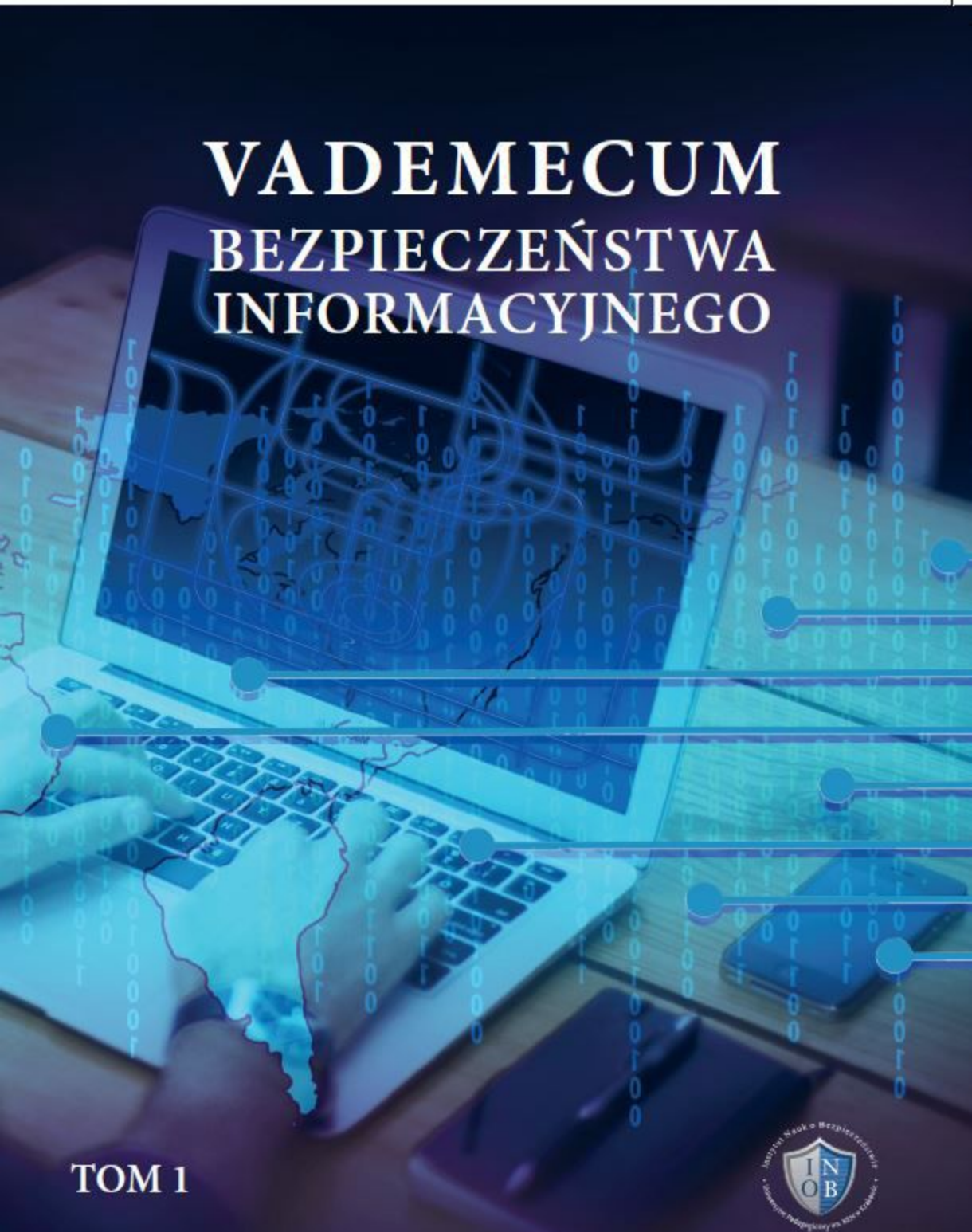
VADEMECUM
BEZPIECZEŃSTWA INFORMACYJNEGO



TOM 1

Instytut Nauk o Bezpieczeństwie
Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej
w Krakowie 2019

VADEMECUM
BEZPIECZEŃSTWA INFORMACYJNEGO

TOM 1

A–M

REDAKCJA NAUKOWA
OLGA WASIUTA, RAFAŁ KLEPKA

ISBN 978-83-66445-07-9
ISBN 978-83-66269-24-8

Recenzenci:
prof. dr hab. inż. Włodzimierz Gogołek
dr hab. Mirosław Lakomy, prof. AIK

Redakcja:
Małgorzata Tarnowska

Korekta:
Anna Surendra, Sebastian Surendra, Joanna Kłos

Skład:
LIBRON

Projekt okładki:
Justyna Rokitowska

Źródło grafiki wykorzystanej na okładce:
https://pixabay.com/pl/illustrations/binarny-r%C4%99ce-klawiatura-dotknij-2380422/

Publikacja sfinansowana przez Uniwersytet Pedagogiczny
im. Komisji Edukacji Narodowej

Wydawcy:

AT Wydawnictwo
ul Zachodnia 9/49
30-350 Kraków
tel.: 504 799 323
e-mail: wydawnictwoat@atgroup.pl
www.atwydawnictwo.pl

Wydawnictwo LIBRON – Filip Lohner
al. Daszyńskiego 21/13
31-537 Kraków
tel. 12 628 05 12
e-mail: office@libron.pl
www.libron.pl

Doubleswitch jest działaniem, którego sprawca może trwale zablokować lub wydłużyć okres, w którym kontroluje konto w serwisie społecznościowym, zmieniając nazwę użytkownika, a następnie usuwając oryginalne konto. Atak *doubleswitch* myli potencjalnych followersów i sprawia, że standardowe mechanizmy odzyskiwania są nieskuteczne. Platformy mediów społecznościowych zazwyczaj nie powiadamiają użytkowników o zmianach w nazwach użytkowników. Metodę można stosować także na innych serwisach społecznościowych, w tym na Facebooku i Instagramie.

Nowa forma ataku uwypukla nieprzewidziane luki w zasadach działania i funkcjach kont na Twitterze i w innych mediach społecznościowych. Powinna stanowić ostrzeżenie dla osób korzystających z tych platform – użytkownicy zagrożeni takimi atakami powinni stosować uwierzytelnianie wieloetapowe, aby w pierwszej kolejności zapobiec przejęciu kontroli nad kontem przez osoby niepowołane, a Twitter i platformy mediów społecznościowych z podobnymi funkcjami konta, takimi jak Facebook i Instagram, powinny aktualizować funkcje i zasady dotyczące ataku *doubleswitch*.

Jakub Idzik, Rafał Klepka

A New Social Media Attack Called "Doubleswitch", 10.06.2017, LatestHackingNews.com (dostęp 30.04.2019); AJ Dellinger, *DoubleSwitch Twitter Hack: New Attack Targets Activists On Twitter*, 06.09.17, IBITimes.com (dostęp 30.04.2019); W. Gogołek, *Komunikacja sieciowa. Uwarunkowania, kategorie i paradoksy*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2010; G. Masters, *'Doubleswitch' Targeting Activists via Social Media, Access Now Report,* 20.06.2017, SCMagazine.com (dostęp 30.04.2019); The "Doubleswitch" Social Media Attack: A Threat to Advocates in Venezuela and Worldwide, AccessNow.org (dostęp 30.04.2019); Q. Wong, *Twitter Hack: Activists and Journalists Targeted in 'Doubleswitch' Social Media Attack*, 9.06.2017, SiliconBeat.com (dostęp 30.04.2019).

DOWÓDZTWO OPERACJI CYBERNETYCZNYCH STANÓW ZJEDNOCZONYCH (U.S. Cyber Command, USCYBERCOM) rozpoczęło swoją działalność w 2009 r. Celem jego utworzenia była przede wszystkim chęć obrony sieci wojskowych przed zagrożeniami płynącymi z → cyberatak ów. Siedziba jednostki znajduje się w Fort Meade w stanie Maryland przy wywiadowczej Agencji Bezpieczeństwa Narodowego (National Security Agency, NSA). W połowie 2017 r. podjęto decyzje o jego unifikacji,

powołując niezależne dowództwo bojowe jako komendę funkcjonalną. Ustanowione 4 maja 2018 r. USCYBERCOM stało się 10. Narodowym Dowództwem Bojowym (ang. *unified combatant command*). Pierwszym dowódcą USCYBERCOM był gen. K.B. Alexander, a następnie – do 2014 r. – ltgen. J.M. Davis. Od kwietnia 2014 r. do maja 2018 r. dowódcą był adm. M.S. Rogers, a obecnie jest nim generał armii USA, dyrektor NSA i szef Centralnej Służby Bezpieczeństwa (Central Security Service, CSS), P.M. Nakasone.

USCYBERCOM prowadzi działalność na podstawie Strategii Cybernetycznej Departamentu Obrony z 2018 r. (Department of Defense Cyber Strategy 2018), a także Narodowej Strategii Cybernetycznej 2018 r. (National Cyber Strategy 2018) i celów opublikowanych w dokumencie wizyjnym z kwietnia 2018 r. (*Vision Document as of April 2018*).

Historyczne uwarunkowania powstania dowództwa nawiązują do postępu technologicznego oraz działalności →hakerów w świecie cybernetycznym. Już w 1972 r. naukowcy i specjaliści współpracujący z Departamentem Obrony USA (U.S. Department of Defense, DoD) dostrzegli problemy związane z lukami w oprogramowaniach wojskowych, a także sieciowych. Znaczenie funkcjonowania →cyberprzestrzeni i kwestie dotyczące jej bezpieczeństwa stały się problemem po zakończeniu zimnej wojny. Pierwszą organizacją, która podjęła się wyzwań związanych z zagrożeniami cybernetycznymi, była Joint Task Force – Computer Network Defence (JTF-CND), podlegająca bezpośrednio pod sekretarza obrony narodowej. Swą zdolność operacyjną i organizacyjną przy DoD nabyła ona 1 grudnia 1998 r., uzyskując pozwolenie na nadzorowanie i kierowanie operacjami służby wojskowej i sieciowej departamentu. JTF-CND w 2000 r. przekształciła się w Joint Task Force – Computer Network Operations (JTF-CNO), a w 2004 r. w Joint Task Force – Global Network Operations (JTF-GNO). W latach 2000–2002 działania operacyjne w cyberprzestrzeni miały również powiązania z Amerykańskim Dowództwem Kosmicznym (USSPACECOM), które w ramach formalnych uwarunkowań przejęło kontrolę nad pojawiającymi się coraz częściej atakami w sieci komputerowej DoD. USSPACECOM zostało ostatecznie rozwiązane, a jego zadania zostały przejęte przez U.S. Strategic Command (USSTRATCOM). Dodatkowo w 2004 r. ogłoszono, że do przestrzeni

lądowej, morskiej, powietrznej i kosmicznej dołączył piąty element współczesnego pola walki – cyberprzestrzeń, w której USA powinny być również zdolne do działań militarnych. W 2005 r. po reorganizacji USTRACOM została utworzona nowa komórka operacyjna do walki z cyberatakami: Joint Functional Component Command – Network Warfare (JFCC-NW). Na początku 2008 r. omówiono sugestie i sposoby zorganizowania cyberdowództwa w celu zwiększenia zdolności organizowania ochrony przed cyberatakami. Na poziomie departamentów przeanalizowano wizje i cele działalności przyszłej organizacji. Utworzone w 2009 r. USCYBERCOM przejęło zadania realizowane dotychczas przez JTF-GNO oraz JFCC-NW. Zdolność operacyjną uzyskało 21 maja 2010 r.

Na ogólnym poziomie działalność USCYBERCOM polegać powinna na działaniach defensywnych i ofensywnych uniemożliwiających pojawienie się zakłóceń funkcjonowania lub też zniszczenia systemów komunikacyjnych czy infrastruktury krytycznej państwa oraz przeciwstawienie się rozwiązaniom przeciwnika w celu uniknięcia ataku. Podstawowymi działaniami dowództwa są synchronizacja, koordynacja oraz planowanie operacji cyberprzestrzennych w obronie USA i ich interesów na świecie. W rezultacie zapewnione i zrealizowane zostają kwestie komunikacyjne, niezawodność w przesyłaniu → i n f o r m a c j i pomiędzy działającymi komórkami ds. zwalczania zagrożeń w cyberprzestrzeni oraz monitorowanie liczby ich występowania. Integracja jest elementem wspierania zdolności specjalistycznych sił zbrojnych do prowadzenia działań w szybkim tempie, ich skuteczności w zwalczaniu już obecnych zagrożeń oraz profilaktyka, która zapewni modernizację infrastruktury informatycznej, co będzie sprzyjać minimalizowaniu ryzyka wystąpienia ataków w przyszłości. Dodatkowo zapewnia ona zdolność do prowadzenia działań militarnych i innych operacji sił zbrojnych, ochraniając systemy uzbrojenia i dowodzenia. USCYBERCOM projektuje przestrzeń cybernetyczną oraz wzmacnia możliwości DoD do obsługiwania nowoczesnych sieci teleinformatycznych i komunikacyjnych, wspierając bezpieczne komunikowanie pomiędzy użytkownikiem a poleceniami głosowymi i funkcjonującymi aplikacjami.

USCYBERCOM składa się z:

- Army Cyber Command (ARCYBER) – jej działalność polega na obronie sieci wewnętrznej i zewnętrznych połączeń wojskowych.

Prowadzi ona operacje przez 24 godziny na dobę przez cały tydzień, ma w swojej strukturze ok. 16 500 żołnierzy i pracowników cywilnych. Priorytetem jej działalności jest bronienie sieci informatycznej Departamentu Obrony, dostarczanie efektywnych rozwiązań w celu zwalczania zagrożeń w realnym świecie, przeciwko wrogom czy ISIS. Odpowiednio wyszkolone jednostki są delegowane do prowadzenia szkoleń w zakresie zagrożeń płynących z cyberprzestrzeni, aby skutecznie i rzetelnie eliminować zagrożenia w przyszłości. Charakteryzują się niezwykle precyzyjnym przygotowaniem logistycznym i planistycznym.

- Air Forces Cyber/ Twenty-Fourth Air Force (AFCYBER) – Cybernetyczne Siły Powietrzne z siedzibą w Joint Base San Antonio-Lackland w Teksasie, odpowiedzialne za utrzymanie i bronienie sieci Sił Powietrznych w celu utrzymania przewagi informacyjnej w oddziałach wojskowych USA na całym świecie. Swą działalność opierają na sześciu filarach: budowania, zabezpieczania, działania i obrony sieci cybernetycznych, a także na taktyce i wsparciu dowódców w celu osiągnięcia przewagi w przestrzeni powietrznej i przeciwstawienie się przeciwnikowi.
- Fleet Cyber Command/ Tenth Fleet – oddział Marynarki Wojennej USA odpowiedzialny za operacje w działalności sieci informacyjnej, defensywne i ofensywne operacje w cyberprzestrzeni. Celem całej floty jest prowadzenie operacji w cyberprzestrzeni z zapewnieniem Marynarce Wojennej swobody działania w podejmowaniu decyzji. Fleet Cyber Command przypadają szczególne zadania, ponieważ jego misją jest planowanie, koordynowanie, integrowanie i synchronizowanie pełnego obrazu informacji. Podobną wizją cechuje się Tenth Fleet, który również dostarcza efekty planistyczne zawierające rozwiązania taktyczne i operacyjne oraz zapewnia ich pomyślną realizację w przestrzeni cybernetycznej.
- Marine Corps Forces Cyberspace Command (MARFORCYBER) – Dowództwo Cyberprzestrzeni Sił Morskich USA, jednostka odpowiadająca za ochronę infrastruktury krytycznej Sił Morskich. Oprócz standardowych zadań planistycznych, koordynacyjnych, synchronizacyjnych i kierowniczych oddział jest również

angażowany do działań operacyjnych w Departamencie Obrony i podległej sieci informatycznej (DoDIN – wsparcie dla integracji zarówno usług głosowych, jak i funkcjonalnych w aplikacjach, które są instalowane z użyciem bezpiecznego, szyfrowanego protokołu internetowego).

Dodatkowo warto również wspomnieć o symbolicznym znaczeniu logo Dowództwa Cybernetycznego Stanów Zjednoczonych, które składa się z kilku elementów. Są to:

- orzeł – symbol narodowy uosabiający przebijanie ciemności oraz zachowanie czujności;
- miecze na tarczy – symbol dowodzenia w obronie społeczeństwa USA;
- błyskawica – symbol szybkości w podejmowaniu trafnych i rzetelnych decyzji przy działalności operacyjnej w cyberprzestrzeni,
- klucz – zabezpieczający działanie mocarstwa w przestrzeni cybernetycznej.

Zwiększenie zasięgu pola walki oraz zmiany, które wynikają z pojawienia się nowych zagrożeń w przestrzeni cybernetycznej, nakładają na państwa (nie tylko na USA) reorganizację oraz wdrożenie nowych rozwiązań umożliwiających zapewnienie bezpieczeństwa. Zdolności planistyczne, organizacyjne wraz z koordynacją działań umożliwiają przechwycenie złośliwego oprogramowania i możliwość odparcia ataku.

Justyna Rokitowska

AFCyber.af.mil (dostęp 18.04.2019); J.L. Bayuk, J. Healey, P. Rohmeyer i in., *Cyber Security Policy Guidebook,* Wiley, New Jersey 2012; R. Ciastoń, *Piąty element. Czy zwycięstwa wojenne wkrótce będzie się odnosić w cyberprzestrzeni, a nie na realnym polu walki?*, „Polska Zbrojna" 2013, nr 11; G.A. Crowther, *USCYBERCOM,* [w:] *Encyclopedia of Cyber Warfare,* P.J. Springer (ed.), ABC-Clio, Santa Barbara, California 2017; Cybercom.mil (dostęp 18.04.2019); *Department of Defense Cyber Strategy*: *Summary 2018*; D. Dziwisz, *Stany Zjednoczone a międzynarodowe bezpieczeństwo cybernetyczne,* Communications4you, Kraków–Warszawa 2015; *Fleet Cyber Command (FCC)/ Tenth Fleet (C10F)*, Public.Navy.mil (dostęp 14.04.2019);

Marine Corps Forces Cyberspace Command, *MARCFORCYBER*, Candp.Marines.mil (dostęp 18.04.2019); *National Cyber Strategy of the United States of America,* September 2018; C. Paul, I.R. Porche III, E. Axelband, *The Other Quiet Professionals: Lessons for Future Cyber Forces from the Evolution of Special Forces,* Rand Corporation, Santa Monica, California 2014; *Achieve and Maintain Cyberspace Superiority Command Vision for US Cyber Command*, April 2018.

DOWÓDZTWO PRZESTRZENI CYBERNETYCZNEJ I INFORMACYJNEJ NIEMIEC (Kommando Cyber- und Informationsraum; KdoCIR) – cyberdowództwo w ramach Bundeswehry do walki w wirtualnej przestrzeni. Zostało powołane – obok wojsk lądowych, lotnictwa i marynarki wojennej – jako nowy, czwarty rodzaj wojsk i jest najmłodszym oddziałem armii niemieckiej. To zdecydowana odpowiedź Niemiec na wojnę w →cyberprzestrzeni.

W listopadzie 2015 r. niemieckie ministerstwo obrony powołało radę rozwoju CIR, której zadaniem było opracowanie planów reorganizacji →cyberbezpieczeństwa, IT, →wywiadu [t. 2] wojskowego, geoinformacyjnych i operacyjnych jednostek komunikacyjnych w obszarze cyberprzestrzeni i →przestrzeni informacyjnej [t. 2] Bundeswehry. 26 kwietnia 2016 r. minister obrony U. von der Leyen przedstawiła →opinii publicznej [t. 2] plany nowego oddziału wojskowego, a 5 października 2016 r. personel dowództwa zaczął działać jako departament w ministerstwie obrony. 14 października 2016 r. von der Leyen mianowała gen. L. Leinhosa szefem dowództwa świeżo utworzonej Przestrzeni Cybernetycznej. Na początku kwietnia 2017 r. uruchomiono nowy rodzaj wojsk – Dowództwo Przestrzeni Cybernetycznej i Informacyjnej z siedzibą w Bonn, które ma integrować zdolności w zakresie obrony cybernetycznej i prowadzenia operacji cybernetycznych w ramach Bundeswehry. Podczas inauguracji von der Leyen wspomniała o kamieniu milowym w niemieckim systemie obronnym, ponieważ →cyberataki stały się podstawowym zagrożeniem dla bezpieczeństwa.

Von der Leyen twierdzi, że Dowództwo Przestrzeni Cybernetycznej i Informacyjnej pozwala w razie ataku cybernetycznego na „ofensywną obronę". Gdy dojdzie do takiego zamachu na na niemiecką infrastrukturę, do działań owej ofensywnej obrony włączone będą inne instytucje państwa