BEZPIECZEŃSTWO MIĘDZYNARODOWE

Magdalena Stefania WITECKA

WYKORZYSTANIE TECHNOLOGII INFORMACYJNYCH W GENEROWANIU ZAGROŻEŃ ASYMETRYCZNYCH

Wprowadzenie

Klasyczne, „twarde" zagrożenia bezpieczeństwa, choć nie znikają całkowicie, tracą na znaczeniu, ustępując miejsca innym zagrożeniom, w tym zagrożeniom jakościowo nowym, których ewolucja dynamizowana jest przez postęp technologiczny. Przewidzenie miejsca, a w szczególności momentu materializacji zagrożenia stanowi obecnie wielkie wyzwanie dla służb bezpieczeństwa i porządku publicznego. Współcześnie najdotkliwszy cios może pochodzić z wewnątrz terytorium kraju, może zostać zadany znienacka, z użyciem nowatorskich, nieoczekiwanych metod. Zimnowojenna równowaga strachu ustąpiła miejsca asymetrii.

Naprzeciw żyjących w dobrobycie rozwiniętych społeczeństw stają pochodzący z biednego południa agresorzy. Agresorzy ci zbyt długo pozostawali na marginesie powstającej globalnej wioski – nie mając wiele do stracenia rozpoczynają walkę o swoje prawa i udziały w świecie, skutecznie zadając ciosy zachodnim społeczeństwom dzięki wykorzystaniu nietradycyjnych środków walki.

Samo pojęcie asymetrii, tak dobrze odzwierciedlające stan zakłócenia równowagi i otaczającego chaosu – nieobcego współczesnemu światu, stało się w ostatnim dziesięcioleciu niezwykle popularne w naukach wojskowych, głównie za sprawą amerykańskiego środowiska badawczego. Termin ten jest ponadto wyjątkowo chętnie stosowany przez media, jako bardziej „chwytliwy" synonim określenia „nowy". Pojawiły się zatem walka asymetryczna, wojna asymetryczna, strategia asymetryczna, a także zagrożenia asymetryczne. Mianem „asymetryczny" zaczęto nazywać zjawiska od dawna istniejące (np. walka

partyzancka – walka asymetryczna) „Asymetria" zastąpiła „równowagę sił" i „równowagę strachu", stając się współczesnym *signum temporis*.

Równocześnie dynamiczny rozwój technologii informacyjnych, coraz szersza skala ich zastosowania oraz dążenie rozwiniętych państw do stworzenia społeczeństw informacyjnych, spowodowały, iż technologie te stały się źródłem poważnego zagrożenia dla bezpieczeństwa państwa, będąc atrakcyjnym narzędziem negatywnego oddziaływania dla podmiotów stwarzających zagrożenie asymetryczne.

Daje się przy tym zaobserwować zwiększającą się podatność państwa na zagrożenia w obszarze cyberprzestrzeni, związane z wrogim wykorzystaniem technologii informacyjnych. Podstawą cyberprzestrzeni jest Internet, pełniący rolę globalnej platformy wymiany danych i informacji. Informatyzacja administracji państwowej oraz systemów infrastruktury krytycznej państwa z jednej strony usprawnia i ułatwia zarządzanie i ich obsługę, z drugiej, poprzez włączenie do ogólnoświatowej Sieci, naraża na jakościowo nowe zagrożenia, do których stwarzania wrogie podmioty wykorzystują największą zaletę Internetu – wolność anonimową.

Postrzeganie technologii informacyjnych jako narzędzia destruktywnej aktywności

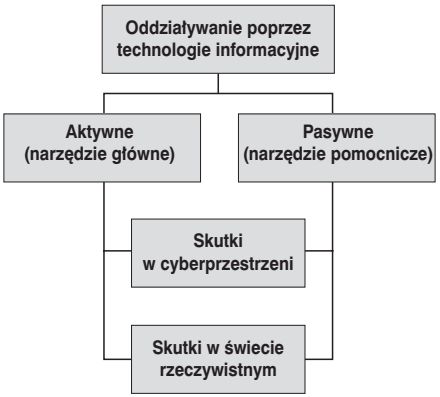
Rolę technologii informacyjnych w generowaniu zagrożeń można postrzegać dwojako (rysunek poniżej). Z jednej strony, technologie informacyjne są wykorzystywane w sposób aktywny, stanowiąc bezpośrednie i podstawowe narzędzie negatywnego oddziaływania na przeciwnika (walki), np. wykorzystywanie możliwości sieci Internet do wyrządzania szkód przeciwnikowi. Z drugiej strony, technologie informacyjne pełnią rolę wspomagającą (pasywną), będąc wykorzystywane w operacjach poszerzających możliwości operacyjne i efektywność działań podmiotów oraz jako *force multiplier*, wzmacniając efekt posunięć innego rodzaju albo zwiększając wartość posiadanych zasobów[1], np. w zapewnieniu łączności, komunikacji, wspomaganiu planowania działań, wymiany i pozyskiwania informacji, rekrutacji, dowodzenia, prowadzeniu akcji propagandowych i informacyjnych itd.

Do negatywnego pasywnego oddziaływania IT można również zaliczyć fizyczne uszkodzenie elementów systemów teleinformatycznych. Obie formy

[1] M. Madej, *Zagrożenia asymetryczne bezpieczeństwa*…, s. 335.

wykorzystania IT – aktywna i pasywna – prowadzą do szkód zarówno w systemach teleinformatycznych atakowanego podmiotu (np. uszkodzenie bazy danych, nielegalne pozyskanie danych), jak i do zniszczeń poza cyberprzestrzenią (np. zakłócenie pracy elementów infrastruktury krytycznej, prowadzące do ich awarii).

Sposoby szkodliwego oddziaływania poprzez technologie informacyjne oraz obszary skutków tego oddziaływania



Źródło: opracowanie własne.

Formy celowego, szkodliwego użycia technologii informacyjnych w kontekście zagrożeń asymetrycznych bezpieczeństwa państwa, zależą również od sposobu pojmowania samej kategorii zagrożeń asymetrycznych. Zgodnie z ujęciem szerokim (wojskowym), asymetria zagrożeń jest orzekana na podstawie odmienności jakościowej potencjałów przeciwników. To ogólne sformułowanie, ze względu na swoją pojemność, pozwala na objęcie różnorodnych, wciąż powstających definicji zagrożeń asymetrycznych. Brak jest jednak ustalonej, jednoznacznej i pełnej definicji tego terminu, którym powszechnie określa się nowe (niemieszczące się w paradygmacie zagrożeń tradycyjnych) zagrożenia bezpieczeństwa państwa, przejawiające się zastosowaniem odmiennych, nieklasycznych metod i narzędzi walki. Dla różnych osób termin ten może oznaczać co innego, ponieważ obierane są różne, subiektywne punkty odniesienia. Ze względu na względność asymetrii, spowodowaną dowolnością w określaniu osi symetrii, tak rozumiany termin zagrożeń asymetrycznych jest nieprecyzyjny, a posługiwanie się nim – utrudnione.

Również kwestia uznania technologii informacyjnych za narzędzie walki w tym ujęciu zagrożeń asymetrycznych nie jest jednoznaczna. Jakościowa i ilościowa odmienność całego potencjału Stanów Zjednoczonych sprawia, iż kraj ten jest przeciwnikiem asymetrycznym wobec każdego innego podmiotu, zarówno państwa, jak i podmiotu pozapaństwowego. Obierając z kolei za oś symetrii poszczególne środki walki, np. broń atomową, zagrożenie asymetryczne stwarzają podmioty nią dysponujące wobec podmiotów nieposiadających arsenału nuklearnego.

Podobnie w przypadku wykorzystania technologii informacyjnych jako środka walki – wrogie użycie technologii informacyjnych jest metodą asymetryczną, jeśli przeciwnik takiej nie stosuje. Takie zagrożenie asymetryczne mogłoby mieć miejsce, jeśli państwo posiadające (oficjalnie lub nieoficjalnie) siły przeznaczone do walki w cyberprzestrzeni (np. Stany Zjednoczone, Rosja czy Chiny) zaatakowałoby państwo nimi nie dysponujące (np. Polska). Z drugiej strony, zastosowanie IT nie byłoby już metodą asymetryczną (a w konsekwencji nie należałoby do zagrożeń asymetrycznych) jeśli przeciwstawić Stany Zjednoczone i Chiny czy Rosję.

Kontynuując rozpatrywanie ujęcia szerokiego, można wreszcie uznać, że Stany Zjednoczone stwarzają zagrożenie asymetryczne przykładowo dla Iraku (chociażby pierwsza wojna w Zatoce Perskiej) bądź organizacji terrorystycznych działających w górach Afganistanu, obierając za punkt odniesienia wykorzystanie technologii informacyjnych jako środka wspomagającego walkę – zaawansowanych technologicznie środków rozpoznania i wywiadu, technologii naprowadzanych pocisków itp. Warto również podkreślić, iż współcześnie praktycznie każdy podmiot, posiadający odpowiednie dla danych warunków środki finansowe, ma dostęp do technologii informacyjnych i może posłużyć się nimi do negatywnego oddziaływania na przeciwnika. W krajach rozwiniętych, dostęp do technologii informacyjnych jest łatwy, a niekiedy wręcz bezpłatny. Na terenach o słabo rozwiniętej infrastrukturze teleinformatycznej korzystanie z technologii informacyjnych również jest możliwe (np. telefonia satelitarna), choć bardziej kosztowne.

Dostęp do Internetu jest teoretycznie możliwy z każdego miejsca na Ziemi. Operacje prowadzone w cyberprzestrzeni są uniezależnione od ograniczeń przestrzennych. Choć państwa mogą starać się kontrolować dostęp do Sieci (np. Chiny) i monitorują ruch w Internecie (np. projekt Echelon), do swobodnego poruszania się w Sieci każdy użytkownik, posiadający wystarczającą wiedzę i umiejętności, może prowadzić dowolną aktywność. Do wykorzystania technologii informacyjnych w stwarzaniu zagrożenia potrzebny jest dostęp do

odpowiedniego w danych warunkach sprzętu (którego koszt zakupu jest w krajach rozwiniętych niewielki) i podstawowe umiejętności użytkownika. Sposób wykorzystania urządzeń zależy od intencji użytkownika, zatem potencjalnie każdy podmiot może stwarzać zagrożenie poprzez celowe użycie (groźbę użycia) technologii informacyjnych.

W świetle zarysowanych powyżej trudności w posługiwaniu się terminem zagrożeń asymetrycznych w ujęciu szerokim, opierającym asymetrię na odmienności metod i narzędzi walki, postrzeganie wykorzystania technologii informacyjnych jako narzędzia walki staje się wysoce subiektywne, utrudniając jednoznaczne rozstrzygnięcie, czy technologie informacyjne mogą być, czy też nie, narzędziem wykorzystywanym do stwarzania zagrożenia asymetrycznego.

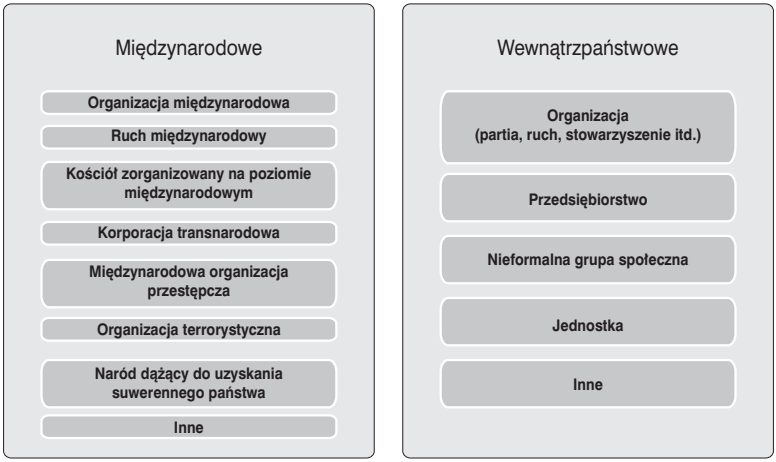
Kwestia celowego wykorzystania technologii informacyjnych w kreowaniu zagrożeń asymetrycznych jest dużo mniej problematyczna w przypadku wąskiego rozumienia zagrożeń asymetrycznych. W ujęciu wąskim (politologicznym), asymetria zagrożeń wynika z odmienności typu przeciwstawianych sobie podmiotów. Zagrożenie asymetryczne bezpieczeństwa państwa jest więc zagrożeniem powodowanym przez podmiot pozapaństwowy. Odmienność sił i środków (będąca podstawą szerokiego, wojskowego ujęcia zagrożeń asymetrycznych) wynika natomiast z odmienności typów przeciwstawianych podmiotów, z których każdy „z natury" dysponuje jakościowo i ilościowo innym potencjałem. Asymetria metod i narzędzi wynika z asymetrii podmiotów. Metody, siły i narzędzia dostępne dla podmiotów pozapaństwowych, jak np. organizacji terrorystycznych, zdecydowanie różnią się od potencjału, jakim dysponuje państwo. Aktywność przestępców, a wśród nich terrorystów, *ex definitione* wiąże się z operowaniem metodami i narzędziami, których użytek przez państwo, instytucję opartą na prawie, jest teoretycznie niedopuszczalny, zatem nadanie cechy asymetryczności zagrożeniom państwa, generowanym przez organizacje przestępcze i terrorystyczne, jest w pełni uzasadnione.

Technologie informacyjne są jednym z narzędzi, jakie podmioty pozapaństwowe mogą wykorzystywać w celowym, negatywnym oddziaływaniu na państwo. Wobec ograniczonych sił i środków podmiotów pozapaństwowych, technologie informacyjne są narzędziem walki osiągalnym dla każdego potencjalnego agresora. Formy szkodliwego użycia IT są różnorodne. Za pomocą technologii informacyjnej prowadzona jest wojna (walka) informacyjna, wykorzystanie IT stanowi również podstawę cyberterroryzmu, a hacking, cracking i tworzenie szkodliwych programów są jednymi z najpopularniejszych form szkodliwej i destrukcyjnej aktywności.

Typy podmiotów w obszarze zagrożeń asymetrycznych

Po przyjęciu założenia, że obiektem zagrożenia asymetrycznego jest państwo, asymetrycznym wobec państwa podmiotem będą podmioty pozapaństwowe. Kategoria podmiotów pozapaństwowych jest niezwykle ogólna, a przez to również pojemna. Zaliczyć do niej można pozapaństwowych uczestników stosunków międzynarodowych, a także wiele innych typów podmiotów, w tym podmioty funkcjonujące na poziomie lokalnym – wewnątrzpaństwowe (rys. poniżej).

Wybrane typy podmiotów stwarzających potencjalne zagrożenie asymetryczne bezpieczeństwa państwa



Źródło: opracowanie własne.

Do niepaństwowych aktorów środowiska międzynarodowego zaliczyć można m.in.: narody dążące do uzyskania niepodległości i utworzenia własnych państw, korporacje transnarodowe, organizacje międzynarodowe, kościoły zorganizowane na poziomie międzynarodowym, ruchy międzynarodowe, transnarodowe grupy przestępcze i organizacje terrorystyczne[2].

[2] *Mały słownik stosunków międzynarodowych*, red. G. Michałowska, Wyd. Szkolne i Pedagogiczne, Warszawa 1996, s. 258.

Starania narodów dążących do uzyskania własnego suwerennego terytorium (państwa) cechuje dualizm postrzegania ich aktywności. Współcześnie, uzyskanie terytorium przez jeden podmiot jest jednoznaczne z utratą terytorium przez dane państwo (państwa). Jeżeli próby uzyskania terytorium w drodze pokojowej (negocjacji z państwami) nie przynoszą rezultatów, naród może wkroczyć na drogę siłową, uciekając się do aktów przemocy, asymetrycznych metod i narzędzi walki (w stosunku do metod, którymi dysponuje państwo – przeciwnik), a także – do terroryzmu. Z jednej strony walczący postrzegani są jako powstańcy, a ich działalność – jako narodowowyzwoleńcza.

Z innego punktu widzenia, dla państwa, którego stabilność wewnętrzna i integralność terytorium są zagrożone, działalność walczących jest postrzegana jako separatystyczna i terrorystyczna, a oni sami – jako rebelianci lub terroryści. Opinia społeczności międzynarodowej nie jest miarodajnym punktem odniesienia, ponieważ jest względna i kształtowana wedle interesów mocarstw. Przykładem narodu, którego walka o niepodległość kraju jest postrzegania dwojako, jest naród czeczeński, którego bojownicy są postrzegani przez Federację Rosyjską za terrorystów.

Działalność w granicach prawa przedsiębiorstw transnarodowych, kolejnego typu podmiotu pozapaństwowego, wynika i jest wymuszana przez międzynarodowe i lokalne prawo umowne oraz zwyczajowe, przez standardy przyjęte w międzynarodowym środowisku gospodarczym, a także przez rynek. Skutkiem ujawnienia niezgodnych z prawem działań przedsiębiorstw są dotkliwe straty finansowe (głównie wynikające z kar nakładanych przez organy państwowe) oraz wizerunkowe. Zniszczenie reputacji i wizerunku korporacji może być bezpowrotne, a ciężar kar finansowych może doprowadzić firmę do bankructwa. Mimo to, działalność przedsiębiorstwa, mająca na celu m.in. powiększanie zysków, poszerzanie rynku zbytu i ograniczenia kosztów, nie zawsze jest skorelowana z celami państwa, także z troską o jego bezpieczeństwo. Podmioty gospodarcze, poprzez lobbing, wpływają na procesy polityczne w państwie we wszystkich obszarach jego funkcjonowania, kształtując otoczenie w sposób korzystny dla siebie. Opanowanie rynku oraz jego uzależnienie pogłębiają wpływ korporacji transnarodowej na państwo.

Na pewien szczególny kontekst stwarzania zagrożeń asymetrycznych przez przedsiębiorstwa zwracają uwagę Piotr Gawliczek i Jacek Pawłowski. Zauważają oni, iż coraz większym nasileniem występuje trend przekazywania obsługi pewnych elementów podsystemu militarnego cywilnym podmiotom gospodarczym (np. ochrona i konserwacja wojskowych systemów informatycznych, ochrona fizyczna obiektów wojskowych). Według autorów, zjawisko to niesie dwojakie

zagrożenie – z jednej strony oznacza rezygnację państwa z monopolu na dysponowanie potencjałem wojennym, a z drugiej strony świadczy o być może lepszym przygotowaniu sektora cywilnego do prowadzenia walki w jej nowym wymiarze. Duże monopole międzynarodowe mogą stanowić zagrożenie dla suwerenności państwowej w wymiarze gospodarczym i politycznym[3].

Zauważone przez Piotra Gawliczka i Jacka Pawłowskiego współczesne trendy polityczno-gospodarcze, Naomi Klein, autorka *Doktryny szoku*, określa jako „kapitalizm katastrofowy". Autorka podkreśla znaczenie kryzysów (np. powodzi, wojen) dla prywatnych przedsiębiorstw. Kryzys, będący momentem przełomowym, uniemożliwiającym pełny powrót do stanu sprzed wystąpienia sytuacji kryzysowej, dzięki zaburzeniu (zburzeniu) dotychczasowego porządku, ułatwia władzom wprowadzanie radykalnych reform w państwie. Doznany szok i bezwład, w jakim przez pewien czas trwa społeczeństwo, umożliwia przeprowadzenie liberalizacji gospodarki w sposób gwałtowny, proponowany przez ekonomistę Miltona Friedmana, propagatora pełnej liberalizacji rynku. Wystąpienie kryzysu w państwie, czy też prowadzenie wojny poza jego granicami są wykorzystywane przez przedsiębiorstwa do opanowania nowych rynków i gwałtownego zwiększenia zysków[4]. Ze względu na to, iż ogólnopaństwowy kryzys stanowi poważny bodziec rozwoju pewnych sektorów gospodarki (np. produkcji i usług związanych z bezpieczeństwem), może dochodzić do sytuacji, w których przedsiębiorstwa dopuszczać będą do wystąpienia sytuacji kryzysowych w państwie lub będą je prowokować.

Korporacje transnarodowe mogą stwarzać zagrożenie asymetryczne również poprzez nieoficjalnie powiązania z innymi podmiotami je stwarzającymi

---

[3] Zob. P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*..., s. 52.

[4] Szok społeczny po wydarzeniach z 11 września 2001 r. umożliwił administracji George'a W. Busha pobudzenie znajdującej się w stagnacji amerykańskiej gospodarki oraz realizację postulatów potężnego lobby sektorów zbrojeniowego i energetycznego w formie globalnej wojny toczonej „[…] na wszystkich frontach przez prywatne firmy, które za swój wkład w wojnę z terroryzmem otrzymują pieniądze z budżetu federalnego". Naomi Klein podaje, iż rząd amerykański zawarł w 2003 r. 3512 kontraktów z prywatnymi firmami świadczącymi usługi zapewniania bezpieczeństwa, natomiast w ciągu kolejnych niecałych dwóch lat było tych kontraktów 115 000. Autorka podaje, iż amerykański przemysł zajmujący się bezpieczeństwem krajowym wart jest obecnie 200 mld $. Prowadzenie działań zbrojnych poza granicami kraju przynosi korzyści producentom sprzętu wojskowego oraz przedsiębiorstwom świadczącym usługi logistyczne i zaopatrzeniowe; szerzej: N. Klein, *Doktryna szoku*, Warszawskie Wyd. Literackie MUZA SA, Warszawa 2009.

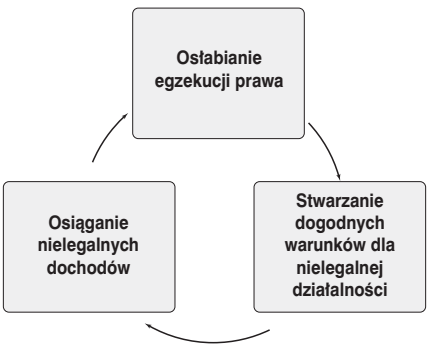
– organizacjami przestępczymi (np. „piorąc" ich pieniądze) lub terrorystycznymi (np. finansując działalność terrorystyczną). Przedsiębiorstwa transnarodowe powiązane z rządami państw– przeciwników mogą zostać wykorzystane przez wrogie państwo jako narzędzie negatywnego oddziaływania na bezpieczeństwo państwa (np. funkcjonujące na wielu rynkach europejskich i azjatyckich przedsiębiorstwo Gazprom, które w związku z uzależnieniem rynków od dostaw rosyjskiego gazu niekiedy nazywane jest „bronią" Federacji Rosyjskiej). Wobec powyższego, trudno jednoznacznie stwierdzić, czy korporacje transnarodowe mogą samodzielnie stwarzać zagrożenie asymetryczne.

Rozpatrywanie działań przedsiębiorstwa w kontekście zagrożeń asymetrycznych ułatwia ewentualne istnienie powiązań korporacji transnarodowej z transnarodowymi organizacjami przestępczymi lub z organizacjami terrorystycznymi. Przykładem jest sposób finansowania działalności Al-Kaidy, m.in. z dochodów międzynarodowych firm lub japońskiej sekty Najwyższa Prawda, która założyła popularną sieć tanich sklepów komputerowych.

W przypadku kościołów zorganizowanych na poziomie międzynarodowym, zagrożenie dla bezpieczeństwa państwa, także asymetryczne, generować mogą np. fundamentalistyczne lub ekstremistyczne odłamy czy sekty. Odłamy takie mogą z czasem przekształcić się w organizacje terrorystyczne. Obecnie najpoważniejszym zagrożeniem są fundamentalistyczne odłamy islamu, których część członków prowadzi działalność terrorystyczną.

Zagrożenie dla bezpieczeństwa państwa, stwarzane przez organizacje przestępcze, można uznać za asymetryczne, traktując jako punkt odniesienia

Trzy płaszczyzny negatywnego oddziaływania na bezpieczeństwo państwa przez organizacje przestępcze



Źródło: opracowanie własne.

charakter podmiotu. Marek Madej uważa, że transnarodowe grupy przestępcze stwarzają zagrożenie asymetryczne, również ze względu na przełamanie przez ten podmiot monopolu państwa na stosowanie siły oraz ze względu na pogłębiające się związki między organizacjami przestępczymi, a innymi podmiotami pozapaństwowymi stanowiącymi zagrożenie asymetryczne (patrz: zagadnienie 1.1.3). Wprawdzie organizacje przestępcze są podmiotem innym niż państwo, jednak należy rozważyć, czy stwarzanie zagrożenia dla bezpieczeństwa państwa, mimo iż nie jest to zasadniczym celem działania organizacji przestępczych, jest wystarczającą przesłanką do określenia transnarodowej przestępczości zorganizowanej czy innych podmiotów przestępczych jako podmiotów stwarzających zagrożenie asymetryczne. Wątpliwość ta jest jednym z przykładów trudności w posługiwaniu się terminem zagrożeń asymetrycznych, wynikających ze względności asymetrii.

Podmiotem, którego zidentyfikowanie jako stwarzającego zagrożenie asymetryczne przysparza najmniej wątpliwości, jest organizacja terrorystyczna. W tym przypadku asymetrię można wykazać na podstawie zarówno odmienności podmiotów, jak i metod, sił oraz narzędzi walki. Terroryzm jest specyficzną kategorią przestępstwa, która obejmuje „[…] przestępstwa popełniane z premedytacją przez pojedyncze osoby lub grupy przeciwko jednemu lub większej liczbie krajów, ich instytucjom lub obywatelom, w celu zastraszenia ich i poważnej zmiany lub zniszczenia politycznych, gospodarczych albo społecznych struktur kraju”[5].

Organizacje terrorystyczne i przestępcze cechuje podobieństwo, bowiem obie stanowią formy przestępczości grupowej, operują specyficznymi formami terroru i prowadzą proceder „prania pieniędzy”[6]. Różnią się między sobą przede wszystkim ze względu na cel podejmowanych działań, bowiem organizacja terrorystyczna dąży do zmiany określonego porządku prawnego – korzyści w obszarze politycznym, ideowym lub religijnym, a nie finansowym. Różnica istnieje również w odbiorze społecznym działalności obu typów podmiotów. O ile działalność grup przestępczych, poza nielicznymi

---

[5] Definicja pochodząca z art. 3 *Decyzji Ramowej Rady o zwalczaniu terroryzmu* Komisji Europejskej z 2001 r.; *W ramach UE*, 25.09.2003 [online]. Terroryzm.com 2010 [dostęp: 11.04.2010]. Dostępny w World Wide Web: http://www.terroryzm.com/article/183/W-ramach-UE.html.

[6] Zob. M. K. Makutynowicz, *Kwerenda powiązania przestępczości zorganizowanej i terroryzmu*, s. 60 [online]. Centralny Ośrodek Szkolenia Straży Granicznej 2010 [dostęp: 11.04.2010]. Dostępny w World Wide Web: http://www.cos.strazgraniczna.pl/downloads/pliki/biuletyn_biezacy/42009/8.pdf.

wyjątkami, jest negatywnie odbierana społecznie, o tyle organizacje terrorystyczne często cieszą się społecznym poparciem, bowiem walczą w imię „wyższych wartości" (np. wyzwolenia narodu, obrony religii i tradycji, ochrony środowiska itd.).

Obecnie, na Kaukazie oraz w rejonie Bliskiego i Środkowego Wschodu obserwowane jest zbliżenie obu typów podmiotów na dwóch płaszczyznach: instrumentalnej – gdy przestępczość zorganizowana jest jedną z form finansowania działalności organizacji terrorystycznych – oraz współpracy – gdy grupy przestępcze odpłatnie dostarczają organizacjom terrorystycznym środki do prowadzenia działalności[7]. „Obecnie organizacje terrorystyczne stopniowo zacieśniają współpracę z przestępczością zorganizowaną, która przekazuje swoje doświadczenia w zakresie prania brudnych pieniędzy i tworzenia legalnych przykrywek działalności. Odnotowuje się również pojedyncze sygnały o współpracy w zakresie przemytu broni i amunicji oraz narkotyków […]. Należy jednak zauważyć, że znaczna część największych międzynarodowych organizacji terrorystycznych unika bezpośredniego zaangażowania w działalność kryminalną. Zaangażowanie takie zwiększa bowiem możliwość wykrycia przez służby specjalne lub policyjne. Dana „grupa terrorystyczna" jest skazana na pozyskiwanie środków finansowych z działalności kryminalnej wtedy, gdy nie posiada ich wystarczająco z innych źródeł, takich jak na przykład: ze składek stowarzyszeń religijnych, sponsorowania przez przedsiębiorców, banki kontrolowane przez państwa popierające terroryzm"[8].

Rozważania dotyczące charakteru podmiotów mogących stwarzać zagrożenie asymetryczne, prowadzą do przynajmniej czterech wniosków.

Po pierwsze, każdy podmiot pozapaństwowy stanowi potencjalne zagrożenie dla państwa, bowiem natura ludzka jest nieprzewidywalna. Na zwiększone obecnie prawdopodobieństwo pojawienia się nieoczekiwanego zagrożenia ze strony danego podmiotu wpływa turbulentność i szczególna nieprzewidywalność współczesnego świata. Wskutek zmniejszającej się skuteczności metod i narzędzi symetrycznych, terroryści oraz inne podmioty godzące w bezpieczeństwo państwa poszukiwać będą nowych sposobów negatywnego oddziaływania. Szkodliwe i destrukcyjne oddziaływanie może materializować się w różnych obszarach funkcjonowania państwa i społeczeństwa, będących domeną podmiotów pozapaństwowych innego typu, o działalności pozornie niestwarzającej zagrożenia. Trudno wyobrazić sobie skalę skutków celowego,

[7] Zob. tamże, s. 61.

[8] Tamże.

szkodliwego dla państwa i jego społeczeństwa działania korporacji. Jakie skutki przyniesie przejęcie firm bezpośrednio związanych z infrastrukturą krytyczną państwa? A jeśli będzie to koncern medialny, dysponujący prasą, telewizją i Internetem? Informacja jest rdzeniem społeczeństwa informacyjnego, a cios z jej wykorzystaniem może być wyjątkowo dotkliwy. Wywołanie konfliktu czy wojny między państwami – sojusznikami poprzez manipulowanie informacją niebyłoby trudnym zadaniem. Skuteczność celowego negatywnego oddziaływania pozapaństwowych agresorów zapewnia nieprzewidywalność, zaskoczenie i asymetria ich strategii. Czarnych scenariuszy, które wydają się niemożliwe do zrealizowania jest wiele, a jedynym ograniczeniem w ich formułowaniu jest ludzka wyobraźnia.

Drugi wniosek, płynący z rozważań na temat charakteru podmiotów stwarzających zagrożenia asymetryczne jest następujący: zagrożenie generowane przez podmiot pozapaństwowy z założenia jest asymetryczne, gdyż asymetria wynika w tej sytuacji z jakościowej różnicy przeciwstawianych sobie podmiotów: państwo – organizacja terrorystyczna, państwo – przedsiębiorstwo, państwo – haker itd.

Po trzecie, w wyniku podjęcia przez podmiot pozapaństwowy określonych działań, powodujących powstanie zagrożenia dla bezpieczeństwa państwa ze strony tego podmiotu, może nastąpić zmiana postrzeganej jego kategorii. Przestępcy, terroryści i ich organizacje z definicji działają poza prawem. Jeżeli jednak działający legalnie podmiot pozapaństwowy zacznie zagrażać bezpieczeństwu państwa, a odbierane przez państwo zagrożenie osiągnie odpowiednio wysoki poziom, podmiot ten może zostać uznany np. za organizację terrorystyczną (np. organizacja religijna, wskutek określonych działań, zostanie uznana za organizację terrorystyczną, korporacja – za organizację przestępczą).

Czwarty wniosek dotyczy powiązań między grupami przestępczymi i organizacjami terrorystycznymi, a innymi podmiotami pozapaństwowymi. Działalność tych pierwszych może być finansowana ze środków finansowych pochodzących z legalnych źródeł – przedsiębiorstw, stowarzyszeń, fundacji, banków itd., co sprawia trudności w ocenie, czy dany podmiot pozapaństwowy stwarzać może zagrożenie asymetryczne. Działalność organizacji terrorystycznych może być również finansowana z działalności przestępczej.

Wykorzystanie technologii informacyjnych w generowaniu zagrożeń asymetrycznych

Dotychczasowe akty materializacji zagrożeń spowodowanych celowym użyciem technologii informacyjnych można zaklasyfikować zarówno do zagrożeń asymetrycznych rozumianych wąsko, jak i szeroko. Dokonywane są przez podmioty różnego typu, również na zlecenie rządów państw, choć władze żadnego z krajów nie przyznają się do dokonanych ataków. Zagrożenie bezpieczeństwa cyberprzestrzeni ze strony państw dysponujących cyberarmią złożoną z hakerów jest o tyle poważne, iż państwo ma możliwość dokonania ataku jednoczesnego, zmasowanego i w pełni skoordynowanego, co wybitnie zwiększa zagrożenie. Atakom cybernetycznym dokonywanym przez państwo mogą towarzyszyć inne formy negatywnego oddziaływania na przeciwnika, w tym walka informacyjna w wymiarze propagandowym oraz tradycyjne działania sił zbrojnych.

Przykładem takich działań jest wojna w Gruzji w 2008 r. Działania wojenne (*nota bene* zainicjowane przez to państwo) były poprzedzone długotrwałymi rosyjskimi atakami na cyberprzestrzeń Gruzji[9]. Jako dysponujące cyber-bronią[10] (ang. *cyberweapon*), zostało do tej pory zidentyfikowanych przynajmniej pięć państw – Stany Zjednoczone, Chiny, Rosja, Izrael i Francja. Kraje te biorą udział w wyścigu zbrojeń w cyberprzestrzeni, w którym uczestniczy minimum 20 państw, rozwijając możliwości wojny i walki w cyberprzestrzeni oraz cyfrowych form działań wywiadowczych[11].

---

[9] Zaatakowanych zostało 20 stron, w tym m.in. witryna gruzińskiego ministerstwa spraw zagranicznych oraz serwisy informacyjne (w tym anglojęzyczny civil.ge), których odblokowanie zajęło gruzińskim informatykom tydzień; zob. K. Głowacki, *Cyberzagrożenie* [online]. Portal spraw zagranicznych, 8.12.2009 [dostęp: 1.05.2010]. Dostępny w World Wide Web: http://www.psz.pl/tekst-25795/Krzysztof-Glowacki-Cyberzagrozenie.

[10] Do cyber-broni zaliczane są: elektroniczne środki zakłócające (*electronic countermeasures*, ECM), osłony przed atakiem elektronicznym, wabiki na pociski naprowadzane na podczerwień (*infrared decoys*), reflektory kątowe (*angle reflectors*), urządzenia fałszujące sygnał o celu (*false-target generators*), rootkity, szkodliwy kod, broń o ukierunkowanej energii (*directed energy weapons, DEWs*), trojany, programy szpiegowskie, back-door'y, programy zwane autonomiczną mobilną cyber-bronią (*autonomous mobile cyber weapons*), keyloggery, botnety, wirusy, robaki i inne techniki nadużycia; *Department of Cyber Defense. An organization who's time has come!* [online]. Technolytics Institute 2007 [dostęp: 29.04.2010]. Dostępny w World Wide Web: http://www.technolytics.com/Dept_of_Cyber_Defense.pdf, tłumaczenie własne.

[11] S. Writers, *China, US, Russia in cyber arms race, says net security chief* [online]. Spacewar, 29.01.2010 [dostęp: 29.04.2010]. Dostępny w World Wide Web:

Rosnące wykorzystanie systemów teleinformatycznych przyczynia się do wzrostu uzależnienia państw wysoko rozwiniętych od ich poprawnego i niezakłóconego działania[12]. Agresja na cyberprzestrzeń państwa wynika z przyjęcia przez agresora koncepcji „atakowania powiązań"[13] i umożliwia doprowadzenie państwa do stanu chaosu wewnętrznego bez masowych zniszczeń fizycznych, towarzyszącym tradycyjnym operacjom wojskowym, bowiem atakowane są nie same obiekty, lecz istniejące między nimi powiązania. Ocenia się, iż obecnie najbardziej podatne na atak są najwyżej rozwinięte kraje obszaru transatlantyckiego[14], co wynika z wysokiego stopnia rozwoju i powiązania technologii informacyjnych z infrastrukturą państwa.

Najgłośniejszym z dotychczasowych przypadków ataku na cyberprzestrzeń państwa jest rosyjski cyberatak na Estonię w 2007 r., często określany jako pierwsza wojna w cyberprzestrzeni (domniemywa się, iż atak został przeprowadzony na zlecenie rządu Federacji Rosyjskiej)[15]. Ze względu na wysoki stopień informatyzacji Estonii, zmasowany atak na systemy informacyjne centralnych organów państwa estońskiego oraz na strony gazet, systemy bankowe i sieć wewnętrzną policji, spowodował paraliż administracji państwowej, odcięcie mieszkańców od zewnętrznych informacji i dostępu do pieniędzy. Cyberatak doprowadził do sytuacji, w której estońskie władze rozważały wystąpienie o wsparcie NATO, poprzez powołanie się na art. 5 Traktatu Waszyngtońskiego (do czego ostatecznie nie doszło). Również hakerzy rosyjscy, prawdopodobnie działający na zlecenie dokonali w 2009 r. zorganizowanego ataku na niektóre polskie serwery rządowe (atak został udaremniony przez Agencję Bezpieczeństwa Wewnętrznego).

Warto zwrócić przy tym uwagę na wzrost podatności cyberprzestrzeni RP na cyberataki, wynikający ze znacznego już stopnia informatyzacji kraju, w tym administracji publicznej. Zagrożona jest zarówno cywilna, jak i militarna sfera funkcjonowania społeczeństwa. Jak zauważają Piotr Gawliczek i Jacek Pawłowski, w siłach zbrojnych państw rozwiniętych „wykonanie precyzyjnych uderzeń ogniowych oparto […] na całkowicie skomputeryzowanym uzbrojeniu,

---

http://www.spacewar.com/reports/China_US_Russia_ in_cyber_arms_race_says_net_security_chief_999.html.

[12] Zob. J. Adamski, *Nowe technologie w służbie terrorystów*, Wyd. TRIO, Warszawa 2007, s. 91.

[13] Zob. P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne…*, s. 52.

[14] Zob. M. Madej, *Zagrożenia asymetryczne bezpieczeństwa…*, s. 350.

[15] Przyczyną cyberataku był konflikt dyplomatyczny między Rosją a Estonią wywołany usunięciem pomnika żołnierzy radzieckich w centrum Tallinia.

a poczta elektroniczna weszła na trwałe do systemów łączności wojskowej […] nawet funkcjonowanie logistyki stało się całkowicie zależne od techniki informatycznej”[16].

W 2009 r. kontrwywiad Stanów Zjednoczonych ujawił, iż amerykańskie sieci energetyczne od dawna są penetrowane przez zagranicznych szpiegów, działających prawdopodobnie na korzyść Rosji i Chin. W infrastrukturze informatycznej amerykańskich sieci energetycznych instalowane jest szkodliwe oprogramowanie, zbierające i przesyłające informacje o ich topografii, które mogą zostać wykorzystane do planowania ataku. Wrażliwość sieci energetycznej wynika z pośredniego jej podłączenia do Internetu (poprzez systemy obsługujących ją przedsiębiorstw)[17]. W 2009 r. rozprzestrzeniane z chińskich rządowych serwerów złośliwe oprogramowanie zaatakowało serwery Google i 30 innych firm, wykorzystując luki w przeglądarce Internet Explorer i oprogramowaniu Adobe[18]. Atak chińskich hakerów na Google i jego polityczne konsekwencje (napięcia w stosunkach amerykańsko – chińskich) są przykładem wrogiego oddziaływania na państwo nie poprzez atak na infrastrukturę państwową, lecz na prywatne i komercyjne podmioty.

Cyberatak na Google był jednym z rosnącej od początku 2009 r. liczby ataków. Zgodnie z wynikami badań przeprowadzonych przez producenta oprogramowania antywirusowego McAfee, obecnie nastąpił pięciokrotny wzrost liczby szkodliwego oprogramowania względem 2008 r., a zdaniem 60% respondentów (menedżerów IT), rządy obcych państw dokonywały infiltracji zasobów cyfrowych firm, w których są zatrudnieni. W styczniu 2010 r. MI5 oskarżyło Chiny o wręczanie brytyjskim przedsiębiorcom „podarunków” (kamer cyfrowych, pendrive'ów), zawierających szkodliwe, szpiegowskie oprogramowanie w celu kradzieży tajemnic gospodarczych[19]. Można stwierdzić, że współcześnie przyczyną działań podmiotów stwarzające zagrożenie asymetryczne bezpieczeństwa państwa są nie tylko pobudki ideologiczne i polityczne, lecz również dążenie do zdobycia przewagi informacyjnej, a dzięki niej, również przewagi gospodarczej.

---

[16] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*..., s. 42.

[17] M. Błoński, *Zarazili sieci energetyczne* [online]. Interia.pl, 9.04.2009 [dostęp: 1.05.2010]. Dostępny w World Wide Web: http://nt.interia.pl/internet/bezpieczenstwo/news/zarazili-sieci-energetyczne,1288603.

[18] *„NYT” o ataku na Google* [online]. PAP, 20.04.2010 [dostęp: 30.04.2010]. Dostępny w World Wide Web: http://info.wiara.pl/doc/506234.NYT-o-ataku-na-Google.

[19] S. Writers, *China, US, Russia in cyber arms…*

Pojedynczy człowiek, jednostka, stanowi zarówno podstawowy element społeczeństwa, jak i najprostszy spośród podmiotów mogących stwarzać zagrożenie dla bezpieczeństwa państwa. Uzbrojona w dostęp do infrastruktury, wiedzę i motywację jednostka jest w stanie poważnie zagrozić bezpieczeństwu państwa. Spośród ogromnej liczby ataków hakerów na infrastrukturę teleinformatyczną państwa warto przytoczyć włamanie Jonathana Jamesa w 1999 r. do systemów NASA oraz Defense Threat Reduction Agency (odpowiedzialnej za redukcję zagrożeń Stanów Zjednoczonych i ich sojuszników różnymi typami broni) oraz serię ataków na serwery m.in. Yahoo!, Amazon.com, CNN, Dell i eBay, dokonaną przez Michaela Calce'a w 2000 r[20]. Ukrywający się pod pseudonimami M0r0n i Nightman hakerzy z Pakistanu wykorzystują Internet jako narzędzie walki w imię islamistycznej ideologii, dokonując od 2008 r. ataków na strony hinduskich bibliotek, izraelskich przedsiębiorstw, a także Amerykańsko-Izraelskiego Komitetu Spraw Publicznych. Trudno jest jednoznacznie rozstrzygnąć, czy podane przykłady są aktami hackingu czy cyberterroryzmu, gdyż granica między tymi pojęciami jest bardzo płynna.

Wykorzystanie technologii informacyjnych jako narzędzia pomocniczego w negatywnym oddziaływaniu na podmiot można czytelnie przedstawić na przykładzie działalności terrorystycznej[21]. Stopniowo wzrasta liczba kombinowanych ataków terrorystycznych, opierających się na zastosowaniu jednocześnie kilku form oddziaływania. Choć ze względu na nasilony podsłuch sieci komórkowych terroryści ograniczają korzystanie z telefonii komórkowej do rozmów, telefony i pagery są z powodzeniem wykorzystywane jako nadajniki i odbiorniki sygnałów dla zdalnych detonatorów ładunków wybuchowych. Internet stał się tanim i efektywnym narzędziem prowadzenia walki informacyjnej w postaci kampanii propagandowych (w tym działalności rekrutacyjnej) i operacji psychologicznych, umożliwiając dotarcie do odbiorców w skali globalnej.

Organizacje terrorystyczne prowadzą witryny internetowe promujące ich działalność, wydają magazyny internetowe, publikują amatorskie filmy propagandowe, obsługują fora internetowe i grupy dyskusyjne o tematyce terrorystycznej. Stacje telewizyjne Al Jazeera i Al Arabiya w ostatnich latach wielokrotnie emitowały nagrania wideo z przesłaniami terrorystów i obrazami egzekucji. Formą walki psychologicznej jest także modyfikacja zawartości

[20] K. Głowacki, *Cyberzagrożenie* [online]...

[21] Przegląd technologii stosowanych współcześnie przez terrorystów wraz z licznymi przykładami przedstawiony jest w kilkukrotnie przytaczanym w niniejszej pracy opracowaniu autorstwa Jacka Adamskiego *Nowe technologie w służbie terrorystów*.

stron internetowych. Poczta elektroniczna bywa wykorzystywana zarówno do przesyłania wiadomości z pogróżkami, jak i do przesyłania informacji między członkami organizacji terrorystycznych (szyfrowanych lub utajonych za pomocą technik steganograficznych), przy czym terroryści przeważnie łączą się z Internetem z punktów darmowego dostępu. Usługi telefonii internetowej są wykorzystywane do komunikacji głosowej między członkami organizacji terrorystycznych, jako forma bezpieczniejsza niż korzystanie z telefonii komórkowej. Internet jest wykorzystywany do uzyskiwania środków finansowych na działalność terrorystyczną, zarówno w legalny sposób, np. w formie zbiórek pieniędzy przez Internet, jak i nielegalny, poprzez cyberataki na system bankowe i finansowe.

Sieć stanowi ważne narzędzie rozpoznania operacyjnego terrorystów, będąc bogatym źródłem informacji o obiektach przyszłego ataku, ze szczególnym uwzględnieniem powszechnej dostępności szczegółowych map satelitarnych i zdjęć lotniczych miast i obiektów należących do infrastruktury krytycznej (np. usługa Google Maps, czy Google Earth). Technologie informacyjne są wykorzystywane do negatywnego oddziaływania na przeciwnika również w formie pasywnej, np. poprzez fizyczną destrukcję elementów infrastruktury technicznej obiektów – stacji przekaźnikowych i nadawczych, kluczowych serwerów internetowych, centrów przetwarzania danych, jednak w zdecydowanej większości przypadków działania te przynoszą efekt jedynie w skali lokalnej i z tego względu służą czasowej dezorganizacji pracy lub odwróceniu uwagi od rzeczywistego celu ataku[22].

Z procesu kształtowania się społeczeństwa informacyjnego wynika dominująca rola Internetu, jako ogólnoświatowej platformy wymiany informacji i kontaktu między użytkownikami, łączącej (i integrującej) wciąż rosnącą liczbę (mulitmedialnych) elementów. Sieć stała się medium umożliwiającym dostęp do teoretycznie wszystkich powiązanych z nią elementów (w tym, w uproszczeniu, do innych technologii informacyjnych), takich jak systemy bankowości, systemy SCADA, sieci wewnętrzne, telefonia, telewizja itd. Poprzez połączenie wyizolowanego obiektu (systemu) z Internetem, otwiera się kanał informacyjny, który może być wykorzystany do niepowołanego dostępu do obiektu.

[22] Zob. J. Adamski, *Nowe technologie...,* s. 94.

Przyszłość IT jako narzędzia w negatywnej konfrontacji asymetrycznego

Technologie informacyjne, ze względu na możliwość zdalnego, dowolnego w czasie i mało kosztownego oddziaływania na „miękkie podbrzusze" państwa (tj. administrację państwową, infrastrukturę krytyczną państwa, czy sieci wewnętrzne służb – policji, pogotowia, straży pożarnej), stanowią atrakcyjne narzędzie dla podmiotów stwarzających zagrożenie asymetryczne bezpieczeństwa państwa. Postęp technologiczny i procesy globalizacyjne upowszechniły rozwiązania techniczne zarezerwowane uprzednio dla sił zbrojnych oraz służb specjalnych i policyjnych. Konwencjonalne metody walki są przez terrorystów wciąż preferowane, jednak nowe pokolenie częściej sięga po nowinki techniczne, trafnie identyfikując przy tym punkty newralgiczne przeciwnika[23].

W działaniach terrorystycznych, jak podaje Jacek Adamski, wykorzystanie elementów walki informacyjnej z użyciem nowoczesnych technologii przynosi terrorystom korzyści w postaci możliwości destrukcyjnego oddziaływania na instytucje zarówno państwowe (wojskowe i cywilne), jak i niepaństwowe, zakłócania przekazu medialnego i przedstawiania korzystnego dla siebie obrazu sytuacji, niskiego kosztu operacji, zmniejszonego ryzyka wykrycia oraz ogólnoświatowego zasięgu oddziaływania. Autor zauważa również, iż „potencjalny przeciwnik, wykorzystując systemy informatyczne, może zakłócić, a nawet obezwładnić istotne elementy infrastruktury cywilnej i wojskowej, bez użycia tradycyjnych metod walki oraz bezpośredniego narażania własnych sił i środków"[24].

Środowisko eksperckie ostrzega, iż ze względu na postępujący wzrost zagrożeń bezpieczeństwa cyberprzestrzeni i technologii informacyjno – komunikacyjnych, atak cyberterrorystyczny, którego skutkiem byłoby poważne naruszenie bezpieczeństwa państwa, jest kwestią czasu. W 1996 r. amerykańska Defense Advanced Research Projects Agency (DARPA) zorganizowała symulację *The Day After… In Cyberspace*, testującą możliwości obrony infrastruktury Stanów Zjednoczonych przed cyberatakiem. Ćwiczenia obnażyły wysoką wrażliwość infrastruktury krytycznej państwa oraz sił zbrojnych na atak cyberterrorystyczny i walkę informacyjną. Podobna symulacja była przeprowadzona w 1997 r. przez amerykańskie siły zbrojne ze wsparciem NSA,

[23] Tamże, s. 7.

[24] Tamże, s. 91.

przynosząc podobny rezultat – paraliż i ograniczenie zdolności bojowej sił zbrojnych[25].

W 2002 r., podczas przygotowań do Olimpiady Zimowej w Stanach Zjednoczonych, przeprowadzono symulację pod kryptonimem *Black Ice*, której celem było zbadanie wzajemnych zależności infrastrukturalnych. Uszkodzenie sieci energetycznej w wyniku ataku terrorystycznego lub katastrofy naturalnej, spotęgowane cyberatakiem na systemy SCADA, doprowadziło do chaosu i paraliżu praktycznie całej regionalnej infrastruktury, ze względu na jej zależność od dostaw energii elektrycznej. Zależności regionalnej infrastruktury badano również podczas kolejnych ćwiczeń pod kryptonimem *Blue Cascades*[26].

Symulacja wykazała, iż „[…] atak terrorystyczny lub naturalne nieszczęśliwe zdarzenie może zakłócić dostawę energii elektrycznej na kilka tygodni, a w niektórych przypadkach – nawet kilku miesięcy, prowadząc do zaników zasilania rozprzestrzeniających się kaskadowo na całym zachodnim terytorium Stanów Zjednoczonych. Pociągałoby to za sobą zakłócenia telekomunikacyjne w całym regionie oraz trudności w działaniu przynajmniej dwóch systemów zaopatrzenia w gaz ziemny oraz stanowiło dużą groźbę dla systemów wodnych i portów morskich zachodniego wybrzeża"[27].

Takie rezultaty mógłby przynieść nie tylko precyzyjny cyberatak, lecz również fizyczne zniszczenie cybernetycznego systemu sterowania. Niepokój wzbudza także możliwość doprowadzenia do użycia broni jądrowej wskutek cyberataku na system wczesnego ostrzegania. Ze względu na izolację systemów kontroli broni atomowej bezpośredni atak nie jest możliwy, jednak błędny sygnał otrzymany przez struktury niskiego szczebla i następnie przez nie eskalowany mógłby doprowadzić do podjęcia przez końcowego decydenta decyzji o odpaleniu rakiety[28].

Współcześnie cyberprzestrzeń staje się piątym wymiarem pola walki, obok trójwymiarowej przestrzeni kartezjańskiej i czasu. Piotr Gawliczek i Jacek Pawłowski zwracają uwagę, iż „światowa infrastruktura informacyjna to fak-

---

[25] Zob. A. Bógdał-Brzezińska, M. F. Gawrycki, *Cyberterroryzm i problemy*…, s. 86.

[26] Zob. D. Verton, *Black Ice. Niewidzialna groźba cyberterroryzmu*, Wyd. Helion, Gliwice 2004, s. 56.

[27] Tamże, s. 60.

[28] Zob. B. Bartoszek, *Cyberwojna to już rzeczywistość* [online]. Mojeopinie.pl, 2.08.2009 [dostęp: 2.05.2010]. Dostępny w World Wide Web: http://www.mojeopinie.pl/cyberwojna_to_juz_rzeczywistosc,3,1249075265.

tycznie realna infrastruktura wymiaru cybernetycznego”[29]. Ze względu na to, iż jej funkcjonowanie opiera się na wybitnie skomplikowanej sieci powiązań i interakcji między ogromną liczbą elementów systemów teleinformatycznych, jest ona szczególnie podatna na zaburzenia funkcjonowania. Skutki tychże zakłóceń są niewspółmierne do użytych, często ograniczonych środków i „[…] prowadzą do poważnych konsekwencji w wymiarze bezpieczeństwa wojskowego, ekonomicznego i politycznego zaatakowanego państwa”[30].

Zwiększenie bezpieczeństwa technologii informacyjno – komunikacyjnych jest zadaniem kluczowym w celu ograniczenia możliwości wykorzystania IT jako narzędzia asymetrycznych zagrożeń bezpieczeństwa państwa. Coraz pilniejsza staje się potrzeba podjęcia działań prawno-organizacyjnych w celu przeciwdziałania zagrożeniom. W świetle rosnącego prawdopodobieństwa wybuchu wojny w cyberprzestrzeni, szczególnie pilna jest potrzeba wprowadzenia rozwiązań na szczeblu międzynarodowym, odnośnie zapewnienia bezpieczeństwa cyberprzestrzeni. Podczas obrad Światowego Forum Ekonomicznego w Davos w styczniu 2010 r. zwrócono uwagę na potrzebę rozważenia kluczowych zagadnień dotyczących bezpieczeństwa cyberprzestrzeni, m.in. ustalenia, kiedy cyberatak na państwo jest równoznaczny z deklaracją wojny. Sekretarz generalny Międzynarodowego Związku Telekomunikacyjnego (MZT), będącej jedną z agend Organizacji Narodów Zjednoczonych, stwierdził podczas obrad, iż następna wojna światowa będzie miała miejsce w cyberprzestrzeni. Zwrócił również uwagę na rosnące z roku na rok ryzyko wystąpienia konfliktu w cyberprzestrzeni między państwami oraz wysunął propozycję paktu pokojowego, zakazującego państwom-sygnatariuszom wykonania, jako pierwszym, cyberuderzenia na inne państwo. Pakt powinien zawierać również zapis o obowiązku ochrony obywateli i ich prawa dostępu do informacji oraz zakaz udzielania schronienia cyberterrorystom.

Choć umowy między państwami stanowiłyby niewątpliwie ważny element systemu zapewnienia bezpieczeństwa cyberprzestrzeni, przypuszcza się, iż kluczem do zwiększenia jej bezpieczeństwa byłaby edukacja użytkowników technologii informacyjno – komunikacyjnych w zakresie bezpiecznego z nich korzystania (użytkownicy, poprzez nieświadome działania powodują powstawanie zagrożeń) oraz wprowadzenie pewnych elementów kontroli dotychczas wolnego i niekontrolowanego Internetu. Istniejące już projekty monitorowania ruchu w Internecie, jak *Carnivore* czy *Echelon*, nie są ukierunkowane bezpo-

[29] P. Gawliczek, J. Pawłowski, *Zagrożenia asymetryczne*…, s. 49.
[30] Tamże.

średnio na zapewnienie bezpieczeństwa cyberprzestrzeni, lecz ich przeznaczeniem jest uzyskiwanie informacji na temat potencjalnych zagrożeń dla bezpieczeństwa narodowego państw uczestniczących w tych projektach.

Podejmowane próby wprowadzenia kontroli Internetu spotykają się z gwałtownym sprzeciwem jego użytkowników, walczących o zachowanie wolności, swobody i względnej anonimowości w Sieci. Działania w tym zakresie wprowadzenia pewnych form kontroli Internetu podjęły Stany Zjednoczone, gdzie toczą się prace nad projektem ustawy o cyberbezpieczeństwie, wzbudzającej protesty obrońców praw obywatelskich ze względu na proponowaną koncentrację w rękach państwa uprawnień i zadań z zakresu cyberbezpieczeństwa i ochrony infrastruktury krytycznej, godzącą przede wszystkim w ochronę danych[31].

Na cyber-zagrożenia szczególnie podatna jest cyberprzestrzeń RP[32]. Zaangażowanie Polski w zagraniczne operacje wojskowe oraz bliskie stosunki ze Stanami Zjednoczonymi zwiększają ryzyko wystąpienia aktu terrorystycznego na terenie kraju. Eskalacja napięcia w stosunkach bilateralnych także może sprowokować przypuszczenie cyberataku na polską cyberprzestrzeń. Pozytywne wyniki i dobre oceny polskiej gospodarki mogą przyciągać wywiady gospodarcze z różnych, nawet najodleglejszych stron globu. Postępująca informatyzacja państwa, której budowa systemu zabezpieczeń cyberprzestrzeni nie dorównuje tempa, powoduje, iż administracja państwowa i kolejne elementy infrastruktury krytycznej stają się coraz bardziej podatne na cyberataki.

W 2008 r. utworzono Zespół Reagowania na Incydenty Komputerowe (CERT) w ramach Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego[33]. W 2009 r. powstał dokument *Rządowy program ochrony cyberprzestrzeni RP na lata 2009–2011. Założenia*. Jak spostrzega Krzysztof Głowacki, wciąż konieczne jest jednak stworzenie „[…] odrębnej, spójnej i efektywnej strategii zapobiegania i obrony przed cyberterroryzmem na wzór estońskiej Strategii Bezpieczeństwa Informatycznego, zharmonizowanie

---

[31] *Rząd przejmie kontrolę nad internetem?* [online]. Interia.pl, 15.04.2009 [dostęp: 30.04.2010]. Dostępny w World Wide Web: http://nt.interia.pl/internet/bezpieczenstwo/news/rzad-przejmie-kontrole-nad-internetem, 1290927,62

[32] M. Ludwiszewski, *Monitoring stanu bezpieczeństwa teleinformatycznego państwa*, [w:] *Bezpieczeństwo teleinformatyczne państwa*, red. M. Madej, M. Terlikowski, PISM, Warszawa 2009, s. 133.

[33] Do podjęcia decyzji o utworzeniu w krajach członkowskich zespołów CERT (Computer Response Emergency Team), NATO skłonił się po rosyjskim cyberataku na Estonię w 2007 r.

polskiego ustawodawstwa w zakresie bezpieczeństwa informatycznego oraz utworzenie scentralizowanej jednostki rządowej (swoistego centrum antykryzysowego) na bieżąco monitorującej sytuację w kraju i na świecie oraz koordynującej działania instytucji w razie kryzysu [podobnej do zajmującego się terroryzmem Centrum Antyterrorystycznego (CAT) w ABW – M.W.]. Najważniejsza wydaje się jednak zmiana nastawienia polityków i zwykłych użytkowników Internetu do zagrożeń płynących z sieci teleinformatycznych" [34]. Aby wypracowanie skutecznej strategii walki z cyberprzestępczością i cyberterroryzmem było możliwe, młode społeczeństwo informacyjne musi zostać uświadomione co do skali i skutków zagrożeń związanych z funkcjonowaniem technologii informacyjnych, począwszy od zagrożeń bezpieczeństwa indywidualnych użytkowników, po zagrożenia bezpieczeństwa narodowego i międzynarodowego.

Zakończenie

Technologie informacyjne, ze względu na m.in. ich dostępność, niewielki koszt oraz możliwość dotarcia do „miękkiego podbrzusza" państwa, stanowią atrakcyjne narzędzie negatywnego oddziaływania dla podmiotów stwarzających zagrożenie asymetryczne, rozumiane zarówno wąsko, jak i szeroko. W związku z postępem technologicznym i informatyzacją dążących do utworzenia społeczeństw informacyjnych państw, stopień powiązania technologii informacyjnych i infrastruktury państwa rośnie. Internet stał się globalną platformą przesyłu danych i informacji, łącząc i integrując kolejne obszary funkcjonowania państw i ich społeczeństw, w tym organy administracji państwowej i infrastrukturę państwa. Największe zalety Internetu, wolność i anonimowość, stanowią równocześnie źródło szerokiego spektrum zagrożeń dla wszystkich jego użytkowników, w tym poważnych zagrożeń dla bezpieczeństwa państwa, przyciągając różne podmioty, których intencją jest wyrządzenie szkód – pojedyncze jednostki, hakerów, przestępców, terrorystów, a także inne państwa.

Przeprowadzane do tej pory symulacje cyberataków wykazują, iż atak terrorystyczny lub katastrofa naturalna, którym towarzyszy jednoczesny atak w cyberprzestrzeni, mogą spowodować efekt kaskadowy zniszczeń, paraliżując kolejne infrastruktury krytyczne i doprowadzając do chaosu w państwie. Takie rezultaty mógłby przynieść nie tylko precyzyjny cyberatak, lecz również fizyczne zniszczenie cybernetycznego systemu sterowania.

---

[34] K. Głowacki, *Cyberzagrożenie* [online]...

Budowa zabezpieczeń w obszarze cyberprzestrzeni, jest procesem ciągłym, którego tempo wyznacza dynamika rozwoju technologii informacyjnych. Dotychczas stosowane zabezpieczenia bazują głównie na neutralizacji zagrożeń zmaterializowanych. Możliwości prewencji jest ograniczona przez trudność w przewidywaniu miejsca i czasu materializacji zagrożenia w cyberprzestrzeni. Do powstawania zagrożeń prowadzi często samo nieświadome działanie użytkowników technologii informacyjnych bądź lekceważenie przez nich zasad bezpiecznego korzystania z IT.

Błędy w postępowaniu i luki w zabezpieczeniach zwiększają możliwości negatywnego oddziaływania na bezpieczeństwo państwa przez wrogie podmioty. Z tego względu w zapewnieniu bezpieczeństwa (z)informatyzowanego państwa ważną rolę powinna pełnić edukacja obywateli w zakresie bezpiecznego korzystania zarówno Internetu, jak i innych technologii informacyjno-komunikacyjnych. Jako jedno z rozwiązań mających zwiększyć bezpieczeństwo cyberprzestrzeni rozważane są możliwości wprowadzenia różnych stopni kontroli Internetu. Wszelkie próby ograniczania wolności i swobody w Sieci spotykają się jednak z gwałtownym protestem użytkowników Internetu, broniących wolności i względnej anonimowości.

Zauważalny jest powszechny brak zrozumienia relacji między bezpieczeństwem a wolnością. Wzrost bezpieczeństwa jest bowiem proporcjonalny do ograniczania wolności – problem ten dobrze opisał Erich Fromm w *Ucieczce od wolności*. Zwiększenie bezpieczeństwa technologii informacyjno – komunikacyjnych jest zadaniem kluczowym w celu ograniczenia możliwości wykorzystania IT przez wrogie podmioty do generowania zagrożeń bezpieczeństwa państwa, zwanych asymetrycznymi. Być może wkrótce społeczność internetowa będzie musiała zrzec się części wolności, aby ułatwić prewencję, zapobieganie i neutralizację cyberzagrożeń, a przez to zwiększyć bezpieczeństwo cyberprzestrzeni, a w konsekwencji – bezpieczeństwo państwa.

Od red.: Artykuł jest fragmentem opracowania Magdaleny Stefanii Witeckiej pt. „Zagrożenia asymetryczne a technologie informacyjne", które ukaże się jako jedna z planowanych w br. edycji „Zeszytów Problemowych TWO".