Cyberwojna czy cyberpokój?

27 kwietnia 2016

W 2007 r., podczas konfliktu władz Estonii z mniejszością rosyjską i samą Rosją, ta była republika radziecka stała się obiektem zmasowanych cyberataków. Jak stwierdza Andreas Schmitt z Uniwersytetu Technicznego w Delft (Holandia), „zagroziły one dostępności i funkcjonalności usług kluczowych dla funkcjonowania społeczeństwa estońskiego", przy czym wygląda na to, że po raz pierwszy w historii użyto ich jako „środka przymusu w konflikcie politycznym z jakimś państwem". Od tego czasu fale cyberataków przeżyły również Gruzja i Ukraina. Światu grożą cyberwojny.

Społeczeństwa uprzemysłowione stopniowo stworzyły „globalną wioskę", proroczo nazwaną tak w 1967 r. przez Marshalla McLuhana: coraz większa część codziennej działalności każdego z nas zależy od tej samej wolnej i otwartej sieci Internetu. Kiedy jednak w cyberprzestrzeni mamy do czynienia z interesami wojska, życie cywilne znajduje się na pierwszej linii. Mówiąc słowami raportu o francuskiej strategii obrony i bezpieczeństwa systemów informacyjnych, sytuacja ta czyni z cyberprzestrzeni zarówno „nową wieżę Babel", jak i „nowe Termopile" [1]. Żyje się w niej, a jednocześnie toczy się w niej walkę.

Mnożące się tam konflikty międzypaństwowe często nazywa się „cyberwojną", choć żaden akt przemocy informatycznej nie wywołał jeszcze zbrojnego konfliktu [2]. Nazwa ta urzeka tym bardziej, że współgra z tłem kulturowym, odkąd w 1983 r. na ekrany wszedł hollywoodzki film „Gry wojenne" i do tego stopnia ukształtował wspólne imaginarium, że wywarł wpływ na politykę publiczną w dziedzinie prowadzenia wojen cyfrowych [3].

ROSJA W AWANGARDZIE, USA TUŻ ZA NIĄ

Cyberwojna pojawiła się na okładce tygodnika Time już w 1995 r., ale dopiero w 2007 r. doszły na wielką skalę do głosu cyfrowe moce ofensywne i defensywne państw, najpierw w serii cyberataków przeprowadzonych z Rosji na serwery instytucji państwowych, banków i mediów Estonii. Następnie, w 2008 r., obiektem podobnych napaści padły serwery państwowe Gruzji. W 2014 r., po Majdanie i wybuchu konfliktu z Rosją, fale cyberataków nękały Ukrainę. Incydenty te potwierdziły, że mają rację ci stratedzy, którzy uważają, iż cyberataki należą obecnie do środków stosowanych w konfliktach międzynarodowych lub dwustronnych. Ilustrowały one również szczególne stosunki zachodzące między sferą cywilną a sferą wojskową: to dzięki nieformalnej pracy i współdziałaniu estońskiej społeczności technicznej państwu temu udało się wyjść z czegoś, co estoński minister obrony Jaak Aaviksso nazwał stanem zagrożenia dla bezpieczeństwa narodowego [4].

Wydarzenia te zachęciły wielkie mocarstwa do organizowania się. W 2010 r. w ramach United States Strategic Command (USSTRATCOM) oficjalnie utworzono United States Cyber Command (USCYBERCOM), którego kwatera znajduje się w Fort Meade (stan Maryland). Gen. Keith Alexander, który od 2005 r. kierował Agencją Bezpieczeństwa Narodowego (NSA), stanął również na czele tej nowej struktury. Jej misja polega, według Departamentu Obrony, na „zapewnieniu Stanom Zjednoczonym i ich sojusznikom swobody działania w cyberprzestrzeni” przy jednoczesnym „pozbawianiu tej swobody” ich nieprzyjaciół [5]. Ten sam człowiek, admirał Mike Rogers, kieruje dziś zarówno USCYBERCOM, jak i NSA i obie te funkcje pozostają pod tym samym dowództwem, wbrew zaleceniom poczynionym po sprawie Edwarda Snowdena przez prezydenta Baracka Obamę [6].

W czerwcu 2010 r. doszło do jednego z najbardziej symbolicznych wydarzeń we współczesnej cyberwojnie. Grupa badaczy białoruskich wykryła robaka komputerowego, który pozwalał atakować systemy przemysłowe elektrowni Siemensa, a zwłaszcza elektrowni atomowych i hydroelektrowni. Program ten,

nazwany Stuxnetem, to pierwsza „cyberbroń” przypadkiem znaleziona „w przyrodzie”, tzn. samoreplikująca i szerząca się w światowej sieci. New York Times ujawnił w czerwcu 2012 r., że chodzi o wyrób amerykański i izraelski, początkowo użyty przeciwko wirówkom wzbogacającym uran, które władze irańskie zainstalowały w Natanz, i wytworzony w ramach programu szpiegostwa informatycznego, zwanego Olympic Games. Cyberwojna nie ma ani reguł, ani konturów, ale pierwsze wystrzały już w niej padły.

Ma ona również swoje wojska. Kiedy dziennikarze Wall Street Journal postanowili sporządzić spis „cyberbroni” na świecie, co jest bardzo trudnym zadaniem, ponieważ panuje tu daleko idąca nieprzejrzystość, okazało się, że co najmniej 29 państw dysponuje jednostkami wojskowymi lub wywiadowczymi formalnie przeznaczonymi do prowadzenia działań ofensywnych w „sferze cyber” – główne z tych państw to Stany Zjednoczone, Rosja, Chiny, Iran, Izrael i Korea Północna. Do tego dochodzi 50 państw, które w podobnych celach zakupują oprogramowania i gotowe narzędzia do hackingu. Uwagę badaczy zwracają na siebie wyroby Hacking Team, Fin Fisher czy Zerodium, ale przemysł ten troszczy się o dyskrecję. „Cyberwojna powoduje nowy wyścig zbrojeń”, stwierdzają autorzy badań przeprowadzonych przez Wall Street Journal [7]. Mądrość wojskowa głosi, że „wszelki konflikt ma obecnie wymiar cyber”, co ze względu na inflację sprzętu może być samorealizującą się przepowiednią.

NIE MA TAM CZEGOŚ TAKIEGO, JAK PRAWORZĄDNOŚĆ

O ile moce państwowe organizują się i kształtują od 2008 r., o tyle ramy prawne takich działań cyber pozostają niejasne. Były dyrektor NSA i Centralnej Agencji Wywiadowczej (CIA) gen. Michael Hayden chętnie to przyznaje i w związku z tym cytuje wypowiedź prezydenta Estonii Toomasa Hendrika Ilvesa. Powiedział on, że z powodu braku umowy społecznej w duchu Locke’a cyberprzestrzeń stanowi niemal czysto hobbesowski świat, w którym nie obowiązują żadne reguły, a „życie człowieka”, jak pisał autor Lewiatana, „jest samotne, biedne,

bez słońca, zwierzęce i krótkie”[8]. A zatem, skomentował Hayden, „po prostu nie ma tam czegoś takiego jak praworządność” [9].

W 2009 r. z inicjatywy afiliowanego do NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) z siedzibą w stolicy Estonii międzynarodowa grupa ekspertów przystąpiła do niezależnej pracy akademickiej nad międzynarodowymi ramami prawnymi, które miałyby zastosowanie do konfrontacji w cyberprzestrzeni. Opublikowany przez tę grupę w 2013 r. Podręcznik talliński stara się odpowiedzieć na następujące pytanie: jeśli międzynarodowe prawo konfliktów zbrojnych ma zastosowanie w cyberprzestrzeni, a z pewnością tak jest, to na czym to polega? [10] Prace te, wychodzące od hipotetycznych reguł mających zastosowanie w okresie konfliktu zbrojnego, a nie od norm, które obowiązują w sporach międzypaństwowych w czasach pokoju, odzwierciedlają stan debat między wielkimi mocarstwami w tej dziedzinie.

Militaryzacja cyberprzestrzeni postępuje znacznie szybciej niż konstrukcja mechanizmów pokoju pozytywnego, która powinna jej towarzyszyć. Dopiero w 2012 r., w wyniku wspólnej inicjatywy Brazylii, Nigerii, Stanów Zjednoczonych, Szwecji, Tunezji i Turcji, Organizacja Narodów Zjednoczonych uznała, że prawa człowieka muszą mieć również zastosowanie online, niezależnie od tego, o jakie media chodzi i bez względu na jakiekolwiek granice. Dopiero w 2013 r. w raporcie Grupy Ekspertów Rządowych Pierwszej Komisji ONZ do spraw Rozbrojenia i Bezpieczeństwa Międzynarodowego oświadczono, że prawo międzynarodowe, a zwłaszcza Karta Narodów Zjednoczonych, ma zastosowanie w cyberprzestrzeni [11]. Teraz konieczne jest określenie, jak to prawo międzynarodowe można wdrażać.

Inną osobliwością wyścigu zbrojeń w sferze cyber jest to, że toczy się on w niestabilnym i ruchomym kontekście, gdzie dyskusyjne jest nawet to, co to jest cyberkonflikt. James Clapper, dyrektor amerykańskiego Wywiadu Narodowego (DNI), poproszony w lutym 2016 r. przez senacką komisję sił zbrojnych

o zdefiniowanie rodzajów cyberataków czy cyberincydentów, które mogłyby spowodować ripostę wojskową, odpowiedział wymijająco: „Jest to kwestia percepcji.” Gen. Vincent Stewart, kierujący Agencją Wywiadowczą Departamentu Obrony (DIA), wyjaśnił, że nie byłoby słuszne zaliczanie wszystkich wydarzeń cyber jako ataków, niezależnie od tożsamości tych, którzy się ich dopuszczają, i od ich motywacji. „Pożyteczne”, stwierdził, „byłoby odróżnienie incydentów cyber od aktów wojennych.” [12] Kontrowersja ożywa wraz z każdym incydentem. W listopadzie 2014 r. atak informatyczny na Sony Pictures Entertainment wywołał kakofonię: w Stanach Zjednoczonych jedni uważali, że jest to akt „cyberterroryzmu” czy „cyberwojny”, a inni – że to „zwykły hack”, przejaw „hacktywizmu”, który można podciągnąć pod „cyberprzestępstwo”. Spór przesądził Obama mówiąc, że to akt „cyberwandalizmu”.

Praktyczne skutki tej debaty semantycznej są fundamentalne dla demokracji: określają ramy prawne, które mają tu zastosowanie, konsekwencje i zamieszanych w takie akty aktorów. W „realu”, tzn. poza linią, nie stawia się armii w stan gotowości z powodu rozbitej płyty chodnikowej. W cyberprzestrzeni taka przesadna reakcja jest możliwa. W miarę bowiem wzrostu zależności społeczeństw od Internetu muszą one dostosowywać swoje prawa i mechanizmy społeczne do potrzeb zachowania pokoju, sprawiedliwości i bezpieczeństwa – i to w kontekście, w którym światowe kompleksy wojskowo-przemysłowe rozwijają i narzucają intruzywne metody kontroli.

PLAC ZABAW CZY POLE BITWY?

A przecież pierwsi architekci sieci i cyberlibertarianie marzyli o cyberprzestrzeni wymykającej się spod wszelkiej kontroli państwowej, niezależnej od suwerenności, której hołdują „znużone giganty z mięsa i stali”, jak to pisał poeta John Perry Barlow w Deklaracji Niepodległości Cyberprzestrzeni [13]. Takiej wizji gen. Hayden przeciwstawia wizję cyberprzestrzeni pomyślanej jako piąta domena operacji wojskowych – po lądzie, przestrzeni, morzu i powietrzu: „Gdy

rzucimy okiem w przeszłość, to okaże się, że nie zdawaliśmy sobie sprawy, iż istniało wówczas całe pokolenie, które uważało cyberprzestrzeń za globalne dobro wspólne, za dziewiczy plac zabaw, a nie za potencjalną strefę konfliktu między potężnymi państwami narodowymi. Debata o tych konkurujących ze sobą archetypach trwa do dziś." [14] Cyberprzestrzeń nie jest ani strefą zmilitaryzowaną, ani dziewiczym placem zabaw; wydaje się raczej, że konflikty, które szerzą się w tej przestrzeni, zarysowują w niej szarą strefę.

Jeśli „szara strefa" tak często cechuje cyberwojnę, to dlatego, że jest ona nieodłączna od samego pojęcia cyberwojny. Pojawiła się już w pierwszych pracach poświęconych zagadnieniom strategii działania państw w cyberprzestrzeni. Np. w Stanach Zjednoczonych jedna z pierwszych definicji „wojny informacyjnej" i jej skutków strategicznych sięga 1976 r. W sporządzonym dla Boeinga raporcie Thomas Rona, doradca naukowy Departamentu Obrony, zdefiniował taką wojnę jako „rywalizację na szczeblu strategicznym, operacyjnym i taktycznym, prowadzoną przez całe spektrum pokoju, kryzysu, eskalacji kryzysu, konfliktu, wojny, zakończenia wojny i odbudowy/renowacji między rywalami, przeciwnikami czy wrogami przy użyciu środków informacji w celu osiągnięcia postawionych sobie celów" [15] – a zatem jako rywalizację, które rozwija się zarówno w czasach pokoju, jak i w czasach wojny.

Niejasność terminu cyberwojna przyczynia się do wzrostu ryzyka wybuchu takiej wojny i termin ten uniemożliwia objęcie sytuacji, które opisuje, jasnymi ramami prawnymi. Powinien zatem budzić nieufność: nie pozwala myśleć o pokoju w cyberprzestrzeni – tam, gdzie jutro pokój będzie nam bardzo potrzebny.

Autorstwo: Camille François
Tłumaczenie: Zbigniew M. Kowalewski
Źródło: Monde-Diplomatique.pl

PRZYPISY

[1] „La stratégie de la France en matičre de cyberdéfense et cybersécurité”, Agence nationale de la sécurité des systčmes d’information, Paryż, luty 2011 r.

[2] Th. Rid, „Cyber War Will Not Take Place”, Oksford – Nowy Jork, Oxford University Press 2013.

[3] S. Ricker Schulte, „Cached: Decoding the Internet in Global Popular Culture”, Nowy Jork, New York University Press 2013.

[4] A. Schmidt, „The Estonian Cyberattacks”, w: J. Healey (red.),” A Fierce Domain: Conflict in Cyberspace, 1986 to 2012″, Wiedeń, Cyber Conflict Studies Association 2013.

[5] „U.S. Cyber Command – U.S. Strategic Command”, www.stratcom.mil.

[6] „Liberty and Security in a Changing World. Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies”, Biały Dom, Waszyngton, 12 grudnia 2013 r., www.whitehouse.gov.

[7] D. Paletta, D. Yadron, J. Valentino-DeVries, „Cyberwar Ignites a New Arms Race”, „The Wall Street Journal”, 11 października 2015 r.

[8] Th. Hobbes, „Lewiatan czyli materia, forma i władza państwa kościelnego i świeckiego” (tłum. Cz. Znamierowski), Warszawa, PWN 1954, s. 110.

[9] M.V. Hayden, „The Making of America’s Cyberweapons”, The Christian Science Monitor, 24 lutego 2016 r.

[10] M.N. Schmitt (red.), „Tallinn Manual on the International Law Applicable to Cyber Warfare”, Cambridge – Nowy Jork, Cambridge University Press 2013.

[11] „Rapport du groupe d’experts gouvernementaux chargé d’examiner les progrčs de la téléinformatique dans le contexte de la sécurité internationale”, Nowy Jork, ONZ, 24 czerwca 2013 r.

[12] „Worldwide Threats”, United States Senate Committee on Armed Services, Waszyngton, 9 lutego 2016 r., www.armed-services.senate.gov.

[13] J.P. Barlow, „Deklaracja Niepodległości Cyberprzestrzeni” (tłum. P. Majewski), „Przegląd Filozoficzno-Literacki” nr 1 (22), 2009.

[14] M.V. Hayden, op. cit.

[5] Cyt. za: P. Stephenson, „Investigating Computer-Related Crime: A Handbook for Corporate Investigators”, Londyn – Nowy Jork, CRC Press 1999, s. 7.