Miron Lakomy

"Cyber War The Next Threat to National Security and What to Do About It", Richard A. Clarke, Robert K. Knake, New York 2010 : [recenzja]

Studia Politicae Universitatis Silesiensis 11, 316-320

2013

Richard A. Clarke, Robert K. Knake: *Cyber War*
The Next Threat to National Security and What to Do About It
New York: Ecco, 2010, ss. 290.

Richard A. Clarke jest jednym z najbardziej uznanych amerykańskich specjalistów zajmujących się problematyką terroryzmu i cyberbezpieczeństwa. Pełnił on wiele ważnych funkcji w administracji Stanów Zjednoczonych. Był między innymi doradcą w Departamencie Stanu w latach osiemdziesiątych XX wieku, członkiem Rady Bezpieczeństwa Narodowego USA oraz Narodowym Koordynatorem ds. Bezpieczeństwa, Ochrony Infrastruktury i Antyterroryzmu. Do 2003 roku pełnił również funkcję specjalnego doradcy ds. cyberbezpieczeństwa Georga W. Busha. Niezwykle bogate doświadczenie zawodowe pozwoliło mu zapoznać się w praktyce z nowymi wyzwaniami dla bezpieczeństwa narodowego i międzynarodowego we współczesnym świecie. Robert K. Knake z kolei jest członkiem Council on Foreign Relations, gdzie pracuje jako ekspert ds. cyberbezpieczeństwa. Pełnił również funkcję doradcy amerykańskiego Departamentu Bezpieczeństwa Wewnętrznego.

Książka *Cyber War. The Next Threat to National Security and What to Do About It* jest jedną z pierwszych, spójnych prób ukazania implikacji rosnącego uzależnienia Stanów Zjednoczonych od technologii informatycznych i sieci komputerowych. Dynamiczny rozwój Internetu od początku lat dziewięćdziesiątych XX wieku może być oceniany z dwóch perspektyw. Z jednej strony, przyniósł on ludzkości ogromne korzyści, pozwalające na dokonanie historycznego skoku technologicznego. Z drugiej jednak, powszechne wykorzystanie komputerów i sieci rodzi również coraz poważniejsze zagrożenia dla bezpieczeństwa państw.

Pozycja ta jest ujęciem o tyle ciekawym, że jej Autorzy w odróżnieniu od Autorów innych tego typu publikacji, pomijają w dużej mierze kwestie teoretyczne. Skupiają się za to na aspektach praktycznych, częstokroć opartych na

doświadczeniach R.A. Clarke'a jako koordynatora ds. cyberbezpieczeństwa w administracji Stanów Zjednoczonych. Monografię napisaną na podstawie analizy pierwszych poważnych incydentów w cyberprzestrzeni (operacja „Orchard", Estonia 2007, Gruzja 2008) można traktować jako próbę odpowiedzi na pytania: Jak może wyglądać w przyszłości pierwsza cyberwojna? oraz: W jaki sposób należałoby jej zapobiec? Próby tej Autorzy dokonują na przykładzie teoretycznego konfliktu dwóch największych potęg w tej dziedzinie — Stanów Zjednoczonych i Chin.

Główną tezą książki Richarda A. Clarke'a i Roberta E. Knake'a jest stwierdzenie, iż szkodliwych działań państw w cyberprzestrzeni nie należy interpretować jedynie jako kolejnego etapu ewolucji zjawiska wojny. Sieci komputerowe, zdaniem Autorów, dają bowiem państwom rosnące możliwości zadawania szkód innym uczestnikom stosunków międzynarodowych, przy relatywnie niewielkim zagrożeniu odwetem. Wykorzystanie cyberprzestrzeni do ataku na elementy infrastruktury krytycznej mogłoby mieć niezwykle poważne konsekwencje nie tylko militarne czy gospodarcze, ale przede wszystkim humanitarne. Jeśli w najbliższym czasie nie zostaną wypracowane odpowiednie mechanizmy zapobiegania cyberwojnie lub przynajmniej kontroli cyberzbrojeń, w przyszłości efekty tych zaniedbań mogą być trudne do przewidzenia. Według Autorów, rozwiązaniem powinna być więc nie „walka w cyberprzestrzeni, ale walka przeciw cyberwojnie".

Książka składa się z ośmiu rozdziałów oraz glosariusza. W rozdziale pierwszym, *Trial Runs*, omówiono dotychczasowe przypadki szkodliwego wykorzystania cyberprzestrzeni przez państwa. Richard A. Clarke w niezwykle przystępny sposób, wyjaśniając kwestie technologiczne, charakteryzuje wiele przykładów: izraelską operację „Orchard" przeciwko Syrii w 2007 roku, obie wojny w Iraku, cyberataki na Estonię oraz Gruzję oraz działania reżimu Korei Północnej. Analiza tych wydarzeń jest niezwykle interesująca, gdyż oprócz informacji powszechnie dostępnych, Clarke przytacza liczne wiadomości znane dotychczas jedynie przedstawicielom amerykańskiej administracji. Co ciekawe, Autor wspomniał, że już podczas operacji „Pustynna burza" istniała możliwość sparaliżowania irackiego systemu dowodzenia i obrony przeciwlotniczej za pomocą cyberataku. Wówczas jednak tego typu rozwiązania zostały odrzucone przez amerykańskie dowództwo. Inną decyzję podjęto w 2003 roku, kiedy tuż przed atakiem wojsk amerykańskich iraccy dowódcy otrzymali wiadomości drogą elektroniczną, nawołujące do porzucenia broni i powrotu do domów. Jak dowodzi Clarke, znaczna część kadry oficerskiej armii irackiej poddała się tej sugestii. Ciekawie ujęto również szkodliwe działania Rosji i Korei Północnej w cyberprzestrzeni w drugiej połowie pierwszej dekady XXI wieku.

Rozdział drugi, *Cyberwarriors*, poświęcony został ewolucji amerykańskiego spojrzenia na walkę w cyberprzestrzeni. Wątek ten rozpoczyna cha-

rakterystyka nowego pojęcia dla amerykańskiej opinii publicznej — „cyberwojowników" — czyli żołnierzy amerykańskiej armii zajmujących się działaniami ofensywnymi i defensywnymi w cyberprzestrzeni. Autorzy omawiają również poszczególne etapy ewolucji amerykańskiego spojrzenia na cyberbezpieczeństwo. W dalszej części rozdziału łączą to zagadnienie z zagrożeniem ze strony Chin. Zdaniem R.A. Clarke'a, operacja „Pustynna Burza" była dla ChRL w dużej mierze szokiem. Zastosowanie inteligentnych środków walki i niespodziewanie łatwe pokonanie armii irackiej wpłynęło na zmianę koncepcji rozwoju chińskich sił zbrojnych. Analizując doświadczenia irackie, decydenci w Pekinie doszli do wniosku, iż w przypadku potencjalnego starcia ze Stanami Zjednoczonymi niezbędna będzie broń, która pozwoliłaby zniwelować przewagę technologiczną USA. Takie możliwości otworzyła cyberprzestrzeń, która od lat dziewięćdziesiątych XX wieku stała się sferą szczególnego zainteresowania chińskiej armii. Dowodem na to są między innymi plany Chińskiej Armii Ludowo-Wyzwoleńczej sparaliżowania amerykańskich grup lotniskowców, systemów dowodzenia czy systemu elektroenergetycznego USA w wypadku konfliktu, np. wokół Tajwanu.

Rozdział trzeci, *Battlespace*, stanowi omówienie wymiaru, w którym toczy się cyberwojna. Autorzy dokonują tu interesującej charakterystyki cyberprzestrzeni, wychodząc od popularnych wyobrażeń z filmu *Matrix*. Ich zdaniem, cyberprzestrzeń „jest wszędzie, wszędzie tam, gdzie jest komputer, procesor albo kabel, który je łączy". Na tej podstawie przedstawiają oni jedne z ciekawszych definicji cyberprzestrzeni oraz hakeryzmu. Dokonują także charakterystyki samego zjawiska cyberwojny, wymieniając i szeroko opisując wiele jej cech. Skupiają się tu przede wszystkim na problemach związanych z samą strukturą komputerów oraz Internetu. Co ciekawe, Autorzy omawiają także pierwszy przypadek szkodliwego wykorzystania sieci komputerowych przez Centralną Agencję Wywiadowczą przeciwko Związkowi Radzieckiemu na początku lat osiemdziesiątych XX wieku.

Rozdział czwarty, *The Defense Fails*, dotyczy przede wszystkim błędów popełnionych przez amerykańską administrację w dziedzinie bezpieczeństwa teleinformatycznego cyberbezpieczeństwa. Autorzy zwracają szczególną uwagę na dysproporcje między zdolnościami ofensywnymi i defensywnymi USA w cyberprzestrzeni oraz reperkusjach tychże dla bezpieczeństwa narodowego. Mimo że polityka cyberbezpieczeństwa Stanów Zjednoczonych należy obecnie do najbardziej zaawansowanych na świecie, R.A. Clarke i R.E. Knake wytykają liczne jej błędy, w okresie prezydentury zarówno B. Clintona, G.W. Busha, jak i B. Obamy. Za główny problem uznają oni przede wszystkim brak rozwiązań chroniących cywilne sieci komputerowe, na których opiera się znaczna część infrastruktury krytycznej. W tym kontekście omawiana jest ponownie dysproporcja między zdolnościami ofensywnymi i defensywnymi USA. Próbując ukazać podstawowe znaczenie tego rodzaju zaniedbań, odwo-

łują się oni do wielu przykładów, między innymi operacji „Titan Rain" z 2003 roku. Co ciekawe, zdaniem Autorów, rosnąca zależność Stanów Zjednoczonych od sieci teleinformatycznych, mimo ogromnego potencjału ofensywnego, stawia USA w zdecydowanie gorszej pozycji niż kraje mniej zaawansowane technicznie, na przykład Chiny. Końcowa część rozdziału stanowi próbę odpowiedzi na pytanie: W jaki sposób należałoby zabezpieczyć cyberprzestrzeń USA? Poruszono tu również problem zasadniczego rozdźwięku między wymogiem przestrzegania podstawowych praw obywatelskich, prywatności w Internecie a potrzebą zapewnienia bezpieczeństwa narodowego.

Rozdział piąty, *Toward a Defensive Strategy*, stanowi przegląd rozwiązań, które, zdaniem Clarke'a i Knake'a, byłyby niezbędne do zapewnienia bezpieczeństwa narodowego USA w cyberprzestrzeni. Pierwszą część rozdziału stanowi w zasadzie lista pytań, które powinny być podstawą opracowania spójnej strategii w tej dziedzinie. Na tej podstawie Autorzy proponują wprowadzenie tak zwanej defensywnej triady. Zastanawiają się także nad rolą zdolności obronnych w cyberprzestrzeni oraz zjawiskiem odstraszania. Na koniec omawiają między innymi znaczenie firm dostarczających usługi internetowe, infrastruktury krytycznej czy zagadnienia wolności obywatelskich w kontekście cyberbezpieczeństwa.

Rozdział szósty, *How Offensive?*, stanowi kontynuację rozważań dotyczących cyberstrategii USA, tym razem z punktu widzenia działań ofensywnych. W celu zobrazowania licznych wątpliwości w tej dziedzinie, Autorzy odwołują się do stosunkowo prostej gry wojennej, która zakłada ograniczony konflikt między USA a Chinami. Zgodnie z przewidywaniami z poprzednich rozdziałów, w starciu w cyberprzestrzeni przewagę zyskują Chiny. Wynika to przede wszystkim ze zbyt dużej zależności USA od technologii informatycznych, w wymiarze zarówno wojskowym, jak i cywilnym. W rozdziale tym podjęto również zagadnienia wykorzystania prawa wojny w przypadku cyberkonfliktu oraz problemów związanych z działaniami odwetowymi.

Rozdział siódmy, *Cyber Peace*, został poświęcony w całości zagadnieniu kontroli zbrojeń w cyberprzestrzeni. Clarke i Knake na kilkudziesięciu stronach omawiają wady i zalety ustanowienia systemu kontroli cyberzbrojeń, przede wszystkim z punktu widzenia amerykańskiego interesu narodowego. Wynikiem tych rozważań jest konstatacja, iż Stany Zjednoczone powinny poprzeć próby wypracowania międzynarodowego systemu kontroli zbrojeń w cyberprzestrzeni.

Wreszcie w rozdziale ósmym, *The Agenda*, Autorzy formułują konkretne propozycje zreformowania amerykańskiej polityki cyberbezpieczeństwa. Wymieniają tu między innymi uchwalenie nowej strategii w tej dziedzinie, lepszą ochronę infrastruktury krytycznej, współpracę z firmami dostarczającymi usługi internetowe oraz podjęcie próby wypracowania międzynarodowego traktatu regulującego zjawisko cyberwojny. Postulują również wpro-

wadzenie pełnego zakazu wykorzystania sieci do atakowania infrastruktury cywilnej oraz naruszania elementów międzynarodowego systemu finansowego.

Książka Richarda A. Clarke'a i Roberta E. Knake'a jest obecnie jedną z najciekawszych pozycji poruszających tematykę cyberwojny. Z jednej strony, przedstawia ona technologiczne wyzwania związane z działaniami w cyberprzestrzeni. Chodzi tu między innymi o wątpliwości związane z samą strukturą i funkcjonowaniem Internetu czy wykorzystaniem sieci Wi-Fi. Z drugiej strony, porusza ona wiele niezwykle ważnych aspektów teoretycznych, takich jak zagadnienie odstraszania, odpowiednia procedura decyzyjna czy kontrola cyberzbrojeń. O wysokiej wartości publikacji świadczy także fakt, iż rozważania te prowadzono na podstawie studiów przypadku, podając przy tym liczne informacje niedostępne dotychczas opinii publicznej.

Należy podkreślić, iż praca ta, dzięki zaakcentowaniu zasadniczego znaczenia cyberprzestrzeni dla bezpieczeństwa narodowego i międzynarodowego, spotkała się w Stanach Zjednoczonych z głosami ograniczonej krytyki. Zdaniem części komentatorów potencjalne cyberwojenne zagrożenia nie muszą być aż tak poważne, jak przedstawili to Autorzy. Odpowiedź na pytanie: Kto ma rację w tym sporze, jest obecnie niezwykle trudna. Wynika to z podkreślonego zresztą przez R.A. Clarke'a, faktu, iż dotychczas państwa w cyberprzestrzeni ograniczały się do wykorzystywania jedynie najprostszych środków ataku, zachowując najbardziej wartościowe techniki na wypadek poważnego konfliktu zbrojnego. Prawdą jest jednak, iż obecna struktura cyberprzestrzeni oraz funkcjonujące zabezpieczenia otwierają hakerom szerokie możliwości działania. Dlatego też, jak postulują Autorzy, intensyfikacja starań o wyeliminowanie wieloletnich zaniedbań w tej dziedzinie jest sprawą o podstawowym znaczeniu dla bezpieczeństwa państw.

Reasumując, należy stwierdzić, iż opracowanie Richarda A. Clarke'a i Roberta E. Knake'a jest godne polecenia polskiemu Czytelnikowi, w szczególności politologom oraz badaczom stosunków międzynarodowych. Obok prac takich autorów jak Martin C. Libicki czy Jeffrey Carr, w pozycji tej najpełniej omówiono zjawisko cyberwojny jako nowego zagrożenia dla bezpieczeństwa narodowego i międzynarodowego.

Miron Lakomy