Interdyscyplinarne Studia Społeczne
Numer 1 (1), 2016

Ilona Balcerczyk
Uczelnia Nauk Społecznych w Łodzi

Wirtualne oblicze terroryzmu

Recenzja książki *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, pod redakcją Andrzeja Podrazy, Pawła Potakowskiego, Krzysztofa Wiaka, Warszawa: Difin, 2013, ss. 293.

Czy miał rację Francis Fukuyama twierdząc, że nastąpił kres konfliktów między wielkimi systemami politycznymi, a współczesne społeczeństwa będą rozwijały się w kierunku liberalnej demokracji (Fukuyama 2000)? Czy świat w XXI wieku będzie wolny od wojen i zagrożeń, których ludzkość doświadczyła w ubiegłym stuleciu? Znakiem naszych czasów jest dynamiczny rozwój internetu i związana z nim galopująca globalizacja społeczeństw. Edyta Pietrzak w książce *Ku globalnemu społeczeństwu obywatelskiemu. Transgresje idei*, powołując się na Anthony-'ego Giddensa, podkreśla, że globalizacja w formie jaką znamy, to proces charakterystyczny dla ostatnich dwudziestu lat (Pietrzak 2014, s. 168). Odnosząc się do ustaleń Guya Standinga oraz Martina Albrowa, autorka zauważa, że nadeszła era znana pod pojęciem *Global Age*, która oznacza, że europejska historia świata jest już zakończona i weszła w fazę epilogu.

Globalizację możemy rozumieć wielorako: z jednej strony, jako zhomogenizowany świat Francisa Fukuyamy, globalną wioskę Marshalla McLuhana czy zmakdonaldyzowane społeczeństwa Georga Ritzera; z drugiej zaś, jako świat opisywany przez teorię indygenizacji głoszącą, że niezachodnie kultury, po okresie fascynacji techniką, którą otrzymały od Zachodu, przeżywają obecnie fazę powrotów do własnych wartości i definiują swoją kulturę odnosząc się do lojalności (Pietrzak 2014, s. 172). Edyta Pietrzak proponuje, by globalizację rozumieć jako „abstrakcyjne i niezinstytucjonalizowane procesy polityczne, społeczne, ekonomiczne, kulturowe i demograficzne niezależne od konkretnych terytoriów narodowych i przebiegające w przestrzeni ponadlokalnej" (tamże, s. 172). Według Giddensa, globalizacja polega na „intensyfikacji relacji społecznych na skalę światową, dzięki której zjawiska regionalne, pozostające wprawdzie w oddaleniu geograficznym, wiążą się ze sobą i mają swoje odpowiedniki w innej części globu" (tamże, s. 169).

Wspólny mianownik powyższych teorii stanowi internet – symbol naszych czasów. Z jednej strony jest on szansą dla ludzkości, z drugiej jednak staje się źródłem wielu zagrożeń. Jak podkreślają Irving Lachow i Courtney Richardson z amerykańskiego National Defense University, internet może być idealnym narzędziem dla grup terrorystycznych z uwagi na pięć podstawowych

cech: szybką komunikację w czasie rzeczywistym, niskie koszty użycia, globalny zasięg działania nawet małych grup terrorystycznych, możliwość rozpowszechniania skomplikowanych rodzajów informacji oraz techniki szyfrujące dające gwarancję niemal całkowitej anonimowości (Lachow, Richardson 2007, s.100).

Używając stylistyki Vaclava Havla, zaczerpniętej z jego słynnego eseju *Siła bezsilnych,* można powiedzieć, że widmo krąży po świecie – widmo, któremu na imię terroryzm (Havel 1984, s. 40). Tylko w roku 2015 terroryści przelali krew w Nigerii (bojówki Boko Haram dokonały masakry cywilów w północnej Nigerii), w Mogadiszu (atak bombowy w pobliżu lotniska międzynarodowego), w Paryżu (w styczniu Paryż doświadczył ataku na redakcję tygodnika „Charlie Hebdo", w listopadzie paryżanie przeżyli serię ataków w centrum Paryża zorganizowanych przez tzw. Państwo Islamskie), w Bamako (terroryści wzięli zakładników w hotelu Radisson), w Mali, Trypolisie (eksplozje w kawiarni w alawickiej dzielnicy Dżabal Mohsen), na Ukrainie, w Kopenhadze (strzelaniny w centrum stolicy Danii), w Tunisie, Susie, Kuwejcie i Saint-Quentin-Fallavier, w Turcji, w Maroua, w Damaturu, w Bejrucie. Politycy mówią o „atakach wojny" i „wojnie z terroryzmem". Współczesny świat to świat permanentnej wojny z terroryzmem.

Zwrócić jednak należy uwagę, że terroryzm ma dzisiaj dwa oblicza – wirtualne i niewirtualne. Część współczesnych działań terrorystycznych odbywa się w cyberprzestrzeni przy wykorzystaniu możliwości, jakie niesie internet. Stosunkowo niedawno i bardzo blisko nas, 23 grudnia 2015 roku w sąsiedniej Ukrainie, atak hakerski odciął na blisko sześć godzin co najmniej 30 ze 135 stacji elektroenergetycznych[1]. W maju 2015 roku hakerzy włamali się do Bundestagu[2], jesienią 2014 roku zaatakowany został Biały Dom[3], w latach poprzednich światem wstrząsnęły wieści o cyberatakach w Estonii, w Gruzji, w Korei Południowej, ataki *Stuxnet,* grupy *LulzSec,* grupy *Anonymous* oraz zmasowane ataki *Shady Rat*. Wśród zaatakowanych były także agendy rządowe Stanów Zjednoczonych, Tajwanu, Korei Południowej, Wietnamu i Kanady oraz co najmniej

[1] „Na początku hakerzy wykorzystali szkodliwe oprogramowanie, aby za pośrednictwem komputerów kontrolujących sieć odłączyć stacje. Następnie do komputerów wprowadzili wirusa, który spowodował, że system sterowani stał się niesprawny" (Robertson, Riley 2016, s. 54). „Atak polegający na sekwencji infekcji BlackEnergy, a następnie KillDisk, został po raz pierwszy opisany przez ukraiński zespół CERT w listopadzie 2015 roku. W tym czasie odbywały się lokalne wybory na Ukrainie i kilka redakcji medialnych zostało zaatakowanych w ten sposób wspomnianymi zagrożeniami. CERT wykazał, że w wyniku tego ataku duża ilość materiałów wideo i dokumentów nt. wyborów została zniszczona. Wcześniej, we wrześniu 2014 roku, eksperci z firmy ESET informowali o zagrożeniu BlackEnergy, które zaatakowało wiele firm i instytucji zlokalizowanych w Polsce i na Ukrainie. Wtedy zagrożenie pozwalało atakującemu m.in. na kradzież plików z zainfekowanego komputera czy zdalne uruchomienie dowolnego złośliwego kodu" (*Cyberatak wstrzymał dostawy prądu na Ukrainie*, 2016).

[2] „Hakerzy zainstalowali wirus, dzięki któremu przez kilka miesięcy bez wzbudzania podejrzeń mieli dostęp do sieci komputerowej Bundestagu. Później dotarli do węzła komunikacyjnego systemu, który łączy wszystkie 20 tys. komputerów, znajdujących się w niemieckim parlamencie" (Klos 2015).

[3] „Komputery w Białym Domu zaatakowane przez hakerów – potwierdziła administracja Baracka Obamy. Ze wstępnych ustaleń wynika, że grupa hakerów działała na zlecenie rosyjskich władz" (rz, 2104).

trzynastu firm realizujących produkcję na potrzeby amerykańskiego departamentu obrony (zob. Keating 2012). Polska również nie jest bezpieczna. Z danych zawartych w raporcie przygotowanym przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL wynika, że z roku na rok w Polsce odnotowywanych jest coraz więcej ataków cyberterroryzmu[4].

Na cyberprzestrzeń jako źródło zagrożenia współczesnych społeczeństwa proponują spojrzeć Andrzej Podraza, Paweł Potakowski i Krzysztof Wiak – redaktorzy naukowi książki *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna.* Książka składa się z powiązanych ze sobą tematycznie artykułów opisujących cyberterroryzm z perspektywy politologicznej i prawnej.

W związku z tym, że zjawisko cyberterroryzmu jest relatywnie nowym zagrożeniem, wciąż napotykamy trudności z jego zdefiniowaniem. Niemalże we wszystkich artykułach autorzy wychodzą od sprecyzowania pojęcia cyberterroryzmu przywołując różne jego definicje. Wskazują także na różnice między terroryzmem a cyberkonfliktem, cyberwojną, cyberagresją czy cyberprzestępstwem. Zdecydowanie najczęściej przywoływaną definicją jest ta opracowana przez Dorothy Denning. Według tej autorki „za cyberterroryzm można uznać ataki na systemy i sieci komórkowe, przeprowadzone w celu zastraszenia lub zmuszenia władz do spełnienia żądań politycznych, wywołujące w ludziach poczucie strachu, których skutki mają charakter przemocy wobec osób i mienia" (za: Podraza, Potakowski, Wiak 2013, s. 145). Dokładnej analizie poddane zostały także pojęcia pokrewne, takie jak cyberatak, cyberwojna, cyberprzestępstwo.

Zdecydowaną zaletą omawianej tu pozycji jest klarowna i przekonująca systematyka, która przedstawia się następująco. Na książkę składają się trzy bloki tematyczne. Pierwszy z nich poświęcony został politycznemu wymiarowi cyberterroryzmu i zawiera opis tego zjawiska z punktu widzenia bezpieczeństwa międzynarodowego z perspektywy państwa, NATO oraz strategii Stanów Zjednoczonych. Znajdziemy tu także studium cyberdżihadu, czyli wykorzystania Internetu przez współczesny terroryzm islamistyczny.

---

[4] „Rok 2014 okazał się rokiem rekordowym pod względem cyberataków na polskie instytucje.(...) Atakowano KBW, giełdę, a także strony internetowe prezydenta oraz administracji państwowej. W minionym roku (2014) zarejestrowanych zostało aż 12017 zgłoszeń, z których 7498 zakwalifikowano jako incydenty. Analogicznie do lat poprzednich najwyższe miejsce, w ramach zarejestrowanych incydentów, zajmują botnety: w 2013 r. zarejestrowanych zostało aż 4270, a w 2014 r. 4681 przypadków dotyczących zainfekowanych stacji roboczych będących składnikami sieci botnet. Również porównując statystyki systemu ARAKIS.GOV z rokiem 2013 można zaobserwować znaczny wzrost ilościowy alarmów: rok 2013 – 18317, rok 2014 – 28322, z czego największy wzrost odnotowany został zarówno wśród tych o priorytecie wysokim i średnim. (...) Dostrzegalna jest także wyraźna dynamika wzrostu uporczywych, długofalowych ataków bazujących na zaawansowanych narzędziach. Oznacza to, że oprócz wzrostu ilościowego obserwowany jest także istotny postęp jakościowy w prowadzonych atakach. Upraszczając – nie dość, że ataków jest więcej, to mogą one aktualnie być także znacznie groźniejsze. Istotnym czynnikiem pozostaje tu udział grup kierowanych i sponsorowanych przez obce państwa" (plk, 2015).

Drugi blok tematyczny traktuje o prawnym i instytucjonalnym paradygmacie cyberterroryzmu. Znajdziemy tu zagadnienia związane z prawnymi aspektami zwalczania cyberterroryzmu oraz zagrożeń łączących się z rozwojem technologii informacyjnych i komunikacyjnych. Poza tym, umieszczono tu zagadnienia dotyczące ochrony prawnej systemów informatycznych wobec zagrożenia cyberterroryzmem, opis instytucjonalnego wymiaru bezpieczeństwa teleinformatycznego, analizę szans i zagrożeń wirtualnej przestrzeni administracji publicznej, studium praw człowieka podczas wprowadzenia stanów nadzwyczajnych z uwagi na działania cyberprzestrzeni, charakterystykę zjawiska wigilantyzmu internetowego oraz omówienie kazusu Wikileaks pod kątem możliwości terrorystycznych hakerów.

Ostatni blok tematyczny w całości odnosi się do wymiaru prawnokarnego cyberterroryzmu. Zawarto w nim analizy prawnokarnych środków przeciwdziałania cyberterroryzmowi, opis przestępstw przeciwko integralności i dostępności do zapisu danych informatycznych, jako przestępstw o charakterze terrorystycznym oraz omówienie odpowiedzialności karnej za przestępstwa o charakterze terrorystycznym popełnione w cyberprzestrzeni.

Kolejną zaletą omawianej książki jest fakt skierowania jej do wielu adresatów – sięgnąć po nią mogą z powodzeniem zarówno politolodzy, jak i informatycy zajmujący się bezpieczeństwem systemów IT, pracownicy administracji publicznej odpowiedzialni za bezpieczeństwo cyfrowe oraz za przeciwdziałanie sytuacjom kryzysowym, socjolodzy i prawnicy, a także zwykli użytkownicy internetu.

Dla politologów i osób zajmujących się doktrynami polityczno-prawnymi szczególnie ciekawe mogą wydać się, między innymi, opracowania na temat przeobrażeń porządku międzynarodowego po zakończeniu zimnej wojny oraz analiza podstawowych podejść teoretycznych w stosunkach międzynarodowych, tj. realizmu, liberalizmu oraz konstruktywizmu społecznego. Interesujące są również rozważania odnoszące się do roli państwa i sposobów reagowania przez państwa i rządowe organizacje międzynarodowe, takie jak NATO i Unia Europejska, na zagrożenia cyberterroryzmu. Na uwagę zasługują także refleksje związane z wykorzystaniem internetu do nagłaśniania idei świętej wojny przez dżihadystów oraz charakterystyka takich problemów jak digitalizacja dżihadyzmu, wykorzystanie przestrzeni wirtualnej do działań propagandowych i kreowania wizerunku oraz rozpowszechniania ekstremistycznej ideologii islamskich grup terrorystycznych. Interesujące są artykuły poświęcone sprzeczności między dobrem publicznym polegającym na ochronie państwa i narodu a przestrzeganiem praw jednostek, które mogą podlegać ograniczeniom w celu zabezpieczenia bezpieczeństwa w cyberprzestrzeni.

Prawnicy znajdą dla siebie analizy kompleksowych regulacji przyjętych w Stanach Zjednoczonych po zamachach z jedenastego września, w tym także w zakresie ochrony infrastruktury oraz zasad zapewnienia współpracy międzynarodowej w zakresie efektywnego ścigania i karania cyberprzestępców. Omówiony został także polski stan prawny gwarantujący ochronę systemów teleinformatycznych. Część opracowań poświęcona została tematyce penalnej za czyny zabronione w cyberprzestrzeni. Autorzy artykułów zajęli się zagadnieniem wyznaczania granic represji karnej w demokratycznym państwie prawnym, analizie poddane zostały znamiona czynów zabronionych zaliczanych do tzw. przestępstw komputerowych, przeprowadzono charakterystykę najpoważniejszych czynów zabronionych popełnionych w cyberprzestrzeni, zaproponowano ich kwalifikację na podstawie przepisów prawa karnego oraz przedstawiono konsekwencje popełnienia przestępstwa cyberterrorystycznego na tle polskiego kodeksu karnego. Rozważaniom natury prawnej poddano także wigilantyzm – poprzez podanie przykładów scharakteryzowano i oceniono to zjawisko.

Pracownicy administracji publicznej za interesujące uznają na pewno treści dotyczące rozwiązań antycyberterrorystycznych w administracji publicznej, ze szczególnym uwzględnieniem ochrony infrastruktury krytycznej. Zestawiono i przeanalizowano pojęcia sfery publicznej, sfery zadań publicznych, przestrzeni publicznej oraz wirtualnej przestrzeni publicznej. Opisano także zagrożenia i trudności związane z funkcjonowaniem wirtualnej przestrzeni publicznej.

Zwykli użytkownicy internetu mogą zapoznać się z charakterystyką ataków hakerskich na komputery małych firm i prywatnych użytkowników sieci oraz zapoznać się z zagrożeniami wynikającymi z niedostatecznej ochrony przed cyberatakami. Książka bez wątpienia może być także przydatna dla specjalistów z obszaru IT.

Dzięki temu, że omawiana pozycja składa się z wielu osobnych artykułów, czytelnik bez trudu odnajdzie interesujące go treści. Dodatkowym plusem jest przyjazny w odbiorze język opracowań, zrozumiały także dla osób z małym stopniem wtajemniczenia w tematykę cyberterroryzmu. Autorami artykułów są przedstawiciele różnych ośrodków akademickich oraz polskiej administracji publicznej, co przełożyło się na szerokie i wielowymiarowe spojrzenie na cyberterroryzm. Niewątpliwym minusem książki (aczkolwiek trudnym do uniknięcia w tego typu publikacjach), jest powtarzalność niektórych treści, przede wszystkich tych związanych z definiowaniem cyberterroryzmu. Na uwagę zasługuje również fakt, iż książka wydana jest bardzo schludnie w sensie dbałości o jakość języka polskiego – błędy typu „literówki" występują sporadycznie, co zwiększa komfort obcowania z publikacją także w czysto edytorskim aspekcie.

Odpowiadając na pytanie postawione na początku niniejszej recenzji „Czy miał rację Fukuyama twierdząc, że nastąpił kres konfliktów między wielkimi systemami politycznymi, oraz że współczesne społeczeństwa będą rozwijały się w kierunku liberalnej demokracji?", po lekturze książki i mając na uwadze ostatnie ataki terroryzmu i cyberterroryzmu, można zaryzykować stwierdzenie, że Fukuyama się mylił. Skłonna jestem przyznać rację Władysławowi Leśnikowskiemu, który za motto swego artykułu o cyberterroryzmie uznał słowa: „Żyjemy w świecie, w którym rodzi się nowego rodzaju zagrożenie dla społeczeństw. Jego imię to cyberprzestępczość, a w konsekwencji – cyberwojna" (Leśnikowski 2012). Dlatego też uważam, że wciąż warto poszerzać swą wiedzę z tego obszaru. Warto sięgać do takich publikacji jak *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna.*

Bibliografia

Cyberatak wstrzymał dostawy prądu na Ukrainie, (2016). http://www.eset.pl/O_nas/Centrum_prasowe/Aktualnosci,news_id,11207 [dostęp: 10.03.2016].

Fukuyama, F. (2000). *Koniec historii,* Poznań: Z-sk i Spółka.

Havel, V. (1984), *Siła bezsilnych*, Warszawa: Krąg.

Keating, J. (2012). *10 najgroźniejszych cyberataków*, http://wiadomosci.onet.pl/ciekawostki/10-najgrozniejszych-cyberatakow/djx4j [dostęp: 10.03.2016].

Kłos, A. (2015). *Największy w historii cyberatak na Bundestag. Komputery niemieckich polityków pod kontrolą Rosji*, „Niezależna", http://niezalezna.pl/67970-najwiekszy-w-historii-cyberatak-na-bundestag-komputery-niemieckich-politykow-pod-kontrola-rosj, [dostęp: 10.03.2016].

Lachow, I., Richardson C. (2007), *Terrorist use of the internet. The real story,* "Joint Force Quarterly" No 45, ss. 101-103.

Leśnikowski W. (2012). *Cyberataki na infrastrukturę krytyczną jako tanie i skuteczne środki do paraliżowania*, Centrum Doktryn i Szkolenia Sił Zbrojnych, http://cdis.wp.mil.pl/plik/file/Publikacje/cyberataki-na-infrastruktur-krytyczn.pdf, [dostęp" 10.03.2016].

Pietrzak, E. (2014). *Ku globalnemu społeczeństwu obywatelskiemu. Transgresje idei*, Warszawa: Elipsa.

plk, (2015). *Szokujący raport CERT. Rosja prowadzi już w Polsce wojnę hybrydową* http://niezalezna.pl/66026-szokujacy-raport-cert-rosja-prowadzi-juz-w-polsce-wojne-hybrydowa, [dostęp 01.02.2016].

Podraza, A., Potakowski, P., Wiak, K. (2013). *Cyberterroryzm zagrożeniem XXI wieku. Perspektywa politologiczna i prawna*, Warszawa: Difin.

Robertson J., Riley M., (2016) *Dziś Ukraina, a jutro... Hakerzy odcinają prąd miastom*, Bloomberg Businessweek, Nr 2 (149), s. 54.

rz, (2014), *Rosyjscy hakerzy zaatakowali Biały Dom. Cyberwojna wkracza w nową fazę*, http://niezalezna.pl/60893-rosyjscy-hakerzy-zaatakowali-bialy-dom-cyberwojna-wkracza-w-nowa-faze, [dostęp 10.03.2016].

Ilona Balcerczyk, doktor nauk prawnych, absolwentka Wydziału Prawa i Administracji Uniwersytetu Łódzkiego, adiunkt w Uczelni Nauk Społecznych oraz pracownik Łódzkiego Urzędu Wojewódzkiego w Łodzi. Jej zainteresowania naukowe koncentrują się wokół tematyki doktryn polityczno-prawnych oraz idei społeczeństwa obywatelskiego.

Kontakt z autorką: ilona.balcerczyk@uns.lodz.pl