PISM | POLSKI INSTYTUT SPRAW MIĘDZYNARODOWYCH
THE POLISH INSTITUTE OF INTERNATIONAL AFFAIRS

BIULETYN

Nr 31 (1007), 26 marca 2013 © PISM

Prawo konfliktów zbrojnych a cyberprzestrzeń

Rafał Tarnogórski

W cyberprzestrzeni granica między pokojem a wojną staje się coraz bardziej umowna. Zarazem zapewnienie ochrony infrastruktury sieciowej staje się jednym z podstawowych celów strategicznych w obszarze bezpieczeństwa państwa. Nie ma norm traktatowych dotyczących operacji militarnych w cyberprzestrzeni, choć może być ona wykorzystana do ataku terrorystycznego czy informatycznego na skalę agresji militarnej. Tę lukę należy wypełnić w formie międzynarodowej konwencji. Opracowanie takiego dokumentu leży w interesie całej społeczności międzynarodowej.

W ostatnich tygodniach prasę światową obiegła informacja, że w strukturze Chińskiej Armii Ludowo-Wyzwoleńczej wykryto rzekomo jednostkę 61398, zajmującą się cyberszpiegostwem. Spowodowało to wzrost zainteresowania światowej opinii publicznej militarnym i wywiadowczym zastosowaniem nowych technologii informatycznych. Nawet jeśli informacji tych nie da się potwierdzić, jest pewne, że Chiny – tak jak wszystkie mocarstwa – mają w swoich strukturach tego rodzaju jednostki, których zadaniem jest rozwijanie elektronicznych narzędzi służących ofensywnym działaniom w cyberprzestrzeni. Wykorzystanie technologii informatycznych stanowi bowiem przedmiot wzrastającego zainteresowania sił zbrojnych i organizacji wywiadowczych różnych krajów. Podejrzenia o udział państw w cyberatakach na dużą skalę towarzyszą takim zdarzeniom niemal zawsze, począwszy od ataku hakerskiego na Estonię w 2007 r. (przypisywanego służbom rosyjskim), przez operacje sabotażowe podczas wojny rosyjsko-gruzińskiej w 2008 r. (blokada gruzińskich rządowych stron internetowych), wykrycie w 2009 r. robaka Stuxnet (prawdopodobnie amerykańsko-izraelski sabotaż irańskiego programu atomowego), a także programów szpiegowskich Flame, Mahdi i Red October (2012), mających za zadanie wydobycie wrażliwych danych z europejskich i amerykańskich serwerów (ataki przypisywane podmiotom państwowym przez media, ale również przez ekspertów od bezpieczeństwa informatycznego). Trudno jednak o dowody, bo atak w cyberprzestrzeni utrudnia identyfikację agresora.

Wzrost militarnego znaczenia technologii cybernetycznych. Broń cybernetyczna dołączyła do arsenału środków współczesnego pola walki, zarazem jednak to, co tradycyjnie nazywano polem walki, uległo przekształceniu. Po ataku z 11 września 2001 r. na WTC Stany Zjednoczone wdały się w asymetryczny konflikt, wypowiadając terroryzmowi wojnę z użyciem tradycyjnych środków militarnych. Szybko zdano sobie sprawę, że również technologie informatyczne mogą być wykorzystane w procederze łamania prawa, ataku terrorystycznym czy ataku informatycznym na skalę agresji militarnej. Podobnie jak miało to miejsce w przypadku walki z terroryzmem, klasyczny zespół reguł prawnych regulujący prowadzenie konfliktów zbrojnych nie przewiduje takich przypadków i wymaga redefinicji. Konieczność ochrony infrastruktury internetowej jako integralnej części obszaru bezpieczeństwa państwa nie budzi żadnych wątpliwości. W przyjętej w 2011 r. amerykańskiej strategii w sprawie cyberprzestrzeni Stany Zjednoczone bezpośrednio wyraziły gotowość odpowiedzi na cyberatak za pomocą środków wojskowych. Pojęcie cyberataku pojawiło się także w strategicznych dokumentach dotyczących bezpieczeństwa innych państw, m.in. Wielkiej Brytanii, Kanady, Rosji; znalazło się również w oficjalnym polskim dokumencie rządowym – programie ochrony cyberprzestrzeni RP na lata 2011–2016.

Potrzeba międzynarodowej regulacji. Cyberprzestrzeń ma wymiar publiczny (obejmujący tzw. infrastrukturę krytyczną, ale także sieci używane przez przedsiębiorstwa czy elementy tzw. e-administracji), który powinien podlegać ochronie, również międzynarodowej, istotnej zwłaszcza w przypadku konfliktów zbrojnych. Dlatego ostatnio coraz częściej podnoszona jest idea regulacji traktatowej tego zagadnienia. W marcu br. ukazał się *Tallinn Manual on the International Law Applicable to Cyber Warfare* powstały z inicjatywy NATO Cooperative Cyber

Defence Centre of Excellence w Tallinnie. Praca ta szczegółowo analizuje problemy związane z prawem konfliktów zbrojnych w cyberprzestrzeni. Nie stanowi ona zbioru obowiązującego prawa międzynarodowego, zawiera tylko sugerowane rozwiązania, nawet w opinii samych autorów podlegające jeszcze dyskusji. Mimo zastrzeżeń wyznaczy jednak ramy normatywne dla działań zbrojnych w cyberprzestrzeni, ponieważ prawdopodobnie zostanie uwzględniona przy tworzeniu narodowych legislacji. Jej główną zaletą jest uwidocznienie obszarów wymagających regulacji: kiedy mamy do czynienia z atakiem cybernetycznym, kto i co może być uprawnionym celem ataku.

Opracowanie podręcznika jasno ukazuje, że trzeba ustalić nowe zasady, ponieważ istniejące reguły nie obejmują nowych okoliczności, chociaż mogą być zastosowane przez analogię. Na przykład Karta NZ uznaje niezbywalne prawo państwa do samoobrony w przypadku napaści zbrojnej, do czasu podjęcia przez Radę Bezpieczeństwa działań w celu utrzymania międzynarodowego pokoju i bezpieczeństwa. Wydaje się, że nie ma przeszkód, by taką napaścią mógł być cyberatak, a przynajmniej taki, który wywołał skutki podobne lub zbliżone do tych, jakie osiągnięto by za pomocą akcji militarnej. Jednak samoobrona podjęta wskutek takiego cyberataku podlega ograniczeniu. Decydujące dla uznania działania państwa jako podjętego w samoobronie są zasady konieczności i proporcjonalności, rozpatrywane w kontekście konkretnego przypadku. Użycie siły militarnej w konsekwencji cyberataku nie jest przez prawo międzynarodowe zakazane, jednak jego legalność będzie podlegała ocenie w oparciu o wymienione wyżej kryteria. W związku z powyższym wydaje się, że cyberatak wymierzony w tzw. infrastrukturę krytyczną państwa może być prawnie uznany za akt agresji zbrojnej pociągający za sobą konwencjonalne środki odwetowe. Jednak nawet obecnie państwa nie mają pełnej swobody działania, podlegają bowiem obowiązującym regułom, nawet jeżeli są one niedoskonałe. Międzynarodowe prawo humanitarne, zwłaszcza konwencje genewskie, mają zastosowanie w razie powstania jakiegokolwiek konfliktu zbrojnego, nawet gdyby nie uznano tego za stan wojny. Odpowiednie reguły będą stosowane także w przypadku wybuchu konfliktu zbrojnego niemającego charakteru międzynarodowego. Zatem w świetle prawa humanitarnego z wojną zostają zrównane wszelkie inne konflikty zbrojne. Kategoria „inne konflikty" powinna obejmować również cyberkonflikty. Stwierdzenie to ma poważne konsekwencje. Prawo humanitarne określa chronione kategorie osób i dóbr w razie wojny, a ich przekroczenie stanowi zbrodnię wojenną. Zatem także bezprawny cyberatak na infrastrukturę cywilną podlegającą konwencyjnej ochronie, np. szpital, może być uznany za taką zbrodnię, a osoby za to odpowiedzialne – ścigane, również za pośrednictwem Międzynarodowego Trybunału Karnego.

Konsekwencje i wnioski. Nie istnieją międzynarodowe normy traktatowe dotyczące operacji militarnych w cyberprzestrzeni. Jest to luka, której nie wypełni opracowany pod auspicjami NATO podręcznik, wymaga ona bowiem usystematyzowania w formie obowiązującego międzynarodowoprawnie dokumentu. W takiej materii nie powinno być wątpliwości co do zasadniczych reguł prawnych. Te ustanowić może wielostronna konwencja odnosząca się do cyberprzestrzeni. W dobrze pojętym interesie społeczności międzynarodowej leży opracowanie uzgodnionych zasad jasno określających, co jest dozwolone prawem, a co nie. Prace nad taką konwencją powinien objąć patronatem Międzynarodowy Komitet Czerwonego Krzyża, a odpowiednie zasady prawne powinny zostać opracowane przez ONZ-owską Komisję Prawa Międzynarodowego, jako organ cieszący się uznanym autorytetem w zakresie postępowego rozwoju prawa międzynarodowego. Opracowanie takiego dokumentu w formie obowiązującego aktu prawa międzynarodowego nie koliduje z polskimi interesami, a prace legislacyjne nad projektem konwencji mogłyby zyskać szerokie międzynarodowe poparcie: sojuszników z NATO i UE, ale także z Rosji czy Chin (które w 2011 r. na forum ONZ wystąpiły z propozycją opracowania wiążących reguł w zakresie bezpieczeństwa informacyjnego (International Code of Conduct for Information Security).

Polski plan ochrony cyberprzestrzeni przed zagrożeniami w wymiarze wewnętrznym został ujęty we wspomnianym programie ochrony cyberprzestrzeni RP na lata 2011–2016. Sformułowano tam ramy legislacyjne (potrzeba określenia nowych zakresów zadań, odpowiedzialności i zmian w strukturach organizacyjnych organów państwa i służb ochrony cyberprzestrzeni, tj. odpowiednio ABW i SKW); proceduralno-organizacyjne (ze szczególną rolą Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz planowanego Międzyresortowego Zespołu do spraw Koordynacji Ochrony Cyberprzestrzeni RP) i techniczne ochrony polskiej cyberprzestrzeni. Jednak militarne aspekty bezpieczeństwa pozostawiono poza spektrum dokumentu. Polska powinna jak najszybciej zbudować zdolności obronne odparcia cyberataku w oparciu o struktury wojskowe, z możliwością adekwatnej odpowiedzi na poważne naruszenia polskiej cyberprzestrzeni nawet za pomocą konwencjonalnych środków wojskowych.