Cyberprzestrzeń w procesie konstruowania bezpieczeństwa

BOGUSŁAW OLSZEWSKI

Wprowadzenie

Cyberprzestrzeń, jako efekt dwudziestowiecznej rewolucji informacyjnej i naukowo-technicznej, oddziałuje współcześnie na niemal wszystkie dziedziny działalności państwa i jego relacje na arenie międzynarodowej. Abstrahując od aspektu ekonomicznego, obecność struktur państwowych w globalnej sieci staje się coraz bardziej zauważalna, a do tej sfery została przeniesiona – w formie reprezentacji cyfrowej – duża część instytucji i urzędów oraz ich zasobów, ustanawiając coraz szersze możliwości interakcji na polu wirtualnych relacji z obywatelami czy społeczeństwem informacyjnym jako takim. Tym samym, rośnie nie tylko skala partycypacji społecznej w zdigitalizowanym środowisku związanym bezpośrednio ze strukturami rządowymi, ale i funkcja władcza państwa, realizująca się m.in. w uzurpowaniu prawa do rozciągania zwierzchności na całość infrastruktury informatycznej oraz, co najważniejsze, do kontrolowania i wykorzystywania cyberprzestrzeni w procesie osiągania szeroko pojętych celów politycznych i wojskowych[1]. Postępujące upolitycznienie cyberprzestrzeni ma miejsce nie tylko w kontekście wspomnianej, zwiększającej się digitalizacji struktur państwowych (e-urzędy, portale rządowe i administracyjne, e-dyplomacja, blogi polityków *&c*.). Jest ono również efektem stanowienia przez nią znaczącego komponentu (warstwy) zdolnego oddziaływać na elementy infrastruktury krytycznej oraz pełnionej, niezwykle istotnej, funkcji narzędzia oddziaływania społecznego. W tej dziedzinie coraz bardziej widoczna staje się aktywność państw związana z bezpieczeństwem (wewnętrznym, narodowym, międzynarodowym). Stąd tezą niniejszej publikacji jest, iż obecnie w odniesieniu do cyberprzestrzeni przebiegają wzmożone procesy sekurytyzacyjne[2].

W obliczu postępujących procesów globalizacyjnych i rosnącej współzależności zarówno państwowych, jak i niepaństwowych aktorów międzynarodowych, domena cyberprzestrzeni w coraz

większym stopniu staje się obiektem podlegającym procesowi konstruowania bezpieczeństwa. Aspekty militarne towarzyszące genezie globalnej sieci teleinformatycznej[3], posiadającej współcześnie coraz szersze zastosowanie w dziedzinie obronności, sprawiły, że ta hybrydowa (materialno-wirtualna) dziedzina została uznana za jeden z newralgicznych elementów współczesnych stosunków międzynarodowych. Stało się to z kolei bezpośrednią przyczyną faktu, że trwające obecnie procesy konstruowania bezpieczeństwa w cyberprzestrzeni skutkują włączaniem jej w międzynarodowy porządek prawny, w tym w sferę dotyczącą konfliktów zbrojnych. Analiza praktyki międzynarodowej na polu bezpieczeństwa politycznego, militarnego i informatycznego sugeruje, że anarchiczne, cywilne środowisko sieciowe może zostać w przyszłości podporządkowane i zmonopolizowane przez uprawnione podmioty określające zarówno charakter, jak i stopień zagrożenia generowany w odniesieniu do i przez użytkowników sieci komputerowych. Wszystkie te implikacje, także o charakterze normatywnym, wiążą się z zagadnieniem teorii sekurytyzacji w ujęciu tzw. szkoły kopenhaskiej[4], zwłaszcza po uwzględnieniu roli konstruowania bezpieczeństwa jako narzędzia oddziaływania politycznego. Punktem wyjścia pozostaje tutaj wpływ wydarzeń na arenie międzynarodowej na zaistnienie „aktu mowy", jako że: „kwestia staje się kwestią bezpieczeństwa poprzez akt mowy niezależnie od tego, czy mamy do czynienia z rzeczywistym odzwierciedleniem egzystencjalnego zagrożenia w warunkach materialnych"[5]. Podejście konstruktywistyczne wydaje się zatem częściowo wyjaśniać obecny trend w podejmowaniu działań zmierzających do zawłaszczenia dziedziny cyfrowej przez podmioty militarne i polityczne, formalnie wydzielone w ramach pięciu sektorów bezpieczeństwa funkcjonujących w obrębie modelu sekurytyzacyjnego. Aby udzielić odpowiedzi na pytanie, w jaki sposób dziedzina cyberprzestrzeni jest włączana do sfery bezpieczeństwa i jakie podmioty międzynarodowe o tym decydują, warto umieścić ją w krótkiej perspektywie historycznej w charakterze czynnika oddziałującego na bezpieczeństwo.

Sekurytyzacja cyberprzestrzeni – casus Estonii

Atak cybernetyczny na Estonię w 2007 roku[6] stał się jednym z najważniejszych incydentów skutkujących eskalacją „mowy bezpieczeństwa" w odniesieniu do cyberprzestrzeni lokującym ją w kategorii zagrożeń w ujęciu państwocentrycznym. Został

przeprowadzony w odpowiedzi na prace związane z przeniesieniem cmentarza Armii Czerwonej i pomnika Żołnierza Radzieckiego z centrum Tallina, a towarzyszyły im równolegle zamieszki na tle politycznym i etnicznym. Miał zatem podłoże ideologiczne, a jego skutki są doskonałym przykładem sekurytyzacji domeny cyberprzestrzeni, przeprowadzonej na gruncie państwa narodowego, jednak w oparciu o niewystarczające przesłanki. Bezpośrednim efektem było umiędzynarodowienie problemu cyberbezpieczeństwa Estonii oraz zaostrzenie przepisów jej kodeksu karnego, dotyczących niepożądanych działań w środowisku sieciowym, co *de facto* przy obecnym stanie prawnym sprowadza się do skutecznych represji niemal wyłącznie na gruncie wewnętrznym. W k.k. Estonii potwierdzono ponadto terytorialną zwierzchność państwa nad infrastrukturą cyfrową, a co więcej, rozciągnięto ją na własność prywatną, co formalnie kłóci się z konstytucyjnymi gwarancjami w tej materii. Ponadto powstaje dodatkowo wrażenie, że rząd Estonii, dokonując zmian we wspomnianych przepisach, próbował w zamian odciążyć finansowo podmioty gospodarcze próbował odciążyć finansowo podmioty gospodarcze (dostawców sieci, właścicieli i administratorów serwerów). Poprzez wdrożenie polityki odstraszania obniżył częściowo koszty ponoszone przez nie na skutek destrukcyjnych działań prowadzonych w cyberprzestrzeni, a tym samym zredukował nakłady łożone na poczet ochrony ich sieci przesyłowych i zasobów informatycznych, stanowiących ostatecznie integralny element infrastruktury krytycznej. Z drugiej strony, jak każde zresztą państwo, wymaga od podmiotów gospodarczych operujących na rynku IT czynnego zaangażowania w ochronę własnych interesów, co sprowadza się do kolejnych gratyfikacji (kontrakty na dostawy i serwis sprzętu, świadczenie usług telekomunikacyjnych i informatycznych *&c.*). Ochrona i nadzór nad terytorialnym systemem informatycznym stały się zatem uniwersalną wartością, wokół której koncentruje się środki i zabiegi kreujące zagrożenie egzystencjalne, przykuwając na tyle uwagę społeczeństwa, by uprawomocnić wprowadzenie dowolnych zasad prawnych w tej materii. Sytuacja ta nie ma bynajmniej charakteru wyłącznie lokalnego, jako że rozwiązania przyjęte przez Estonię są powielane w innych państwach regionu i świata.

„W centrum procesu sekurytyzacji znajduje się tzw. akt mowy, rozumiany jako dyskursywna reprezentacja danej kwestii jako egzystencjalnego zagrożenia dla bezpieczeństwa”[7]. Podczas działań wymierzonych w elementy infrastruktury cyfrowej Estonii, w istocie

skierowanych głównie przeciwko zasobom sektora komercyjnego, a w mniejszym stopniu administracyjnego i rządowego, niemal od razu zdefiniowano charakter zagrożenia, przenosząc je na płaszczyznę ponadnarodową i wskazując jednocześnie na Federację Rosyjską jako animatora tych działań. W maju 2007 roku minister spraw zagranicznych Estonii Urmas Paet oskarżył Rosję o bezpośrednie zaangażowanie w cyberataki[8]. Nie było jednak technicznych możliwości jednoznacznego udowodnienia jej wiodącej roli, a jedyny ujawniony rosyjski rządowy adres IP nie stanowił w tym wypadku dostatecznej okoliczności obciążającej. Należy jednak przyznać, że w dużym stopniu ataki informatyczne były faktycznie prowadzone zupełnie otwarcie przez część obywateli estońskich, instruowanych na rosyjskojęzycznych forach internetowych w kwestii użycia gotowych programów hakerskich obciążających serwery atakami typu DoS, podczas gdy ruch sieciowy generowany spoza granic kraju nie wskazywał jednoznacznie lokalizacji atakujących, głównie z uwagi na możliwość podszycia się pod dowolny numer IP (*spoofing*). Jakkolwiek cyberataki były przeprowadzone za pośrednictwem globalnej, rozproszonej infrastruktury sieciowej (łącznie ze 178 krajów), szybkie zdefiniowanie motywów i wroga uruchomiło prostą sekwencję wykluczającą podważenie zasadności podejmowanych działań i późniejszych regulacji prawnych. Wydaje się logiczne, że *gros* ataków wymierzonych za pośrednictwem sieci w Estonię było osnutych wokół przeniesienia memoriału Armii Radzieckiej i prowadzonych również z terytorium Federacji Rosyjskiej, w tym prawdopodobnie poprzez elementy infrastruktury i przez podmioty związane ze sferami rządowymi. Jednak paradoksalnie żaden podmiot zagraniczny nie poniósł żadnej odpowiedzialności za atak, a jedynym skazanym w tej sprawie pozostał mieszkaniec Estonii, Rosjanin Dmitrij Galuszkiewicz, student uczelni technicznej[9]. Nie wzięto również pod uwagę faktu, że niepokoje wewnętrzne w dowolnym państwie mogą zostać sprowokowane przez aktorów globalnych o różnych intencjach, w tym także przez osoby niezwiązane bezpośrednio z dynamiką sytuacji na gruncie ideologicznym, ale zmierzające do destabilizacji regionu i eskalacji konfliktu w oparciu o najniższe pobudki, czy nawet samą chęć sprawdzenia własnych zdolności informatycznych w warunkach realnego cyberkonfliktu.

Po zmianach w kodeksie karnym Estonii nie dokonano (podobnie jak w estońskiej „Strategii Cyberbezpieczeństwa") rozróżnienia na „zwykłych" hakerów i tzw. hakerów patrio-

tycznych, czyli obywateli kierujących się silnym poczuciem identyfikacji narodowej i prowadzących działania w imieniu państwa pochodzenia; z racji braków legislacyjnych zostali oni zakwalifikowani jako zwykli cyberprzestępcy. Tym samym, z jednej strony oddalono ryzyko eskalacji sporu międzynarodowego opartego na pochopnej nadinterpretacji cyberprzestrzennej sytuacji konfliktowej, zwłaszcza w obliczu obserwowanego braku skuteczności norm prawa międzynarodowego i wiążących umów bilateralnych, z drugiej zaś uznano w ten sposób społeczny charakter cyberkonfliktu z 2007 roku, wprowadzając ostatecznie nowe regulacje wewnętrzne ograniczone faktycznie do terytorium zainteresowanego państwa. Przyznano tym samym, że na gruncie międzynarodowym prawo cyberprzestrzeni pozostaje bezsilne, natomiast amorficzny charakter dziedziny cyfrowej uniemożliwia skutecznie egzekwowanie prawa. Dostrzeżono również łatwość sprowokowania klasycznego, kinetycznego konfliktu zbrojnego poprzez wykorzystanie globalnej sieci teleinformatycznej. Jednak fakt, że „istotne jest przekonanie odbiorców przekazu do działań aktora sekurytyzującego”[10], a zatem ich uwarunkowanie i wymuszenie zaakceptowania przez nich wyższej konieczności, sprawił, że nieodzowne stało się podtrzymanie sugestii i obaw związanych z potencjalną powtórką wydarzeń. Z podobnym efektem świat zetknął się w 1999 roku na fali indukowanego przez media „problemu roku 2000”, w dużej mierze wygenerowanego sztucznie wokół zmiany daty systemowej[11]. Doprowadziło to do zwiększonej inwestycji w oprogramowanie i usługi mające uchronić konsumentów i instytucje przed tym, jak się okazało przecenionym, niebezpieczeństwem; decydującym czynnikiem sprawczym były tu przewidywane zyski sektora IT.

Kolejnym efektem cyberataku na Estonię była narodowa strategia cyberbezpieczeństwa, przyjęta w 2008 roku, jak i równoległe powołanie Cooperative Cyber Defence Centre of Excellence (CCD COE) z siedzibą w Tallinie. Jest to międzynarodowa komórka badawczo-szkoleniowa funkcjonująca w ramach NATO, oparta o kooperację specjalistów IT pochodzących z państw członkowskich. Fakt umiejscowienia ośrodka w Estonii, kraju dotkniętym realnym cyberatakiem, pozostaje nie bez wpływu na kształtowanie świadomości społecznej dotyczącej cyberzagrożeń. W 2013 roku grupa badaczy wojskowych i akademickich działających w ramach CCD COE wydała *Talliński podręcznik prawa międzynarodowego mającego zastosowanie w cyber-działaniach wojennych* – zbiór prawnie niewiążących

rekomendacji dotyczących zasad prowadzenia cyberwojny, opracowany na podstawie istniejących zasad prawnych: *ius ad bellum* i *ius in bello*, znajdujących ich zdaniem zastosowanie w dziedzinie konfliktów cyberprzestrzennych. Doraźny charakter tego dokumentu i jego zapisy, stanowiące niejednokrotnie zaadaptowane wyjątki z kodeksów wojennych opracowanych jeszcze w czasach rewolucji przemysłowej, skłaniają do refleksji nad forsowaniem nieadekwatnych obecnie norm prawnych, mających funkcjonować w odniesieniu do postindustrialnych konfliktów w sferze cyfrowej i oddalających *ad infinitum* moment wypracowania nowych regulacji. Tymczasem w praktyce międzynarodowej sugeruje się stosowanie kodeksów etyki środowiskowej (tzw. netykiet)[12], wewnętrznych regulacji portali internetowych i regulaminów dostawców usług. Są one jednak zupełnie nieprzydatne, kiedy przeniesienie dyskursu na poziom polityczny implikuje automatycznie zagrożenia natury militarnej. Stają się nimi działania, które w innych kontekstach takimi nie są, jak np. proste ataki typu DoS. Plastyczność cyberprzestrzeni sprawia, że dowolny jej element może zostać uznany za istotne zagrożenie dla bezpieczeństwa państwa. Skłania to niektórych badaczy do wysunięcia tezy o konstruktywistycznym, czy nawet fikcyjnym pochodzeniu problematyki cyberwojny[13].

Wielowymiarowość sekurytyzacji cyberprzestrzeni

Cyberbezpieczeństwu podlegają zatem coraz to nowe sektory, aktorzy sekurytyzujący (liderzy polityczni, biurokraci, rząd, system edukacji, lobbyści i grupy nacisku) oraz obiekty referencyjne – w tym przypadku państwo stojące w obliczu możliwych zagrożeń egzystencjalnych w tym sektorze bezpieczeństwa, głównie w kontekście wojskowym i politycznym. Hybrydowy charakter cyberprzestrzeni sprawia, że kategoria ta jest niezwykle pojemna i warto zauważyć, że główną przyczyną demonizowania i podejmowania coraz to nowych prób regulacji przestrzeni cyfrowej jest wprzęgnięcie jej w różnego rodzaju aspekty działań militarnych. Wobec wdrażanych strategii bezpieczeństwa, postulujących coraz szersze wykorzystanie cyberprzestrzeni w działaniach zbrojnych, w tym koncepcji dotyczących wojny sieciowej oraz i opracowania modeli prowadzenia walki na poziomie taktycznym (np. *swarming*[14]): „Coraz więcej osób zabiera głos, w publicznej dyskusji potwierdza poczucie zagrożenia i sygnalizuje, że nadszedł czas, aby podjąć działania na rzecz bezpieczeństwa cyberprzestrzeni"[15].

Wzmożone tendencje regulacyjne w odniesieniu do aktywności społeczeństwa sieciowego wykazywane są również przez podmioty prywatne silnie powiązane ze sferą polityki, zaś sektor przemysłowy i informatyczny jest obecnie niezwykle aktywnym aktorem sekurytyzującym: „Konieczność ich [regulacji prawnych – B.O.] wprowadzenia dostrzeżono wyraźnie w ostatniej dekadzie XX wieku, kiedy nasilił się proces wykorzystania Internetu dla celów komercyjnych"[17]. Brak spójnego prawa, jego sprzeczny charakter, opieszałość legislacyjna czy niemożność skutecznego egzekwowania istniejących przepisów prawnych, wykluczają obecnie stworzenie efektywnego i jednolitego ko-deksu norm obowiązujących w sieci, jednak to sektor prywatny wydaje się legitymować największym doświadczeniem w kształtowaniu tej materii. Obiekty referencyjne są opisane w wielu dokumentach i co więcej, w obliczu prognozowanego dynamicznego wzrostu znaczenia sektora IT podkreślana jest dalsza eskalacja zagrożeń na tym polu, co pozwala przewidywać dynamiczny rozwój rynku bezpieczeństwa cyfrowego.

Zagrożenie ma zatem charakter wielopłaszczyznowy, co pozwala objąć procesem sekurytyzacyjnym całość cyberprzestrzeni, jej aspekt militarny, ekonomiczny, ideologiczny, tożsamościowy i ekologiczny oraz warstwę geofizyczną. Działalność państwa w ramach sieci globalnej posiada szereg implikacji nie tylko w obszarze przetwarzania danych osobowych, dostępu do informacji publicznej, funkcjonowania e-urzędów i e-wyborów. Prowadzi do nadania bytowi wirtualnemu znamion realnego zagrożenia egzystencjalnego na zasadzie samospełniającej się przepowiedni, jako że: „Oznaczenie danej kwestii jako kwestii bezpieczeństwa międzynarodowego staje się pochodną znaczenia jej nadawanego"[18]. Co ciekawe, aby uprawomocnić tę aktywność, akt mowy często koncentruje się na bezpieczeństwie społecznym i ludzkim, indukując bierną akceptację dla państwowych regulacji i dowolności rządowych działań w sieci, nawet jeśli wiążą się one z ograniczeniem praw obywatela, utrudnieniem dostępu do informacji czy naruszeniami konstytucyjnego prawa do prywatności. Tym samym, społeczeństwo jako odbiorca (*audience*) odgrywa w procesie sekurytyzacji cyberprzestrzeni istotną rolę, przede wszystkim otrzymując i podtrzymując złudzenie współdecydowania o kwestiach cyberbezpieczeństwa, kiedy faktycznie od początku stoi tutaj na przegranej pozycji. Podkreślenie przez aktora sekurytyzującego samych tylko negatywnych stron i zagrożeń oraz przedstawienie gotowych rozwiązań, przyjmowanych najczęściej *post factum*,

modeluje niemal bezwarunkową akceptację dla jego działań. Ten zabieg może służyć autorytarnemu umacnianiu władzy, ograniczaniu wolności oraz łamaniu praw człowieka i obywatela, przy jednoczesnych deklaracjach ich ochrony w sytuacji sugerowanego, permanentnego zagrożenia.

Ten paradoks jest szczególnie widoczny w kontekście zwalczania zjawisk cyberprzestępczości i cyberterroryzmu. Odnotowując fakt, że rozproszona sieć, jaką w warstwie fizycznej i logicznej jest Internet, stanowi globalną i technologiczną noosferę, a zamieszczane tam treści wymykają się jurysdykcji państw, ograniczając ją do jego terytorium, kategorie te dotyczą z reguły zachowań możliwych do objęcia represyjnymi przepisami egzekwowanymi w obrębie prawa wewnętrznego. Skuteczne reperkusje skierowane przeciwko podmiotom zagranicznym, a już w pełni w odniesieniu do aktywnie działających aktorów niepaństwowych, leżą głównie w sferze teorii akcentującej rozwój międzynarodowej kooperacji i dostarczenie skutecznych narzędzi prawnych. Tymczasem, nawet na tym polu dochodzi do konfliktów kompetencyjnych i cichego przywłaszczania elementów dziedziny normatywnej związanych z nadzorem nad zdarzeniami w cyberprzestrzeni. Kształtująca się praktyka sądów oparta jest bowiem w dużej mierze o anglosaski system *common law*, co w pewien sposób wskazuje na tendencje monopolizacyjne w sferze cyberprawa, przejawiane przez głównych graczy międzynarodowych funkcjonujących najczęściej na podstawie tego porządeku prawnego.

Wnioski

Sekurytyzacja w sektorze politycznym i militarnym wpływa wybitnie na zagadnienia związane ze sferą przestrzeni cyfrowej, jak: terytorialna suwerenność państwa, adekwatność i skuteczność norm prawnych, digitalizacja państwa, e-dyplomacja, bezpieczeństwo ludzkie i prawa człowieka, inżynieria społeczna czy problematyka dotycząca zagrożeń wynikających z zaangażowania i uprzywilejowania sektora przemysłowego oraz instytucji państwowych. Wszystko to sprawia, że szczególnej obserwacji należy poddać ewolucję wartości i norm zachodzącą obecnie w kontekście środowiska wirtualnego. Ich dalsza kodyfikacja może bowiem stanowić próbę ustanowienia skutecznej kontroli nad tą grupą społeczną, którą stanowią użytkownicy Internetu, realizowaną pod pretekstem przeciwdziałania negatywnym aspektom wyłonionym w procesie sekurytyzacyjnym,

a dotyczącym: cyberprzestępczości, cyberterroryzmu, cyberszpiegostwa, cyberwojny, cyberstalkingu, haktywizmu[19] *&c*. Ponieważ „nie tworzy się specjalnych aktów prawnych wyłącznie na potrzeby internetu"[20], inkorporacja norm przewidzianych do stosowania w bardziej statycznych, klasycznych środowiskach, podda regulacji mały wycinek rzeczywistości sieciowej, deformując pozostałą część tego medium i grawitując w kierunku stosowania nieprzystających, nieprzyjaznych przepisów prawnych. Dodatkowe ograniczenia, wynikające z braku szerszej współpracy państw na arenie międzynarodowej oraz adaptacji arbitralnych rozwiązań proponowanych przez lobby przemysłowe i militarne, również rodzą wiele wątpliwości. Ponadto pytanie, czy zupełnie nowe przepisy powinny zastąpić istniejące zapożyczenia z kodeksów prawa publicznego, prywatnego, gospodarczego, wojennego i zwyczajowego, jest nadal pytaniem o adekwatność zewnętrznych norm stosowanych w środowisku sieciowym. A także o negatywny, destrukcyjny wpływ forsowania na tym polu wielu przestarzałych regulacji, wymuszających m.in. ograniczenie obywatelskiej aktywności w sieci.

Jeśli chodzi o samą cyberprzestrzeń, stopień jej sekurytyzacji określa faktyczny stopień suwerenności państwa na arenie międzynarodowej i to nie tylko w perspektywie skutecznej odpowiedzi na potencjalne cyberzagrożenia. Jest również probierzem społecznej partycypacji w procesach decyzyjnych i miarą jakości społeczeństwa obywatelskiego: „O ile w reżimach demokratycznych odbiorcą zazwyczaj będzie całe społeczeństwo, to np. w reżimach autorytarnych cały proces sekurytyzacji będzie mógł mieć miejsce w obrębie elit politycznych"[21]. Obydwa zagadnienia łączą się ze sobą nierozerwalnie. Należy też zwrócić uwagę na fakt, że strategie cyberbezpieczeństwa przyjmowane na gruncie narodowym są w istocie kopiami rozwiązań proponowanych przez kraje zaawansowane technologicznie, o wysokim stopniu usieciowienia, występującym w zinformatyzowanej gospodarce opartej na wiedzy oraz w sektorze militarnym (na poziomie strategicznym, taktycznym i operacyjnym). Nie są to zatem zapisy uniwersalne, umożliwiające skuteczną implementację i stosowanie w odniesieniu do państw stojących na niższym poziomie rozwoju informatycznego, realizujących swoje funkcje władcze w środowisku faktycznego niedoboru czy też nieadekwatności posiadanych zasobów i infrastruktury cyfrowej. Wówczas kreowanie i zapewnianie cyberbezpieczeństwa sprowadza się najczęściej do górnolotnych sloganów, produkcji dokumentacji niemającej odzwierciedlenia w rzeczywistości,

penalizacji trywialnych zagrożeń sieciowych leżących najczęściej w gestii operatorów komercyjnego sektora IT, a nawet do swoistej mody i kultywowania poczucia przynależności do elitarnego klubu. Ponadto, jest to najczęściej wynikiem bezrefleksyjnego wdrażania zapożyczonych rozwiązań, stanowiących konglomerat ponownie zebranych i ogólnie znanych reguł funkcjonujących na niwie obowiązującego prawa.

Wszystkie wymienione powyżej problemy dotyczące sekurytyzacji pozostaną aktualne tak długo, jak nieobecne będą efektywne przepisy wynikające z faktycznej, a nie postulowanej współpracy międzynarodowej, zaś egzekwowanie prawa nie będzie skuteczne w odniesieniu do najistotniejszych zagrożeń na tym polu. Tymczasem, jak wspomniano, ogranicza się ono do najmniej szkodliwych i politycznie niepożądanych zjawisk, jak przejawy haktywizmu czy relatywnie banalne osiągnięcia *script kiddies* w postaci np. krótkotrwałej i nieszkodliwej w rzeczy samej zmiany wyglądu witryn na serwerze rządowym (*defacement*), utrzymywanym przez niekompetentnych administratorów. Co zresztą w tym przypadku skłania do zadania pytania o faktyczne przygotowanie rządowych specjalistów IT do prowadzenia działań obronnych w przypadku poważnego ataku o podłożu militarnym czy do zapobiegania niekorzystnym próbom wywołania określonych decyzji administracyjnych poprzez przejęcie cybertożsamości wpływowego decydenta politycznego, wycieku danych *&c*. W przeciwnym razie może powstać państwowy aparat represji, którego ostrze będzie skierowane przeciwko własnemu społeczeństwu, głównie w kontekście ochrony bieżących interesów klasy politycznej, przedsiębiorstw komercyjnych i pozostałych grup czerpiących zyski z sekurytyzacji cyberprzestrzeni. W tym kontekście warto wciąż ponawiać pytania kwestionujące automatyzm podejmowania decyzji i implementacji rozwiązań legislacyjnych. Od odpowiedzi zależy bowiem nie tylko przyszłość samej dziedziny cyberbezpieczeństwa, ale aktualne ramy wolności obywateli i ich potencjalna rola w ewentualnym cyberkonflikcie, ze wszystkimi tego faktu konsekwencjami.

PRZYPISY

1. Szerzej na ten temat: D. J. Beds, T. Stevens, *Cyberspace and the State: Toward a Strategy for Cyber-power*, Abingdon 2011.
2. Zob. M. Rothman, T. Brinkel, „Of Snoops and Pirates: Competing Discourses of Cyber Security", [w:] P. Ducheine, F. Osinga, J. Soeters [red.], *Cyber Warfare: Critical Perspectives*, Hague 2012, s. 49–71.

3. Advanced Research Projects Agency Network (ARPANET), koncepcja sieci opracowana i realizowana na uczelniach wyższych w Stanach Zjednoczonych od 1963 roku, wykorzystana przez Departament Obrony USA do celów wojskowych; jej efektem jest sieć Internet – obecnie zakończono już część cywilną projektu (w 1990 r.), część militarna jest nadal realizowana przez agencję DARPA.
4. Zob. R. Emmers, „Securitization", [w:] A. Collins [red.] *Contemporary Security Studies*, New York 2007, s. 110.
5. Ł. Fijałkowski, „Teoria sekurytyzacji i konstruowanie bezpieczeństwa", *Przegląd Strategiczny*, 2012, nr 1, s. 157, http://studia strategiczne.amu.edu.pl/wp-content/uploads/2013/03/12.FIJALKOWSKI.pdf.
6. Szerzej na ten temat: E. Tikk, K. Kaska, L. Vihul, *International Cyber Incidents: Legal Considerations*, Tallinn 2010, ss. 15-34.
7. Ł. Fijałkowski, op. cit., s. 157. .
8. A. Bright, *Estonia Accuses Russia of «Cyberattack»*, http://www.csmonitor.com/2007/0517/p99s01-duts.html, [dostęp: 12.03.2015 r.].
9. Zob. E. Tikk, K. Kaska, L. Vihul, op. cit., przypis 70, s. 22.
10. Ł. Fijałkowski, op. cit., s. 156.
11. Zob. J. Quiggin, „Y2Kbug May Never Bite", *Australian Financial Review*, 2 September 1999 ,http://web.archive.org/web/20080524084926/http://www.uq.edu.au/economics/johnquiggin/news/Millennium9908.html.
12. Treść podręcznika na: https://ccdcoe.org/tallinn-manual.html [dostęp: 16.03.2015 r.].
13. Zob. dokument RFC 1855, https://www.ietf.org/rfc/rfc1855.txt [dostęp: 12.03.2015 r.].
14. E. Gartzke, „The Myth of Cyberwar. Bringing War in Cyberspace Back Down to Earth", *International Security*, 2013, vol. 38, issue 2, ss. 41–73 (http://www.mitpressjournals. org/doi/pdfplus/10.1162/ISEC_a_00136).
15. Szerzej na ten temat: Sean J.A. Edwards, *Swarming on the Battlefield: Past*, *Present*, *and Future*, Santa Monica 2000.
16. B. Pacek, R. Hoffmann, *Działania sił zbrojnych w cyberprzestrzeni*, Warszawa 2013, s. 8.
17. R. Grabowski, „Prawo w Internecie", [w:] R. Grabowski [red.], *Wpływ Internetu na ewolucję państwa i prawa*, Rzeszów 2008, s. 53.
18. Ł. Fijałkowski, op. cit., s. 151.
19. Szerzej na ten temat: M. Marczewska-Rytko [red.], *Haktywizm (cyberterroryzm*, *haking*, *protest obywatelski*, *cyberaktywizm*, *e-mobilizacja)*, Lublin 2014.
20. R. Grabowski, op. cit., s. 57.
21. Ł. Fijałkowski, op. cit., s. 157.