entralnego Ośrodka Szkolenia Straży Gra-
ci Józefa Piłsudskiego w Koszalinie" 3/2010,

'ane problemy transgranicznego bezpieczeń-
n.

P. (2012). Bezpieczeństwo personalne grup
twa. W: W. Horyń, L. Wełyczko (red.), *Edu-
' XXI wieku. Człowiek – bezpieczeństwo –*
nictwo Wyższej Szkoły Oficerskiej Wojsk
ściuszki we Wrocławiu.

)ieczeństwa w nauce o stosunkach między-
ed.), *Bezpieczeństwo narodowe i międzyna-*
ırszawa.Fundacja Studiów Międzynarodo-

Threats in cyberspace
Zagrożenia w cyberprzestrzeni

dr Zygmunt Domański
Wyższa Szkoła Gospodarki Euroregionalnej
im. Alcide De Gasperi w Józefowie

Abstracts

Jesteśmy obecnie świadkami gwałtownych zmian zachodzących na wielu płaszczyznach. Funkcjonowanie współczesnych społeczeństw zrewolucjonizowały m.in. techniki komputerowe jak również niezwykłe możliwości komunikacyjne. W niespotykany dotychczas sposób wykorzystuje się urządzenia cyfrowe do gromadzenia różnego rodzaju informacji, przechowywania ich, przetwarzania i przesyłania. Do tego procesu włączyły się także media i niemal codziennie dostarczają nam wiadomości o świecie „cyberprzestrzeni" i zagrożeniach w nim występujących. Informacja stała się towarem, traktowanym jako szczególne dobro niematerialne, porównywalne lub cenniejsze od dóbr materialnych. Pojawił się szybki rozwój usług związanych z przechowywaniem, przesyłaniem i przetwarzaniem różnych informacji. Cyberprzestrzeń, cyberprzestępczość i cyberterroryzm to terminy ściśle ze sobą powiązane. Cyberterroryzm to pojęcie używane już w latach osiemdziesiątych XX wieku. Świat globalnej sieci szybko się rozrastał i stawał się coraz bardziej podobny do świata rzeczywistego, a zatem zarówno przestępczość jak i terroryzm znalazły swoje miejsce w przestrzeni wirtualnej. Zmasowane ataki na komputery zanotowano pod koniec lat dziewięćdziesiątych ubiegłego wieku. Powszechnie są znane, słynne ataki hakerów na różne obiekty, a także akty „phishingu" na placówki bankowe i ich skutki, a także zawirusowania komputerów osobistych, wskazują, że niezbędne jest podkreślenie wagi omawianych zagadnień.

We are currently witnessing rapid changes taking place on many levels. The functioning of modern societies was revolutionized by, among others, computer technology and extraordinary communication capabilities. In an unprecedented way, there are digital devices used to collect, store, process and transmit all kinds of information. This process was also joined by

ay they provide us with information about
:" and these dangers that occur within it.
nmodity, treated as a special possession of
valuable than material goods. Appeared in
ces related to the storage, transmission and
ion . Cyberspace, cybercrime and cyber ter-
l . Cyber terrorism is the term used already
th century. World global network quickly
nore like the real world. Thus, both crime
place in the virtual space. Massive attacks
ate nineties of the last century. Commonly
s attacks on different objects, as well as acts
s and their effects, and personal computer
ssary to stress the importance of the issues

its in cyberspace, cybercrime,

n, cyberprzemoc, zagrożenia w cyberprze-

)aństw dążą do stworzenia własnej, naro-
rjnej. Starają się tym samym odegrać swoją
)zycję w regulowaniu tak burzliwego wzro-
informacyjnej, czyli w cyberprzestrzeni.
elkie dane zwłaszcza te wrażliwe, oraz sze-
zanie nią bez wątpienia wpływają znacząco
twa (Adamski, 2001, s.12). Z dotychczaso-
współczesnych konfliktów zbrojnych wy-
a nowoczesnych działań jest zintegrowanie
wansowanym potencjałem sił konwencjo-
ci z operacji wojennych, jak np. sukces sił
ej, interwencja w Somalii czy na Bałkanach
Coraz większego znaczenia nabiera walka
ym świadczą kazus kosowski i tajwański

(1999), kazus chińsko-amerykański (2002), estoński (2007), gruziński (2008), irański (2010) i inne (Białoskórski, 2011, s. 48–53, 89–108).

Aktywna działalność hakerów oraz przypadkowe albo celowe awarie systemów komputerowych, zagrażające wielu ważnym instytucjom z punktu widzenia społecznego i bezpieczeństwa państwa sprawiły, że nasiliły się obawy powstania zupełnie nowych zagrożeń bezpieczeństwa narodowego. Pojawiło się nawet niebezpieczeństwo „wojny informacyjnej".

Potencjalni przeciwnicy mogą próbować nowoczesnych rozwiązań w przyszłej konfrontacji, np. zdecydować się na zakłócenie infrastruktur informacyjnych. Groźba wtargnięcia do systemów informatycznych państw, w tym także wojskowych, stanowi znaczące ryzyko dla bezpieczeństwa narodowego danego kraju. Potencjalne zagrożenia w postaci ataków cyfrowych zmuszają zatem do przeciwdziałania „cyberterroryzmowi". Rosnące obawy „cyberzagrożeń " zmuszają instytucje odpowiedzialne za bezpieczeństwo narodowe do stawiania czoła wyzwaniom wynikających z tych zagrożeń, jako konsekwencji wzrastającego uzależnienia od infrastruktur informacyjnych.

Zagrożenia związane z wojną informacyjną są rozległe; począwszy od „wojny symulacyjnej", aż po rzeczywistą destrukcję zasobów informacyjnych i bezpośrednie niszczenie środków łączności.

Można mówić o nowym zagrożeniu i możliwość wybuchu „strategicznej" wojny informacyjnej jako nowego środka walki, za pomocą którego strony konfliktu mogą toczyć wojnę, bezpośrednio atakując infrastrukturę informacyjną przeciwnika. Może być także zastosowany zdalny atak cyfrowy, jako nowy rodzaj tzw. „mikro sił", będących w dyspozycji stron konfliktu.

Rozprzestrzenianie się broni masowego rażenia i szeroki zasięg terroryzmu wzbudzają obawy w środowiskach odpowiedzialnych za bezpieczeństwo państw i społeczeństw. Aktualnie stratedzy bezpieczeństwa narodowego i planiści wojskowi zmagają się z wpływem nowych technik informacyjnych na stan obronności. Wykorzystanie technik cyfrowych do wzbogacenia tradycyjnych działań współczesnego pola walki stało się integralną częścią myśli wojskowej. Sukces Stanów Zjednoczonych w Zatoce Perskiej w znacznym stopniu wynikał z wykorzystania współczesnych, wyrafinowanych systemów informacyjnych. Zatem nową sferą wymiany informacji cyfrowych, poza dotychczasowymi płaszczyznami takimi jak

inne, stała się także, a może przede wszyst-
aszczyzna przyszłych konfliktów pojawiła
strzeń. W tej sytuacji stratedzy obronności
ukturę militarną do nowych wyzwań i spo-
my informacyjne mogą dziś pełnić funkcję
nnych. Wojna w cyberprzestrzeni oznacza
militarne, ale towarzyszy jej zupełnie nowe
odowego. Potencjalny przeciwnik będzie
unktów w systemach informacyjnych.

NFORMACYJNEJ

ormacji elektronicznej na operacje woj-
ło zrozumienia nowoczesnych zagrożeń
Vojna w Zatoce Perskiej została uznana za
Operacje informacyjne (ang. Information
ve wszystkich fazach działań i w całym za-
z na każdym poziomie wojny. Wojna infor-
operacji informacyjnych podczas kryzysu
ıb promować określone cele w stosunku do

ych posługuje się pojęciem „wojny infor-
inem programy zagraniczne i możliwości
informacyjną rozumie się także ochronę
ıktury o znaczeniu krytycznym (Rattray,

Martin Libicki wymienia siedem oddziel-
jną informacyjną: 1) wojna w zakresie do-
ıa opierająca się na wywiadzie, 3) wojna
ılogiczna, 5) wojna obejmująca działania
nformacje ekonomiczne i 7) „cyberwojna"
2003, s. 68.).

owego zjawiska autorzy starają się nie po-
nego dla definicji. Jednak różnorodność
finicji nie pomaga przy próbach określe-
wadzenia analiz. Termin „wojna informa-
ı wrogich działań dotyczących informacji,

poczynając od działań pojedynczych hakerów aż do potencjalnych, szeroko zakrojonych i skoordynowanych ataków jednego państwa przeciwko drugiemu, w celu osiągnięcia liczących się efektów politycznych (Białoskórski, 2011, s. 41–47).

Już w latach dziewięćdziesiątych minionego stulecia narastały obawy związane z wojną informacyjną. Analitycy amerykańscy zaczęli się zastanawiać, w jaki sposób przeciwnicy USA mogliby uderzyć za pomocą środków cyfrowych. Jednym z głównych budzących niepokój sposobów było to, że państwa i korporacje międzynarodowe mogłyby prowadzić walkę z konkurencją, atakując i wykorzystując systemy informacyjne przeciwnika. Za jedną z możliwości wybuchu wojny informacyjnej uznano walkę międzynarodowych korporacji prowadzących destrukcyjne ataki informacyjne przeciwko konkurentom.

Winn Schwartau, pisze o „globalnej wojnie informacyjnej", która może być prowadzona przeciwko przemysłowi, politycznym sferom wpływów, ugrupowaniom ekonomicznym o światowym zasięgu, a nawet przeciwko całym państwom" (Schwartau, 1996, s. 54.).

Przedmiotem obaw środowisk gospodarczych, są zagrożenia ze strony pozbawionych skrupułów konkurentów. Realnym zagrożeniem jest szpiegostwo przemysłowe lub gospodarcze skierowane przeciwko informacjom stanowiącym tajemnicę zasobów firmowych. Za pomocą nowoczesnych narzędzi cybernetycznych mogą być zagrożone lub zniszczone „wrażliwe dane" dotyczące projektowania, polityki cenowej, marketingu, strategii, udziału w przetargach i inne zasoby informacyjne. Wynikające stąd straty dla firm i ich konkurencyjności mogą być znaczące.

Autorzy takich koncepcji uważają nawet, że konkurencja ekonomiczna zastępuje wojnę i staje się głównym przedmiotem troski rządu zagrożonego państwa. Zaciekłe, choć bezkrwawe, wojny informacyjne, w których firmowe bazy danych są atakowane, manipulowane lub niszczone w celu uzyskania korzyści na światowym rynku, postrzega się jako zapowiedź zjawisk i zagrożeń w teraźniejszości i w przyszłości. Obawy budzi także posługiwanie się informacjami gromadzonymi przez państwowe agencje wywiadu i wykorzystywanie ich w celu wspierania prywatnych firm i korporacji.

Konkurencja gospodarcza prowadzona w formie wojny informacyjnej mogłaby mieć znaczenie strategiczne ze względu na swój potencjalny wpływ na znaczną liczbę ludzi oraz na zdolność państw do prowadzenia działalno-

erzające do uzyskania wpływów gospodar-
ıusu fizycznego w rodzaju embarga nie są
ugiwanie się szpiegostwem gospodarczym
ıb przedsiębiorstwa komercyjne ma długą
ery informacji cyfrowej. Najnowsze osią-
ıacznie odmieniły zbieranie i wykorzysty-
ierzające do zakłócenia, uszkodzenia lub
nych lub zasobów baz danych przeciwnika
akceptowane granice konkurencji gospo-
ówwnowagi wojskowej.

ąca systemy gospodarcze jest zawsze moż-
ıt wysokie, ze względu na łatwą identyfika-
lobna do uzyskania przewaga przeciwnika
ıraniczenia (Rattray, 2004, s. 23.).

:ia do wojny strategicznej wynika, że dzia-
ıstemów informacyjnych i sieci, będących
ańswa, mogą umożliwiać przeciwnikom
ıorów życia społecznego mających ważne
ıoczej „Defense Science Board", zatytuło-
na pola walki, autorzy przedstawili dwa
ıformacjach.

‚informacja w wojnie", aby przeanalizo-
ıżyciem zasobów informacyjnych, oraz
ń informacyjna". Odniesiono się także
ataków informacyjnych przeciwko ste-
ı telekomunikacyjnym, bazom danych,
aczeniu i komputerom przeciwnika, co
ı operacji informacyjnych, zarówno ko-

wojny informacyjnej odległość geogra-
znajdujące się w granicach państwa są
ılnym teatrze działań (Molander, Ridle,

iny" Daniel J. Ryan i Julie J. C. H. Ryan
:znej wojny informacyjnej. Po pierwsze,
st wojną. Nie jest tylko samym terrory-

zmem informacyjnym, przestępstwem komputerowym, działalnością hakerów, ani też szpiegostwem sponsorowanym przez państwo i polegającym na użyciu sieci z zamiarem dotarcia do pożądanej informacji. Wszystkie te nowe i niebezpieczne zjawiska mogą wystąpić we współczesnym świecie on-line, ale nie są one jeszcze kwalifikowane jako wojny informacyjne („info wojny"). W „infowojnie" stosuje się na dużą skalę siłę niszczącą przeciwko zasobom i systemom informacyjnym, przeciwko komputerom i sieciom obsługującym różne systemy (Ryan, 1996, s. 28.).

Od pracy komputerów uzależnione są np.: kierowanie ruchem lotniczym, transakcje bankowe i giełdowe, rejestry finansowe, wymiana walut, łączność internetowa, telefoniczna, rejestry kredytowe, transakcje zawierane drogą elektroniczną itp. Wszystkie te dziedziny życia społecznego i gospodarczego uzależnione są od zastosowania zabezpieczenia sieci i komputerów.

Dwa liczące się sztaby ekspertów opublikowały studia nad cyberprzestrzenią jako nową areną konfliktów. Studium RAND Corporation zatytułowane Strategic Information Warfare Rising (Nadchodzi strategiczna wojna informacyjna) jest oparte na wcześniej już prowadzonych badaniach tej placówki. Stanowi ono próbę wskazania i uporządkowania zagadnień i problemów politycznych, przed którymi stoją wszystkie kraje, w tym Stany Zjednoczone, oraz wyzwań i warunków towarzyszących tej nowej postaci wojny. Badacze amerykańscy z RAND Corporation wyróżnili dwie generacje strategicznej wojny informacyjnej (ang. Strategic Information Warfare, SIW). Pierwsza generacja rozumiana jest jako wojna sterowana za pomocą wielu narzędzi. Druga generacja to samodzielny, całkowicie nowy rodzaj wojny zapoczątkowany przez rewolucję informacyjną, który może być prowadzony w nowych obszarach wojny strategicznej, np. w obszarze gospodarki. Może on charakteryzować się znacznie dłuższym czasem trwania, w porównaniu z tym, jaki na ogół przypisywany jest wojnie strategicznej (Molander, Riddle, Wilson, 1998, s. 6.).

W Ośrodku Studiów Strategicznych i Międzynarodowych (Center for Strategic and International Studies) również opracowano raport grupy roboczej zatytułowany „Cybercrime ... Cyberterrorism... Cyberwarfare". Został w nim omówiony szereg zagrożeń stwarzanych przez ataki cyfrowe. Zwrócono także uwagę na problem strategicznej wojny informacyjnej. Podkreślono konieczność sprostania zsynchronizowanym atakom cyfrowym dokonywanym przez wyrafinowanych przeciwników. Zagrożenie

ia odpowiedniej polityki bezpieczeństwa
nymi możliwościami wywiadowczymi.
nej stała się popularna w kręgach akade-
ch się bezpieczeństwem narodowym.

pcji strategicznej wojny informacyjnej
erzenie pojęcia „strategiczna", które w li-
yło zarezerwowane dla użycia broni ją-
entalnym. Dzisiejsze rozumienie pojęcia
ej" wykracza poza ramy pojedynczej kla-
różnorodne środki, łącznie z technikami
zakłócania infrastruktury informacyjnej,
ne", niezależnie od ich zakresu i zasięgu.
i i systemów komputerowych zarówno
h w sektorze państwowym, militarnym,
na ten temat daje się do zrozumienia, że
o państwo, jak i inni udziałowcy konflik-
tem ataku. Ponadto autorzy opracowań
odstawy, na których były oparte analizy
ni często, że cyberprzestrzeń stanowi cał-
ządzące się nowymi regułami.

, czym jest wojna i jakie są jej wymiary
alizowane i zdefiniowane ponownie, aby
osób istniejące podstawy wiedzy mogą
zmodyfikowane na potrzeby analizy no-
y informacyjnej.

owana jako zespół środków umożliwia-
innym osiąganie celów poprzez ataki cy-
eciwnika. Jeżeli środkami ciężkości mają
którzy prowadzą strategiczną wojnę in-
umieć specyficzne wyzwania ofensywne
jnego cyberprzestrzeni. Nagromadzenie
nego może ułatwić zrozumienie wyzwań

ń o wojnie jest teza niemieckiego teore-
nie z którą to cel polityczny, jaki ma być
ynnikiem determinującym realizowane

cele wojskowe i podejmowane wysiłki. Twierdzi on, że „wojna jest polityką prowadzoną innymi środkami, nigdy zaś czymś autonomicznym". Chociaż często niesłusznie uważany jest on za zwolennika wojny totalnej, jasno wykazuje, że natura konfliktu zależy od motywów i kontekstu politycznego. Poprzez całą historię do czasów najnowszych wojny prowadzone są ograniczonymi środkami wojskowymi, w celu osiągnięcia możliwych korzyści politycznych. Clausewitz zauważa także, że „jeżeli jedna ze stron nie jest w stanie całkowicie rozbroić drugiej, pragnienie pokoju będzie narastało i opadało wraz z prawdopodobieństwem dalszych sukcesów i wysiłkiem, jakich będą one wymagały" (Clausewitz, 2013, s. 12.).

„Większość sytuacji, nawet wojennych, stanowi kombinację różnych zachęt do współdziałania i rywalizacji, nie zaś wyłącznie dążeń do całkowitego zniszczenia". Zależność pomiędzy celami politycznymi a użyciem środków wojskowych stanowi podstawę analiz strategicznej wojny informacyjnej.

Jednak takie podejście niesie ze sobą dwa ważne pytania: „co rozumiemy przez cele polityczne?" oraz „czyje cele bierzemy pod uwagę?". W większości dawnych rozważań strategicznych odpowiedzi na pierwsze pytanie dotyczą wzajemnego oddziaływania dwóch suwerennych państw. Carl von Clausewitz i inni podobnie myślący teoretycy skupiali się na sile wojskowej jako narzędziu władzy państwowej, pozostającym w wyłącznej dyspozycji rządów i służącym do osiągania celów państwa drogą wojen.

Rozwój i upowszechnienie w skali światowej technik transportu i łączności odegrały rolę czynnika wyzwalającego to zjawisko. Coraz powszechniejsze posługiwanie się technikami informacyjnymi zarówno przez państwowe systemy informacyjne, jak i niepaństwowe, czyni jednych i drugich zarówno użytkownikami, jak i celami strategicznej wojny informacyjnej.

Analizując zachowania sprawców wojen, należy odnieść się także do celów politycznych. Teoretycy stosunków międzynarodowych skupili się na celach politycznych związanych z korzyściami poszczególnych państw, takich jak zabezpieczenie terytorium, ustanowienie swobody handlu i dostępu do zasobów, lub dążeniu do mniej namacalnych celów, jak na przykład potęga międzynarodowa. Clausewitz i podobnie jak on myślący stratedzy postrzegali wojnę jako prowadzoną przez ustabilizowane jednostki polityczne o jasno określonych granicach.

Gregory J. Rattray w swojej książce TAO (Tajemnica. Atak. Obrona).

estrzeni nie oddziela motywów polityczwojny, a raczej odnosi się do celów poli- motywacji i wyników pożądanych przez siły.

INFRASTRUKTURĘ I MANIPULOWANIE

attray odróżnia ataki prowadzone za po- zakłócenia infrastruktury informacyjnej ediami i percepcją informacji przez dokategoria jest określana jako zarządzanie cji w celu wpłynięcia na decyzje politycznarodu i zakłócenia działalności gospoąca od starożytnych Greków aż po XXI aganda i technika piątej kolumny, którą rniły się do jego początkowych sukcesów zas zimnej wojny Związek Radziecki pro- celu osłabienie poparcia dla wydatków z spójności sojuszu atlantyckiego. Stany ły się w działalność kwalifikowaną jako ania skryte.

zgłośni telewizyjnych w czasie rzeczyietem przez przeciwników politycznych nych konfliktów. Wiek informacji niesie odzi o rolę dyplomacji państwowej, zaropagandy. Jednak to opracowanie konięcia sukcesu w nowoczesnym konflikcie frastruktury informacyjnej przeciwnika.

inna być traktowana jako zjawisko całtualną" lub „niefizyczną" naturę operacyberprzestrzeni. Wyrażenie „cyberści „science fiction" Wiliama Gibsona u lat dziewięćdziesiątych ubiegłego wielu komentatorów zajmujących się świa-

tem cyberprzestrzeni podkreśla, że jest to miejsce różniące się zasadniczo od normalnego świata oddziaływań fizycznych. Nicholas Negroponte z Massachusetts Institute of Technology z Media Lab stwierdził, że składnikiem elementarnym nie jest już atom, lecz cyfra binarna, czyli bit jako jednostka danych przedstawiana zwykle jako 0 lub 1. W „Time" opisano cyberprzestrzeń jako „przypominającą poziom form idealnych Platona, przestrzeń metaforyczną, rzeczywistość wirtualną".

Cyberprzestrzeń jest jednak w rzeczywistości domeną fizyczną, będącą wynikiem utworzenia systemów informacyjnych i sieci, które umożliwiają wzajemne oddziaływania drogą elektroniczną. Działalność człowieka na tym polu wymaga świadomego sterowania przepływem energii. Do przesyłania informacji komputerowych potrzeba jedynie niewielkiej energii w porównaniu z przelotem samolotu. Obydwa te działania wymagają jednak utworzenia i zapewnienia materialnych warunków.

Ci, którzy podejmują wojnę informacyjną, muszą znać zasady fizyczne i systemy rządzące środowiskiem informacyjnym, podobnie jak tradycyjni żołnierze, lotnicy i marynarze muszą rozumieć środowisko, w którym prowadzą wojnę.

Rodzaje ataków na infrastrukturę informacyjną

Potencjalni przeciwnicy mogą prowadzić ataki strategiczne na infrastrukturę informacyjną przy użyciu różnorodnych środków mechanicznych, elektromagnetycznych i cyfrowych.

1. Ataki mechaniczne. Systemy informacyjne i sieci od dawna były atakowane metodami mechanicznymi zmierzającymi do ich zakłócenia lub zniszczenia, zarówno podczas wojny jak i pokoju. Systemy dowodzenia i kierowania mogą być bombardowane, kable światłowodowe mogą być przecinane, anteny mikrofalowe niszczone, a komputery rozbijane lub po prostu wyłączane. Fizyczne przechwytywanie kurierów miało poważny wpływ na wyniki bitew w starożytności. Ataki mechaniczne wymagają od przeciwnika uzyskania bezpośredniego, fizycznego dostępu do celu. Wyniki tych ataków są na ogół łatwiejsze do zaobserwowania niż wyniki ataków prowadzonych środkami elektronicznymi.
2. Ataki elektromagnetyczne. Podzespoły elektroniczne oraz transmisja w systemach informacyjnych i w sieciach są wrażliwe na zakłócenia

rowaną na nie energią elektromagnetycz-
ıisji stosowano już od I wojny światowej,
: radia. Podczas zimnej wojny wiele uwagi
ɔulsu elektromagnetycznego, powstające-
ych. Jak wiadomo, wybuch jądrowy po-
a elektromagnetycznego, które wywołają
ch materiałach przewodzących. W rezul-
zniszczone systemy komunikacyjne i in-
ęćdziesiątych XX wieku zwrócono uwagę
efektów podobnych do impulsu elektro-
wionej i ukierunkowanej postaci. Jeżeli
zyskać i zachować odpowiednie zbliżenie
h, mogą uwzględnić w swoich planach
kowanej.

ożliwe i niebezpieczne są zagrożenia po-
óceniu systemów komputerowych i sieci
tych systemów informacyjnych. Efektem
ɔwity paraliż lub czasowe ich wyłączenie,
ie błędów do danych, kradzież informa-
ɣalne monitorowanie systemów i przej-
az wprowadzenie fałszywych informacji.
próbować wstawiać spreparowane ele-
rmacyjnej przeciwnika, co umożliwiłoby
e lub niszczenie jego systemów i sieci.

nacyjnej mogą być zastosowane wszyst-
ormacji i rozkazów składających się na
ch komputerowych są zapisywane w pa-
zas nadawania w obwodach komunika-
ı lub usunięcie informacji obejmuje bar-
je niewielkie ilości energii. Jednak są to
wanie kontroli nad systemem komputeo-
ości przez Internet jest w istocie atakiem
e być wyśledzone, a sam atak może być
a w przypadku ataków cyfrowych są cał-
ni mamy do czynienia przy użyciu broni
k taki sam, jak mechanicznych i elektro-

mechanicznych: spowodowanie zakłóceń i zniszczeń.

Strategiczna wojna informacyjna może być przeprowadzona z użyciem przemocy fizycznej lub może być jej pozbawiona. Gdy atak bombowy zniszczy węzeł komunikacyjny, lub atak elektromagnetyczny zablokuje mechanizmy sygnalizacji metra, powodując zderzenie pociągów, w sposób oczywisty mamy do czynienia z przemocą. Atakom cyfrowym mogą towarzyszyć podobne efekty, takie jak stopienie reaktora w elektrowni jądrowej spowodowanych wygięciem prętów sterowniczych lub zderzenia samolotów spowodowane wygaszeniem ekranów w systemach kontroli ruchu powietrznego. Ataki cyfrowe mogą również prowadzić do mniej widocznych efektów fizycznych, takich jak np. choroby powodowane zakłóceniami urządzeń sterujących uzdatnianiem wody. Chociaż ataki siejące tego rodzaju spustoszenie są rzadziej kwalifikowane jako ataki z użyciem przemocy, jednak wywoływane przez nie cierpienia bez wątpienia mogą być uznawane za czyn wojenny. Broń cyfrowa charakteryzuje się znacznym potencjałem uderzenia na przeciwników bez użycia przemocy. Zmiana informacji w systemach sterowania satelitów wojskowych danego kraju lub powodowanie zakłóceń, które podważają zaufanie do rynków giełdowych, mogą nie powodować bezpośrednio śmierci ani zniszczeń, jednak mimo to zagrażają operacjom istotnym dla bezpieczeństwa narodowego oraz instytucjom finansowym.

Rozważa się również kwestię, czy takie ataki oznaczają użycie siły w sensie tradycyjnym, opartym na poglądzie wyrażonym przez Clausewitza i powtarzanym przez wielu, że „istotą wojny jest przemoc". Jednak klasyczni analitycy wojny uznają, że przemoc nie musi odgrywać centralnej roli w osiąganiu celów, dla których prowadzone są wojny.

W porównaniu z innymi formami siły wojskowej broń cyfrowa ma charakter „mikro siły". Zmiany właściwości technicznych dotyczące rozwiniętych sił konwencjonalnych spowodowały również znaczące zmiany koncepcji ich użycia. Zwraca uwagę różnica między bronią informacyjną a energią używaną przy stosowaniu sił konwencjonalnych. Powstanie broni sterowanych precyzyjnie (ang. Precision Guided Munitions, PGM) słabo wykrywanych przez radary zwiększa znaczenie własnych źródeł informacji i redukuje informacje dostępne dla przeciwnika, umożliwiając maksymalne zniszczenia celów przy minimalnym wysiłku. Uważa się, że „precyzyjne zaangażowanie" stanowi koncepcję operacyjną, która zapewni stronie ją wykorzystującej dominację we wszystkich rodzajach konflik-

rmalizowania użycia własnych informacji
ości nieprzyjaciela do uzyskania informa-
zminimalizowania wymaganego wysiłku
ie wojny cyfrowej, będącej, jak wspomi-

y informacyjnej nie został dotychczas
zność w osiąganiu celów politycznych
ogicznie, tak jak w przypadku sił kon-
dzi o właściwe rozpoznanie, jakie wnio-
ch analiz, oraz na ile te podstawy muszą

NEJ WOJNY INFORMACYJNEJ

a obejmuje dążenia do pokonania prze-
obiekty. Przy próbie określenia podmio-
ategicznej wojny informacyjnej przydat-
ja jednostki strategicznej sformułowana
wierdzi, że: „jednostka strategiczna jest
iałać autonomicznie, która się sama kie-
ką strategiczną jest państwo, a także jest
zaju mafii, lub organizacja gospodarcza,
tnie, ani armia, ani lotnictwo nie są jed-
aż nie są one ani samokierujące się, ani
s. 7.).

e, jak i niepaństwowe muszą być ostroż-
dolni do prowadzenia wojny strategicz-
dzić, atakujący musi dysponować zdol-
ów oraz do kontrolowanego użycia siły
sywnych.

yć prowadzona przez grupy wewnątrz
b policję, dążące do zmiany porządku
raniczają się do przypadków obejmują-
. Istnieje jednak ważna szara strefa obej-
y one prowadzić strategiczną wojnę in-
ństw nieprzyjacielskich. Taka zbieżność
juszu i koordynacji oraz wsparcia z ze-

wnątrz destrukcyjnej działalności.

Podobnie jak w wypadku pozostałych form wojny, legalność struktur oraz obecność czynników religijnych i kulturowych odnoszących się do działań zaliczanych do kategorii strategicznej wojny informacyjnej może również wpływać na zachowanie uczestników.

Powstaje kilka pytań:

- Jakie rodzaje strategicznych ataków informacyjnych stanowiłyby akt wojny lub agresji, uprawniający państwa do powołania się na prawo do samoobrony?
- Kiedy efekt takich ataków stanowiłby wykroczenie przeciwko prawom osób nieuczestniczących w walce?
- Jakie zobowiązania mają strony neutralne, jeśli chodzi o posługiwanie się systemami telekomunikacyjnymi w celu transmitowania strategicznych ataków informacyjnych?
- Kiedy prezydent mógłby powoływać się na odpowiedzialność państwa za obronę infrastruktury informacyjnej, w ramach stanu wyjątkowego lub działań wojennych?
- Jak powinny być traktowane potencjalne ataki informacyjne dokonywane przez sprawców niepaństwowych?

Odpowiedzi na te pytania będą miały wpływ na decyzję wszystkich uczestników wojny oraz ofensywnych i defensywnych aspektów wojny informacyjnej.

Podsumowanie

Jak zatem widzimy, pojawiło się sporo trudności w sprecyzowaniu jasno wyrażonych granic prawnych co do wykorzystania cyberprzestrzeni w złych zamiarach. Powstała nowa dziedzina prawa obejmująca ochronę własności intelektualnej czy prywatności handlu elektronicznego. Istnieje jednak możliwość przekraczania granic narodowych przez osoby dokonujące wykroczeń w cyberprzestrzeni oraz maskowania ich tożsamości. Oznacza to, że obecnie odróżnienie interesów państwowych od prywatnych jest niezwykle trudne. Trudności sprawia także kwalifikacja co do rodzajów konfliktu: międzynarodowy czy wewnętrzny? Zawarte w Karcie Narodów Zjednoczonych zakazy użycia siły, jak również dalsze próby zdefiniowania agresji lub interwencji, nie mają w sposób klarowny zastosowa-

ıwionych elementów destrukcji. Problem
erprzestrzeni, cieszy się rosnącym zainte-

jne, które powodują bezpośrednią prze-
kty o charakterze przemocy, w sposób
jako akty agresji.

ıej strony wojny informacyjnej pojawia-
go statusu wojny cyfrowej pozbawionej
aki na system bankowy lub bazę danych
:h).

lturowych i politycznych czynników od-
rony konfliktu może okazać się trudne
zenia strategicznej wojny informacyjnej.
:h jest sprawą zasadniczą dla polityki od-
ów informacyjnych lub polityki upoważ-
frowych jako środków przymusu.

w cyberprzestrzeni. Toruń: Wydawnictwo

rmacyjne a bezpieczeństwo państwa pol-
Adam Marszałek.
ożenia w środowisku bezpieczeństwa XXI
ırszawa: WSCiL.
M.F. (2003). *Cyberterroryzm i problemy*
o we współczesnym świecie. Warszawa:

o sieci. Warszawa: PWN.
ıgadnienia z zakresu prowadzenia ope-
aca wojska z mediami. *Myśl Wojskowa,*

formacyjna i bezpieczeństwo informacji.
kowo-Techniczne.
zenia w kształtowaniu społeczeństwa in-

formacyjnego. Dylematy cywilizacyjno- kulturowe. Kraków:; AGH.

Jachowicz, Ł. (2003). *Cyberterrorism and Cyberhooliganism.* Warszawa: Collegium Civitas.

Kisielnicki, J.(2011). Cyberterroryzm jako element zagrożenia współczesnej cywilizacji, Pozyskano (02.08.2013) z http://www.dobrauczelnia.pl/279.

Liedl, K. (2008). *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego.* Toruń: Wydawnictwo Adam Marszałek.

Lombard, D. (2009). *Globalna wioska cyfrowa. Drugie życie sieci.* Warszawa: Wydawnictwo MT Biznes.

Madej, M. (2007). *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego.* Warszawa: PISM.

Molander, R.C, Riddle, A.S., Wilson, P. A. David A. Mussington, D.A., Richard F. Mesic, R. F.(1998). *Strategic Information Warfare Rising.* Santa Monica CA: RAND Corporation.

Rattray, G.J. (2004), *Wojna strategiczna w cyberprzestrzeni.* Warszawa: Wydawnictwa Naukowo-Techniczne.

Ryan J. D. i Ryan J. C. H. (1996). Protecting the National Information Warfare: Cyberterroryzm: Protecting Your Personal Security in the Electronic Age. New York: Thunder`s Mouth Press, 2nd ed .

Schwartau, W. (1996). *Information Warfare.* New York: Thunder Mouth Press, 2nd ed.

Sienkiewicz, P. *Wizje i modele wojny informacyjnej.* Pozyskano (22.08.2014) z http://winntbg.bg.agh.edu.pl/skrypty2/0095/373-378.pdf.

Von Clausewitz, C. (2013). *O naturze wojny.* Biblioteka Analiz. Format PDF.

Warden, J. A. *The Enemy as a System.* Airpower Journal, Spring 1995. Pozyskano (22.08. 2014) z http://www.airpower.maxwell.af.mil/airchronicles/apj/apj95/spr95_files/warden.htm.