FOLIA 280

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 9(2) (2019)
ISSN 2657-8549
DOI 10.24917/26578549.9.2.1

ARTYKUŁY

Olga Wasiuta
ORCID ID 0000-0003-0481-1567
Uniwersytet Pedagogiczny w Krakowie

iWar – bezprecedensowa forma wojny internetowej

Rozwój technologiczny postępuje tak szybko, że współczesne społeczeństwo ma trudności z przystosowaniem się do rzeczywistości, którą tworzą zarówno nowe środowisko informacyjne[1], relacje między państwami, organizacjami i osobami, a także sposoby prowadzenie wojny. Wojna nowej generacji zaciera granice między pokojem a wojną, podkreślając tym samym przewagę nowoczesnego środowiska informacyjnego. Dziś łatwiej i potencjalnie taniej przełamać zdolność wroga do stawiania oporu poprzez stosowanie ukierunkowanych ataków cybernetycznych i informacyjnych aniżeli poprzez użycie konwencjonalnej siły militarnej. Mamy do czynienia z rzeczywistością, w której zorganizowane trollingowanie w sieciach społecznościowych[2], manipulacyjne programy telewizyjne[3], zhackowana korespondencja e-mail i atak cybernetyczny na systemy bankowe mogą przynieść większą szkodę społeczeństwom i rządom niż konwencjonalny wojskowy atak na dużą skalę.

1 Przykład definiowania środowiska informacyjnego według amerykańskiej doktryny informacyjnej: „Środowisko informacyjne jest sumą osoby, organizacji i systemu, które zbierają, przetwarzają, rozpowszechniają lub działają zgodnie z informacjami. Składa się z trzech wymiarów – fizycznego, informacyjnego i poznawczego. Fizyczny wymiar składa się z polecenia i kontroli systemu, kluczowych decydentów i wspierającej je infrastrukturą osoby i organizacji do tworzenia efektów. Wymiar informacyjny określa, gdzie i w jaki sposób informacje są gromadzone, przetwarzane, przechowywane, rozpowszechniane i chronione. Wymiar poznawczy obejmuje umysły tych, którzy przekazują, otrzymują i odpowiadają lub działają na informacjach" http: //www.dtic.mil/doctrine/new_pubs/jp3_13.pdf, [dostęp: 27.02.2018].

2 O. Wasiuta, *Sieci społecznościowe jako nowe narzędzia prowadzenia wojen informacyjnych we współczesnym świecie*, [w:] *Refleksje o przeszłości, spojrzenie na współczesność. Monografia poświęcona Profesorowi Sergiuszowi Wasiucie z okazji 60-letniego Jubileuszu i 35-lecia pracy zawodowej,* red. O. Wasiuta, Wydawnictwo Drukarnia Styl Anna Dura, Kraków 2018, s. 184–209.

3 Więcej na ten temat: O. Wasiuta, S. Wasiuta, *Wojna hybrydowa Rosji przeciwko Ukrainie,* Arcana, Kraków 2017, s. 162–253; S. Wasiuta, *Elementy kampanii informacyjnej w konflikcie rosyjsko-ukraińskim*, [w:] *Wojna hybrydowa na Ukrainie. Wnioski i rekomendacje dla Europy i świata*, red. B. Pacek, J. Grochocka, Wydawnictwo Uniwersytetu J. Kochanowskiego w Kielcach, Piotrków Trybunalski 2017, s. 253–266; O. Wasiuta, *Media narzędziem wprowadzenia agresji informacyjnej*, [w:] *Media jako instrument wpływu informacyjnego i manipulacji społeczeństwem,* red. H. Batorowska, R. Klepka, O. Wasiuta,. Wydawnictwo Libron, Kraków 2019, s. 127–143.

Cytując Sun Tzu, można się spierać czy sztuka pokonania wroga bez konwencjonalnych walk była stosowana już około 500 lat p.n.e., bez wątpienia jednak skala i szybkość informacji cyfrowej, którą można przetwarzać w XXI wieku, była na ówczesne czasy niewyobrażalna. Cyfrowy świat umożliwia oszustwa i manipulacje na potężną skalę.

Społeczeństwa stały i stają się każdego dnia coraz bardziej zależne od środowiska informacji i nowych technologii. Doskonałym przykładem zmian jakie nastąpiły jest cykl podejmowania decyzji, który, skurczony do kilku sekund, zupełnie odmienił proces działania. Zaobserwować tę zmianę można chociażby u polityków, liderów, dla których wymagana szybkość procesu decyzyjnego jest coraz trudniejsza, a możliwość manipulacji coraz łatwiejsza. Takie przyspieszenie na polu decyzyjności pozwala stosunkowo prosto otrzymać informację, przetwarzać ją i przekazywać w celu osiągnięcia pożądanego rezultatu.

W wyniku rozwoju nowych technologii, które przyspieszyły procesy globalizacyjne i przyczyniły się do powstania jednej przestrzeni informacyjnej, wojny informacyjne stały się jedną z najbardziej skutecznych metod osiągnięcia postawionego celu. Wykorzystanie wojny informacyjnej jako środka konfrontacji geopolitycznej można zaobserwować na przykładzie wojen w Zatoce Perskiej, Czeczeni, a także na wschodzie Ukrainy i na Krymie.

Rozwój środowiska internetowego umożliwia pojawianie się coraz nowszych form konfrontacji. Jedną z nich są wojny internetowe nazywane iWar. Termin ten używany jest przez NATO do opisania formy wojny prowadzonej w Internecie[4], a także na oznaczenie ataków przeprowadzanych w sieci, które są ukierunkowane na infrastrukturę internetową konsumenta, taką na przykład, jak strony internetowe zapewniające dostęp do usług bankowości internetowej. W tym rozumieniu iWar różni się od cyberwojny, cyberterroryzmu, wojny informacyjnej czy walki informacyjnej, które wiążą się z kontrolą komunikacji, dostępem do infrastruktury wojskowej i krytycznej, szpiegostwem elektronicznym oraz dowodzeniem i kontrolą pola walki, a ich polem bitwy jest sieć łączności i wywiad satelitarny.

Cyberwojna (*cyberwarfare*) definiowana jest jako: wykorzystanie komputerów, internetu i innych środków przechowywania lub rozprzestrzeniania informacji w celu przeprowadzania ataków na systemy informatyczne przeciwnika, wykorzystując do tego systemy i sieci teleinformatyczne[5]. Wojna informacyjna natomiast dotyczy „działań, które można scharakteryzować jako manipulację, dezinformację i propagandę, mających na celu zdobycie lub utrzymanie przewagi w polityce globalnej albo regionalnej. Polega ona na kontrolowaniu mediów, w tym społecznościowych, oraz innych kanałów przepływu informacji, np. blogów, forów internetowych

4 J. Ryan, *iWar: A new threat, its convenience and our increasing vulnerability*. *Analysis,* NATO Review. Winter 2007, https://www.nato.int/docu/review/2007/issue4/english/analysis2.html, [dostęp: 27.02.2019].

5 D. Fabaniec, *Cyberwojna. Metody działania hakerów,* Wydawnictwo Helion, Gliwice 2018; A. Kaźmierska, W. Brzeziński, *Strefy cyberwojny,* Wydawnictwo Oficyna 4eM, Lublin 2018; M. Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford 2014; K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku,* „Bezpieczeństwo Narodowe", 2011, nr 17, s. 15–28.

w celu sterowania świadomością i aktywnością ludzi. Wojna informacyjna łączy instrumenty psychologicznego oddziaływania i nowoczesne technologie, dające możliwość publikowania komentarzy, filmów czy nagrań niemal w czasie rzeczywistym, a jednocześnie skutkują niewystępującą nigdy wcześniej szybkością rozprzestrzeniania się informacji"[6]. Walkę informacyjną można zdefiniować jako zorganizowaną w formę przemocy aktywność zewnętrzną państwa prowadzącą do osiągnięcia określonych celów politycznych, skierowaną na niszczenie lub modyfikowanie systemów informacyjnego komunikowania przeciwnika lub przepływających przez nie informacji oraz ochronę własnych systemów informacyjnych przed podobnym działaniem przeciwnika[7].

Forma iWar jest zupełnie inna, wykorzystując wszechobecną infrastrukturę o niskim poziomie bezpieczeństwa, dotyczącą określonych zasobów w ramach nadbudowy Internetu i odnosi się do ataków przeprowadzanych w Internecie, ukierunkowanych na infrastrukturę internetową dla konsumentów, taką jak np. strony internetowe zapewniające dostęp do usług online[8]. W rezultacie, podczas gdy same państwa narodowe mogą angażować się w cyberwojny i wojny informacyjne, iWar może być prowadzona przez jednostki, korporacje i społeczności. Małe „i" wskazuje na jej wspólny rodowód z gadżetami i urządzeniami używanymi przez młode pokolenie wykorzystujące najnowszej technologie[9].

Koncepcja ta po raz pierwszy została wprowadzona zimą 2007 r. w przeglądzie NATO przez pracownika Instytutu Spraw Międzynarodowych i Europejskich Johnnego Ryana[10]. Inny badacz problemu, Mark Andrejevic, używając terminu iWar, uwzględnia istotne cechy współczesnej wojny, mówiąc o „interaktywnej stronie wojny z terrorem"[11], która opiera się na nowych praktykach monitorowania i zarządzania populacjami. Według niego nowe technologie mediów uczestniczących tworzą „cyfrową obudowę", w której każde działanie i transakcja generuje informacje o sobie, które następnie mogą być wydobywane i wykorzystywane do celów gospodarczych lub politycznych[12].

Ataki typu „odmowa usługi" znane od końca lat 80. stanowią jedną z powszechnych form iWar. Próbują one zablokować komputer lub system sieciowy, bombardując go dużą ilością żądań informacji. Jeśli się powiedzie, atak taki sprawi, że system docelowy nie będzie w stanie odpowiedzieć na żądania, które mogą obejmować zapewnienie dostępu do określonej witryny. Rozproszony atak typu „odmowa usługi" (DDoS) działa na tej samej zasadzie, ale zwielokrotnia swój wpływ, kierując botnet komputerów w sieci, które zostały zdalnie przejęte, aby bombardować

6 W. Cendrowski, *Wojna informacyjna*, [w:] *Vademecum bezpieczeństwa*, red. O.Wasiuta, R. Klepka, R. Kopeć, Wydawnictwo Libron, Kraków 2018, s. 696.

7 K. Liedel, P. Piasecka, *Wojna cybernetyczna...*, s. 17.

8 J. Ryan, *iWar: A new threat...*

9 J. Ryan, *iWar: pirates, states and the internet,* https://www.opendemocracy.net/article/iwar_pirates_states_and_the_internet, [dostęp: 27.02.2019].

10 J. Ryan, *iWar: A new threat..*

11 M. Andrejevic, *iSpy: Surveillance and Power in the Interactive Era,* University Press of Kansas, Lawrence, KS 2007, s. 163.

12 Ibidem, s. 2.

system docelowy wieloma żądaniami w tym samym czasie. Botnety mogą być kontrolowane przez jedną osobę. Jednym z przykładów działań przeprowadzonych w formie iWar może być atak na Estonię 27 kwietnia 2007 r., kiedy rozproszone ataki typu DoS (Denial of Service) skierowane zostały na ważne strony internetowe[13]. Trwało to do połowy czerwca. Strony internetowe prezydenta, parlamentu, wiodących ministerstw, partii politycznych, głównych serwisów informacyjnych i dwóch dominujących banków w Estonii zostały zablokowane, co uniemożliwiło interakcję z klientami[14]. Estoński minister obrony nazwał ataki zagrożeniem bezpieczeństwa narodowego. Niektóre botnety w atakach na Estonię zawierały nawet 100 000 maszyn, które w tym samym momencie wysuwały żądania informacji z docelowych stron internetowych[15]. Jak zaznacza J. Ryan, ataki iWar mogą być najbardziej innowacyjną formą wojny od czasu wynalezienia prochu[16].

Badacze wydzielają pięć cech iWar, które wskazują, że mogą one zrewolucjonizować konflikt, są nimi: potencjał do rozszerzenia działań ofensywnych; zasięg geograficzny; trudności w rozpoznaniu (wyjawieniu); łatwość proliferacji oraz wpływ na cele „gotowe". Te cechy sugerują, że nadejście iWar może oznaczać nową rewolucję militarną na równi z wynalezieniem prochu lub bomby atomowej. Analizując każdą z nich: po pierwsze, iWar rozszerza serię działań ofensywnych o bezprecedensową liczbę amatorów, których jedyną kwalifikację stanowi ich dostęp do sieci. Osoba atakująca, podobnie jak muszkieter z zapałkami, jest wyposażona w tani, potężny sprzęt, który wymaga niewielkiego przeszkolenia[17].

Po drugie, iWar jest niedrogi i łatwy do prowadzenia w sposób rewolucyjny. Być może działania tego typu, po raz pierwszy uwalniają od kosztów, przeszkód i wysiłków, które tradycyjnie powstrzymywały ofensywne działania przeciwko geograficznie odległym celom. Konwencjonalna technologia ofensywna polegająca na fizycznych środkach zdolnych do niszczenia celów za pomocą środków kinetycznych jest kosztowna i stosunkowo powolna, czego doskonałym przykładem są samoloty muszące wykonywać długie loty, aby zrzucić ładunek. Działania iWar, choć zapewniające znacznie mniej ofensywne uderzenie, mogą być prowadzone z dowolnego punktu w dowolnym miejscu na Ziemi, praktycznie bez żadnych kosztów[18].

Po trzecie, iWar jest trudny do rozpoznania, udowodnienia i ukarania. Do dnia dzisiejszego nadal nie jest jasne, czy Estonia padła ofiarą cyberataków hakerów bez zezwolenia ze strony Kremla, czy też działania zostały oficjalnie usankcjonowane i skoordynowane przez inne, wrogie państwo. Nawet jeśli uda się udowodnić winę innego państwa, nie jest jasne, w jaki sposób jedno państwo powinno zareagować na atak iWar innego. Również śledztwo cyfrowe byłoby nie mniej problematyczne, nawet jeśli można by wykryć szkodliwy botnet na pojedynczym komputerze, który zarządza atakiem DDoS (który zwykle trwa tylko przez krótki, intensywny okres),

13 Niektórzy badaczy uważają, że była to pierwsza w historii wojna cybernetyczna.

14 V. Mite, *Estonia: Attacks Seen As First Case of 'Cyberwar'*, https://www.rferl.org/a/1076805.html, [dostęp: 27.02.2019].

15 J. Ryan, *iWar: pirates, states...*

16 J. Ryan, *iWar: A new threat...*

17 J. Ryan, *iWar: pirates, states...*

18 J. Ryan, *iWar: A new threat...;* J. Ryan, *iWar: pirates, states...*

jest mało prawdopodobne, aby można było podjąć skuteczne działania w celu wniesienia oskarżenia, ponieważ „winny" komputer może znajdować się pod inną jurysdykcją, z którą brak współpracy utrudnia egzekucje. Dodatkowo – nawet jeśliby pojawiła się współpraca – komputer mógł być obsługiwany z kafejki internetowej lub innej anonimowej publicznej sieci łączności, uniemożliwiając określenie, kto z wielu przejściowych użytkowników był zaangażowany w atak DDoS[19]. Działania tego typu to doskonały sposób na wykorzystanie rosnącej zależności wszystkich struktur państwowych od komputera.

Po czwarte, iWar nie jest ograniczony położeniem geograficznym, które hamowałoby rozprzestrzenianie się wcześniejszych innowacji wojskowych, a zatem szybko rozprzestrzenił się na całym świecie. Mozna to pokazać na przykładzie rozprzestrzeniania się prochu w Europie: technologia pojawiła się w Chinach w 7. lub 8. wieku, ale debiutowała w Europie dopiero we Flandrii w 1314 roku. Narzędzia i wiedza niezbędna do prowadzenia iWar są dostępne w Internecie. A w 2007 r. fora internetowe o atakach DDoS na Estonię szybko rozpowszechniły informacje o tym, jak uczestniczyć w danym ataku[20].

Po piąte, ataki iWar wraz z postępującym rozwojem technologicznym nabierają coraz większego znaczenia. Internet z dnia na dzień będzie odgrywał coraz ważniejszą rolę w codziennym życiu politycznym, społecznym i gospodarczym. W ostatnim dziesięcioleciu rządy, społeczności, korporacje i osoby fizyczne nieprzerwanie wykorzystywały sieć jako środek dostarczania usług i kontaktów z obywatelami, klientami w grupach rówieśniczych i innych grupach społecznych. Na przykład w Estonii, która zajęła 23 miejsce w rankingu e-gotowości w 2007 r., odnotowano prawie 800 000 klientów banków internetowych w populacji liczącej prawie 1,3 miliona osób, a 95% operacji bankowych prowadzonych jest elektronicznie. W wielu państwach dostarczanie treści medialnych za pośrednictwem sieci konkuruje teraz z konwencjonalną dystrybucją gazet i muzyki (wkrótce potem następuje transmisja telewizyjna). Niezbędność technologii internetowych w wewnętrznej działalności organizacji biznesowych staje się coraz wyraźniejsza[21]. Tak, w Wielkiej Brytanii wydatki na reklamę w Internecie przerosły reklamy w prasie krajowej[22].

Instytucje i organizacje mogą w coraz większym stopniu polegać na technologiach internetowych w swojej wewnętrznej działalności, wykorzystując aplikacje internetowe, takie jak Google Docs[23], aby zastąpić konwencjonalne pakiety, takie jak

19 Ibidem.

20 J. Ryan, *iWar: A new threat...*

21 J. Ryan, *iWar: pirates, states...*

22 J. Ryan, *iWar: A new threat...*

23 Google Docs – Dokumenty Google – to edytor tekstu dołączony jako część darmowego, dostępnego przez Internet pakietu oprogramowania biurowego oferowanego przez Google w swoim Dysku Google usługi. Ta usługa obejmuje również Arkusze Google i Prezentacje Google, odpowiednio arkusz kalkulacyjny i program prezentacji. Dokumenty Google są dostępne jako aplikacja internetowa, aplikacja mobilna na Androida, Windows, BlackBerry oraz jako aplikacja komputerowa w Chrome OS Google. Aplikacja jest zgodna z formatami plików Microsoft Office. Umożliwia ona użytkownikom tworzenie i edytowanie plików online podczas współpracy z innymi użytkownikami w czasie rzeczywistym. Zmiany są śledzone przez użytkownika w historii zmian. Pozycja redaktora jest podświetlona specyficznym dla edytora kolorem i kursorem. System uprawnień reguluje

pakiet Microsoft Office. Dlatego iWar zagraża nie tylko interakcjom między organizacjami i ich klientami czy między państwem a obywatelem, ale także wewnętrznym działaniom organizacji.

Żadne państwo nie ma pełnej kontroli nad Internetem, żeby egzekwować prawo w stosunku do wykorzystywania iWar. Prowadzone jednostronne „policyjne" inicjatywy nie mają możliwości skutecznego przeciwdziałania iWar, ponieważ, podobnie jak piractwo przez wieki, jest ona zjawiskiem o charakterze globalnym, które działa i wykorzystuje wspólne zasoby Internetu[24]. Polityka ochrony mórz w przeszłości doprowadziła do opracowania nowych międzynarodowych norm postępowania, takich jak nieformalne, zwyczajowe przepisy chroniące dostęp do morza. Z czasem działalność w Internecie może doprowadzić do skodyfikowania zasad i przepisów oraz opracowania nowych międzynarodowych norm zachowania w celu ochrony funkcjonowania i dostępu do Internetu[25]. Ale nawet jeśli takie międzynarodowe prawo ostatecznie powstanie, może to zająć trochę czasu. Internet jest zdefiniowany jako światowe połączenie poszczególnych sieci obsługiwanych przez rząd, przemysł, środowisko akademickie i podmioty prywatne. Początkowo służył do łączenia laboratoriów zaangażowanych w badania rządowe, a od 1994 roku został rozszerzony, aby służyć milionom użytkowników i wielu celom we wszystkich częściach świata. W ciągu zaledwie kilku lat Internet utrwalił się jako potężna platforma, na zawsze zmieniając sposób działania i komunikacji. Jak żadne inne medium komunikacyjne nadał konsumentom wymiar międzynarodowy lub „globalny", stając się uniwersalnym źródłem informacji dla milionów ludzi w domu, w szkole i w pracy.

Internet cały czas się zmienia i ewoluuje. Sieć społecznościowa i technologia mobilna zmieniły sposób, w jaki ludzie korzystają z Internetu, wprowadzając nowy sposób komunikacji. Od momentu powstania w 2004 roku Facebook stał się światową siecią skupiającą ponad 2 230 milionów aktywnych użytkowników. Technologia mobilna natomiast, umożliwiając znacznie większy zasięg Internetu, zwiększyła liczbę użytkowników na całym świecie[26]. Jeszcze w 1995 r. dostęp do niego miało jedynie 16 milionów użytkowników na świecie (0,4%), pod koniec 2000 r. było ich już 361 milionów (5,8%), w grudniu 2005 r. – 1,018 miliarda (15,7%), we wrześniu 2010 r. – 1,2 miliardy (28,8%), w marcu 2011 r. – ponad 2 miliardy (30,2%), pod koniec 2015 r. – 3,366 miliardów (46,6%), w 2017 r. – 4,156 miliardów (54,4%), a w czerwcu 2018 r. – 4,208 miliardów (55,1%)[27].

Internet jest nadal najbardziej demokratycznym medium ze wszystkich środków masowego przekazu. Przy bardzo niskich nakładach każdy może stać się właścicielem strony internetowej. W ten sposób niemal każda firma może dotrzeć do

to, co mogą robić użytkownicy. Aktualizacje wprowadziły funkcje wykorzystujące uczenie maszynowe, dzięki czemu użytkownicy mogą przypisywać zadania innym użytkownikom.

24 J. Ryan, *iWar: pirates, states...*

25 Ibidem.

26 *Internet World Stats, Internet Growth Statistics,* Today's road to e-Commerce and Global Trade Internet Technology Reports, www.internetworldstats.com/emarketing.htm, [dostęp: 04.03.2019].

27 Ibidem.

dużego rynku w sposób bezpośredni, szybki i ekonomiczny, bez względu na swą wielkość i lokalizację. Przy bardzo niskich nakładach, prawie każdy, kto umie czytać i pisać, może mieć dostęp do sieci World Wide Web. Blogowanie skonsolidowało media społecznościowe, a ludzie na całym świecie wyrażają i publikują swoje pomysły i opinie, jak nigdy dotąd.

Pojawia się zatem ważne pytanie: czy jest to narzędzie wyłacznie w rekach państw, czy też istnieje możliwość, by aktorzy niepaństwowi atakowali państwa i siebie nawzajem? iWar może być wykorzystywana przez narody do wywierania nacisku na słabszych przeciwników, przez podmioty niepaństwowe natomiast do przeprowadzania ataków na infrastrukturę państwa narodowego. Nowa perspektywa anarchii i piractwa, podważającego interesy władzy, jest w zasięgu ręki. Potrzeba zarówno środków zaradczych w zakresie bezpieczeństwa, jak i odpowiednich ram prawnych, aby sprostać temu zagrożeniu[28].

Choć szkody jakie przynoszą działania w ramach iWar są niekonwencjonalne, agresorzy mogą zadawać szybkie uderzenia z dowolnego miejsca, praktycznie bez kosztów. Udostępnianie informacji na poziomie NATO pozwoli na wczesne ostrzeganie o podejrzanych działaniach i profilowanie możliwych ataków. Niektóre państwa NATO zaczęły chronić się przed zagrożeniami związanymi z zagrożeniami internetowymi, powołując krajowe komputerowe zespoły reagowania kryzysowego (CERT). Koordynacja CERT na poziomie NATO, we współpracy z Unią Europejską, byłaby przydatnym krokiem w ograniczaniu skutków ataków iWar w perspektywie krótkoterminowej. Na przykład, jeśli zostanie wykryty atak na czeską stronę przez użytkownika w sieci francuskiej, czeski CERT może poprosić swojego francuskiego odpowiednika o odcięcie połączeń, która są używane do ataku[29]. Niestety wiele rządów jednak nie ustanowiło jeszcze własnych zespołów CERT.

Pojawienie się iWar odzwierciedla potężne trendy, które zdominowały pierwszą dekadę XXI wieku: rozprzestrzenienie się Internetu, wzmocnienie pozycji jednostek i względny spadek władzy państwa w kontrolowaniu infrastruktury komunikacyjnej. Dostępność materiałów instruktażowych online, odpowiedniego oprogramowania i wszechobecnej łączności z Internetem umożliwia praktycznie każdemu sprawnemu i zaangażowanemu graczowi atakowanie odległych przeciwników czy wrogów[30].

Prawdopodobne jest, że niedługo iWar jako forma wojny internetowej rozprzestrzenie się na całym świecie. Ta forma siły bojowej będzie wzrastać, gdy gospodarki, rządy i społeczności będą w coraz większym stopniu wykorzystywać infrastrukturę konsumencką. iWar będzie się szybko rozprzestrzeniała i może być prowadzona przez każdego, kto ma połączenie z Internetem i może postępować zgodnie z uproszczonymi instrukcjami online. Tendencja do zwiększania podatności na zagrożenia, w połączeniu z wygodą i zaprzeczeniem ataku, może doprowadzić do zagrożeń ze strony jednostki, korporacji, narodów czy sojuszy[31]. Jej wpływ może

28 J. Ryan, *iWar: pirates, states...*

29 J. Ryan, *iWar: A new threat...*

30 Ibidem.

31 Ibidem.

być ogromny, a członkowie NATO będą mieli mało czasu na przeprowadzenie skutecznej reakcji.

W krótkim okresie działania typu iWar szybko się rozwinęły i stanowią rosnące zagrożenie dla członków NATO, poprzez wzmocnienie pozycji społeczności internetowej i nieprzyjaznych rządów. Dopiero okaże się, czy iWar staje się narzędziem samych aktorów państwowych, czy też aktorzy niższego szczebla utrzymują swoją zdolność do wykorzystywania iWar przeciwko państwom narodowym. Ponieważ międzynarodowy konsensus jest mało prawdopodobny, NATO musi podejść do tego problemu jako do bezpośredniego zagrożenia i dążyć do wypracowania praktycznej współpracy obronnej[32].

W 2015 roku, praktycznie w tym samym czasie, pojawiły się dwie publikację dotyczące iWar i jej znaczenia dla przyszłego bezpieczeństwa[33]. Ich autorzy rozszerzają definicje iWar i analizują jej przyszłość. Norweski badacz Holger Pötzsch[34] zaproponował rozszerzenie zaproponowanej przez Ryana i Andrejevica definicji iWar, w pełni uwzględniające konsekwencje nowych mediów i technologii komunikacyjnych dla zmieniających się praktyk i percepcji współczesnej wojny[35]. Holger Pötzsch wprowadził 5 wymiarów społeczno-technicznych charakteryzującą nowy wymiar wojny: **indywidualizację, niejawność, interaktywność, odrębność i bezpośredniość,** w ramach których rozwija się dynamika współczesnej wojny i łączy się z konkretnymi aplikacjami technologicznymi[36].

Dążenie do walki w sieci koncentruje się na zdolnościach militarnych do niszczenia infrastruktury komunikacyjnej wroga, infrastruktur informacyjnych, a wreszcie do skutecznego zarządzania przepływem obrazów i danych do i od coraz bardziej zdecentralizowanych światowych stron internetowych[37].

Wymiar indywidualizacji odnosi się do technologicznie dostarczanych procesów, które personalizują praktyki i postrzeganie działań wojennych. Można go scharakteryzować jako rozproszone formy działań ofensywnych, które indywidualizują zdolność do prowadzenia cyberwojny; nowe technologie, które pozwalają na zwiększenie zdolności ukierunkowanych na konkretne jednostki podczas ataków militarnych; oraz zautomatyzowane systemy zarządzania internetem. Rozproszone

32 Ibidem.

33 G.J. Voelz, *The rise of iWar: identity, information, and the individualization of modern warfare,* Strategic Studies Institute and U.S. Army War College Press, October 2015; H. Pötzsch, *The Emergence of iWar: Changing Practices and Perceptions of Military Engagement in a Digital Era*, „New Media &Society", 2015, vol. 17(1).

34 H. Pötzsch jest pracownikiem Uniwersytetu w Tromsø z doświadczeniem w dziedzinie komunikacji i mediów.

35 R. Klepka, *Wojna w mediach: wybrane zagadnienia dotyczące relacjonowania konfliktów zbrojnych*, „Wojny i konflikty. Przeszłość–Teraźniejszość–Przyszłość" 2016, t. 1, nr 1; R. Klepka, M. Piekarz, *Konflikt militarny w mediach: jak polska prasa i telewizja pokazuje wojnę w Syrii,* [w:] *Transformacja środowiska międzynarodowego i jego wielowymiarowość*, red. R. Kordonski, A. Kordonska, D. Kamilewicz-Rucińska, Lwowski Uniwersytet Naukowy im. Iwana Franki, Lwów–Olsztyn 2017, t. 5.

36 H. Pötzsch, *The Emergence of iWar*…, s. 2.

37 Ibidem, s. 79.

zdolności ofensywne zostały określone w definicji iWar przedstawionej przez J. Ryana[38] i wskazują na zwiększoną zdolność jednostek do przeprowadzania ataków DDoS na wojskową i cywilną infrastrukturę internetową[39]. Biorąc pod uwagę rosnące znaczenie usług internetowych, takie działania stanowią dziś zwiększające się zagrożenie dla bezpieczeństwa państw narodowych. Przy analizie zagrożenia bezpieczeństwa trzeba uwzględnić „rozproszony wyciek" informacji niejawnych za pośrednictwem sieci haktywistycznych i anonimowych witryn, takich jak WikiLeaks. Również w tych przypadkach poszczególni aktorzy stosują technologie sieciowe, aby wymusić pomnożenie efektów ich politycznych aspiracji, co może mieć katastrofalne skutki dla reputacji i interesów państw lub dużych organizacji.

Indywidualizacja odnosi się do coraz częściej prowadzonych, zautomatyzowanych praktyk selekcji osób jako celów specjalnych operacji, wykorzystania dronów i innych form wojny zdalnej, post-terytorialnej. Wysiłki militarne państw Zachodu nie są dziś tak bardzo ukierunkowane na siły tradycyjnych masowych armii, ale raczej przypominają polowanie z wyprzedzeniem w celu złapania lub likwidacji konkretnych osób, zakładając, że mogą one zagrażać bezpieczeństwu państwa. Wojna w coraz większym stopniu przyjmuje formę rozszerzonych kampanii, tak zwanych zabójstw prawnych określonych osób. Wybór celów dla takich kampanii odbywa się często na podstawie algorytmów, które trałują dostępne bazy danych i kategoryzują osoby lub grupy na podstawie pewnych cech, wzorców zachowań lub innych wyznaczników.

Analizując następny wymiar iWar – niejawność – M. Andrejevic twierdzi, że „w erze zindywidualizowanych działań wojennych systemy dowodzenia i kontroli polegają na rozprzestrzenianiu i intensyfikacji technologii gromadzenia informacji i strategii"[40]. Według H. Pötzscha niejawność podkreśla niektóre z nowości technologicznych oraz zwraca uwagę na sposoby zapisywania codziennych czynności online użytkowników w praktykach wojennych i związanych z bezpieczeństwem. To pociąga za sobą zmianę koncepcji uczestnictwa użytkownika i Internetu jako wolnej i amoorganizującej się sieci. Połączenie producenta i użytkownika prowadzi do zacierania różnic między świadomym wytwarzaniem informacji lub towarów w celu sprzedaży i konsumpcji, a milczącymi ulepszeniami i zestawami danych, które można wytworzyć, przez pozornie jedynie użycie aplikacji[41].

Zbieranie i gromadzenie dużych zbiorów danych ma poważne implikacje dla niemal wszystkich aspektów życia prywatnego i publicznego, a także potwierdza znaczny potencjał kontroli, tkwiący w tych technologiach. Niejasne są formy gromadzenia i eksploracji danych, a także profilowania użytkowników. Internet jest zarówno poziomo zorganizowaną, rozproszoną siecią, jak i hierarchiczną strukturą kontrolującą użytkowników. Stąd wysiłki władz USA zmierzające do zapewnienia współpracy firm takich, jak Facebook, Google, Microsoft i inne, które kontrolują globalny ruch internetowy. Ta technologia pozwala sieciom klasyfikować

38 J. Ryan, *iWar: A new threat...;* J. Ryan, *iWar: pirates, states...*

39 H. Pötzsch, *The Emergence of iWar*..., s. 7.

40 M. Andrejevic, *iSpy: Surveillance and Power...*, s. 175.

41 H. Pötzsch, *The Emergence of iWar*..., s. 8.

i kontrolować ruch w oparciu o treść i umożliwia dostawcom usług internetowych skuteczne monitorowanie, przyspieszanie, spowalnianie, blokowanie, filtrowanie lub podejmowanie innych decyzji dotyczących ruchu użytkowników na podstawie wiedzy o tym, jakie informacje przekazują[42].

Trzecim wymiarem iWar jest interaktywność, zawierająca w sobie wojnę jako technologicznie świadczone interaktywne doświadczenie, w które obywatele angażują się na nowe sposoby oraz interaktywne monitorowanie, śledzenie i kategoryzację różnorodnych urządzeń, w tym nowe technologie rozrywki, takie jak interaktywne gry wojskowe i aplikacje szkoleniowe, a także wykorzystanie technologii śledzenia.

Zwiększona odrębność jest kolejnym ważnym wymiarem współczesnej wojny, którą można wyjaśnić za pomocą koncepcji iWar[43]. Obecnie nowe urządzenia do noszenia i łączenia w sieć wiążą się z nowym potencjałem intymności pomiędzy publicznym i indywidualnym, pomiędzy zdalnie sterowanymi pilotami dronów i ich celami, oraz między publicznością a ofiarami działań wojennych. Kluczowymi technologiami zapewniającymi specyficzną dynamikę wymiaru intymności są coraz bardziej wyrafinowane sieciowe telefony komórkowe lub kamery hełmowe, a także dokładność i rozdzielczość materiału dostarczanego przez kamery i czujniki.

Piątym wymiarem iWar jest bezpośredniość, która opisuje, w jaki sposób rozproszone technologie komunikacyjne i wszechobecność sieci zwiększają prędkość, z jaką informacje o wojnie stają się dostępne i są przetwarzane przez decydentów politycznych, personel wojskowy, media i społeczeństwo[44]. Uniwersalność sieci, rozproszenie urządzeń do noszenia na ciele i globalny zasięg relacji na żywo – to kluczowe technologie umożliwiające dynamikę tego wymiaru.

iWar nie zastępuje takich pojęć jak wojna konwencjonalna lub wojna rozproszona. Przeciwnie, wszystkie koncepcje zachowują swoją ważność i znaczenie, ponieważ podkreślają różne, ale równie wyważone cechy współczesnej wojny[45].

Pułkownik Glenn J. Voelz, pracownik Wydziału Wywiadowczego Międzynarodowego Sztabu Wojskowego przy siedzibie NATO w Brukseli[46], charakteryzując iWar, zwraca uwagę na trzy odrębne elementy: indywidualizację, tożsamość i informację, które stanowią ramy koncepcyjne do analizy zmian w doktrynie, technologii i celu strategicznym. Cechy te na nowo zdefiniowały sposób prowadzenia wojny za granicą.

42 Ibidem, s. 78–79.

43 Ibidem.

44 Ibidem, s. 80.

45 Ibidem, s. 81–82.

46 Pułkownik Glenn J. Voelz jest oficerem wywiadu wojskowego, a ostatnio członkiem amerykańskiej Akademii Wojskowej w Massachusetts Institute of Technology (MIT), Studium Bezpieczeństwa i MIT's Lincoln Laboratory. Obecnie pracuje w Wydziale Wywiadowczym Międzynarodowego Sztabu Wojskowego przy siedzibie Organizacji Traktatu Północnoatlantyckiego w Brukseli w Belgii. W trakcie swojej kariery pułkownik Voelz służył na różnych stanowiskach w Agencji Wywiadu Obronnego oraz w Połączonych Sztabach w Pentagonie. Jego obowiązki wojskowe obejmowały zadania w Azji, Afryce, na Bliskim Wschodzie i w Europie. Voelz jest autorem kilku książek i artykułów na tematy obejmujące historię dyplomatyczną, kontraktowanie rządu, politykę wywiadowczą i strategię wojskową.

• **Indywidualizacja:** w ciągu ostatniej dekady XXI wieku bezpieczeństwo narodowe zostało przesunięte z tradycyjnego podejścia w kierunku zagrożeń ze strony przeciwników, którzy walczą w sposób rozproszony albo indywidualnie. Ta reorientacja doprowadziła do przyjęcia nowych metod analitycznych i podejść operacyjnych w oparciu o systematyczne zagrożenia ze strony indywidualnych osób[47].

• **Tożsamość**: przeniesienie ataków do sieci doprowadziło do naglącej potrzeby identyfikacji prowadzących te działania podmiotów. W wieku iWar nie ma przeciwników, których można zidentyfikować jako żołnierzy i których można wyróżnić na podstawie ich statusu. Nowe rodzaje informacji i metody, w tym biograficzne, biometryczne i kryminalistyczne dane oraz wykorzystanie analizy sieci do łączenia tożsamości z miejscami, działaniami i powiązania z innymi osobami, stają się podstawą dzisiejszych działań[48].

• **Informacja:** iWar zależy od zarządzania informacją wokół technologii zaprojektowanych w celu różnicowania poszczególnych aktorów na polu bitwy i odsegregowania przyjaciół od wrogów. Zadania te różnią się od analitycznych wyzwań epoki przemysłowej wojny i wymagają nowych narzędzi i metod do zbierania, przetwarzania i przekazywania informacji o tożsamości[49].

Te elementy iWar odzwierciedlają nowe funkcjonowanie paradygmatu, który pojawił się w odpowiedzi na nieoczekiwanego przeciwnika, który walczy jako sieć a nie formacja. Zgodnie z działaniami iWar walczących nie można łatwo zidentyfikować na polu bitwy, a ich anonimowość działa na ich korzyść. Ich działania nie ograniczają się do jednoznacznie określonego pola bitwy lub celów wojskowych. Te cechy pozwoliły im stawić opór przytłaczającej przewadze państwa w konwencjonalnych manewrach wojennych, powietrznych i logistycznych. Procesy te i zmiana zagrożeń stały się katalizatorem dla poważnej reorientacji bezpieczeństwa narodowego, a przede wszystkim do reorganizacji strategii opartej na potrzebie identyfikacji sieci i jej użytkowników. W ramach tego nowego paradygmatu nie można zniszczyć fizycznej infrastruktury przeciwnika lub kontrolować jego terytorium.

Narzędzia i metody iWar nie ewoluowały jako rezultat nadrzędnego projektu. Ścieżka innowacji została raczej zdefiniowana przez awarię operacyjną, adaptację taktyczną i nowe priorytety strategiczne, które pojawiły się w odpowiedzi na nieoczekiwanego przeciwnika. Doprowadziło to do dekady, w której rola innowacji doktrynalnej i technicznej, skoncentrowanej na zadaniu identyfikacji i targetowania zagrożeń ze strony użytkowników Internetu znacząco wzrosła. To pobudziło bezprecedensową rewolucję w zarządzaniu informacjami i udostępnianiu danych w całym aparacie bezpieczeństwa narodowego. Te zmiany odzwierciedlają nowe podejście strategiczne, które umieściło zagrożenia ze strony podmiotów niepaństwowych i indywidualnych na równi z tradycyjnymi zagrożeniami ze strony państw[50].

Pojawienie się iWar odzwierciedla trendy nowego stulecia: rozprzestrzenienie się Internetu, wzmocnienie pozycji jednostek i względny spadek władzy państwa

47 G.J. Voelz, *The rise of iWar...*, s. 2.

48 Ibidem, s. 3.

49 Ibidem, s. 4.

50 Ibidem, s. 4–5.

w zakresie kontroli infrastruktury komunikacyjnej. Instrukcje online i niezbędne oprogramowanie umożliwiają praktycznie każdemu graczowi połączenie z Internetem w celu przeprowadzenia ataku skierowanego nawet w stronę odległych przeciwników. Wzmocnienie pozycji aktorów niższego szczebla i nieprzyjaznych rządów w krótkim okresie może stanowić rosnące zagrożenie dla członków NATO. Nie jest dotąd wiadome bowiem, czy iWar stanie się narzędziem samych aktorów państwowych, czy też aktorzy niższego szczebla otrzymają zdolność do wykorzystywania iWar przeciwko państwom narodowym. Skoro międzynarodowy konsensus jest mało prawdopodobny i od dawna wyraża przyjęte normy prawne, NATO musi podjąć problem jako bezpośrednie zagrożenie i starać się rozwijać praktyczną współpracę obronną.

Terminu iWar używa się, aby uwzględnić istotne cechy współczesnej wojny, a przede wszystkim głębokie odejście od fundamentalnych założeń systemu westfalskiego, który określił kontekst wojny państwowej na ponad 300 lat od zakończenia wojny trzydziestoletniej. Ta historyczna chwila oznaczała ważny punkt przejściowy z epoki prywatnych konfliktów najemników do nowoczesnej konstrukcji wojny, w której walczących zaczęto postrzegać jako instrumenty państwa. Opisywanie iWar musi nastąpić poprzez dodanie odrębnej technologii i wymiaru umożliwiającego niespotykaną dotąd dynamikę, jaką dają nowe technologie sieciowe i komunikacyjne. iWar może być prowadzona przez każdego, kto ma połączenie z Internetem, co pociąga za sobą zasadniczą zmianę w równowadze zdolności ofensywnych, dającą jednostkom możliwość zastraszenia i ataków na rządy i duże korporacje.

Bibliografia

Andrejevic M., *iSpy: Surveillance and Power in the Interactive Era*, University Press of Kansas, Lawrence, KS 2007.

Cendrowski W., *Wojna informacyjna*, [w:] *Vademecum bezpieczeństwa,* red. O. Wasiuta, R. Klepka, R. Kopeć, Wydawnictwo Libron, Kraków 2018.

Fabaniec D., *Cyberwojna. Metody działania hakerów,* Wydawnictwo Helion, Gliwice 2018.

Gertz B., *IWar: War and Peace in the Information Age*, The Institute of World Politics, Simon & Schuster, Reprint edition, Washington 2017.

*Internet World Stats, Internet Growth Statistics.*Today's road to e-Commerce and Global Trade Internet Technology Reports, www.internetworldstats.com/emarketing.htm [dostep: 04.03.2019].

Kaźmierska A., Brzeziński W., *Strefy cyberwojny,* Wydawnictwo Oficyna 4eM, Lublin 2018.

Kiyuna A., Conyers L., *Cyberwarfare Sourcebook*, Lulu.com, 2015.

Klepka R., Piekarz M., *Konflikt militarny w mediach: jak polska prasa i telewizja pokazuje wojnę w Syrii,* [w:] *Transformacja środowiska międzynarodowego i jego wielowymiarowość*, t. 5, red. R. Kordonski, A. Kordonska, D. Kamilewicz-Rucińska, Lwowski Uniwersytet Naukowy im. Iwana Franki, Lwów–Olsztyn 2017.

Klepka R., *Wojna w mediach: wybrane zagadnienia dotyczące relacjonowania konfliktów zbrojnych*, „Wojny i konflikty. Przeszłość–Teraźniejszość–Przyszłość" 2016, t. 1, nr 1.

Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku.* „Bezpieczeństwo Narodowe" 2011, nr 17.

Mite V., *Estonia: Attacks Seen As First Case Of 'Cyberwar',* https://www.rferl.org/a/1076805.html [dostęp: 30.05.2007].

Pötzsch H., *The Emergence of iWar: Changing Practices and Perceptions of Military Engagement in a Digital Era*, „New Media &Society" 2015, vol. 17(1).

Roscini M., *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Oxford 2014.

Ryan J., *iWar: pirates, states and the internet.* ttps://www.opendemocracy.net/article/iwar_pirates_states_and_the_internet, [dostęp: 6.02.2008].

Ryan J., *iWar: A new threat, its convenience and our increasing vulnerability. Analysis*. NATO Review. Winter 2007, https://www.nato.int/docu/review/2007/issue4/english/analysis2.html, [dostęp: 04.03.2019].

Voelz G.J., *The rise of iWar: identity, information, and the individualization of modern warfare*, Strategic Studies Institute and U.S. Army War College Press, October 2015.

iWar – an unprecedented form of Internet war

Abstract

The aim of the article is to present the concept of iWar, a new, unique idea of war. Understanding and specificity of the concept is associated with changes that take place in the way of functioning of modern societies. The term iWar is used to describe the form of war on the Internet, as well as the signs of attacks carried out on the web, which are targeted at the consumer's internet infrastructure, such as websites providing access to online banking services. Thus, iWar differs from cyberwar, cyberterrorism, information warfare of information fights that involve communication control, access to military and critical infrastructure, electronic espionage, and command and control of the battlefield, and their battlefield is a communication network and satellite intelligence. The article presents the socio-technical dimensions that characterize the new dimension of war: individualization, secretiveness, interactivity, separateness and directness, within which the dynamics of modern war develops and is combined with specific technological applications. The main tool and methods of iWar are also presented.

Słowa kluczowe: iWar, internet, wojna internetowa, nowoczesna wojna, atak internetowy

Key words: iWar, internet, internet war, modern war, internet attack

Olga Wasiuta
profesor zwyczajny, doktor habilitowany, Dyrektor Instytutu Nauk o Bezpieczeństwie, Kierownik Katedry Bezpieczeństwa Narodowego Uniwersytetu Pedagogicznego im. Komisji Edukacji Narodowej w Krakowie. Zajmuje się problematyką bezpieczeństwa regionalnego i europejskiego oraz wojną hybrydową. Jest autorką lub współautorką m.in. takich monografii, jak: *Wojna hybrydowa Rosji przeciwko Ukrainie* (Kraków 2017), *Państwo Islamskie ISIS. Nowa twarz ekstremizmu* (Warszawa 2018); współredaktor monografii wieloautorskich poświęconych bezpieczeństwu: *Współczesne wyzwania bezpieczeństwa europejskiego* (Kraków 2016), *Współczesne problemy bezpieczeństwa państwa* (Stalowa Wola 2017)*, Wyzwania bezpieczeństwa międzynarodowego* (Stalowa Wola 2017)*; Vademecum bezpieczeństwa* (Kraków 2018); jest również autorką licznych artykułów naukowych. Jest członkiem Polskiego Towarzystwa Geopolitycznego; przewodniczącą Rady Programowej czasopisma „Annales Universitatis Paedagogicae Cracoviensis. Studia de Securitate"; zastępcą redaktora naczelnego czasopisma naukowego „Socjologia prawa" (Ukraina, Kijów). E-mail: olga.wasiuta@up.krakow.pl.