatologię i etiologię zjawiska. Zakres badań powinien być szeroki i dotyczyć nie tylko cyberprzestrzeni, będącej obiektem potencjalnych zagrożeń terrorystycznych, ale również społeczeństwa w aspekcie wiktymologicznym.

Uczestnicy Konferencji uznają za wskazane zwrócić się do JM Rektorów o wprowadzenie do programów naukowo-badawczych zagadnień związanych z przeciwdziałaniem cyberterroryzmowi oraz zasad działania i zarządzania w sytuacjach kryzysowych. Wskazane jest również, aby wspomniana tematyka była przedmiotem obieranej tematyki prac dyplomowych i wspomagała osiągnięcia praktyków z organów administracji państwowej i samorządowej.

Efektem pracy uczestników Konferencji jest także publikacja zbiorowa zatytułowana: **Cyberterroryzm – nowe wyzwania XXI wieku** pod redakcją prof. prof. T. Jemioły, J. Kisielnickiego, K. Rajchela, wydana nakładem Wyższej Szkoły Informatyki, Zarządzania i Administracji w Warszawie, Wyższej Szkoły Policji w Szczytnie oraz Wydziału Strategiczno-Obronnego Akademii Obrony Narodowej.

Książka składa się z trzech rozdziałów: „Cyberterroryzm jako zagrożenie bezpieczeństwa w XXI wieku", „Organizacyjne, technologiczne i prawne uwarunkowania cyberterroryzmu", „Bezpieczeństwo informacyjne Polski", w których usystematyzowano 49 artykułów. Publikacja liczy 709 stron, na których oprócz tekstów znalazły się liczne

wykresy, tabele i schematy. Jest również sporo przypisów odsyłających dociekliwych Czytelników do innych druków zwartych i do artykułów prasowych bądź internetowych.

REPORT ON THE SCIENTIFIC CONFERENCE "CYBERTERRORISM – A NEW CHALLENGE OF XXIth CENTURY"

Summary

In the article it was presented the report from the conference whose aim was to discuss the issues connected with cyberterrorism as the highest danger for the contemporary information society. The assessment of the present legal regulations which are applied for the crimes prevention was done.

Złożono w redakcji w grudniu 2009 r.