THE WAR MUST GO ON

DYNAMIKA WOJNY W UKRAINIE I JEJ REPERKUSJE DLA BEZPIECZEŃSTWA POLSKI

POD REDAKCJĄ
ARTURA GRUSZCZAKA

THE WAR MUST GO ON

Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski

SOCIETAS

seria pod redakcją
BOGDANA SZLACHTY

138

THE WAR MUST GO ON

Dynamika wojny w Ukrainie i jej reperkusje dla bezpieczeństwa Polski

pod redakcją
Artura Gruszczaka

Kraków 2023

Artur Gruszczak
Uniwersytet Jagielloński
https://orcid.org/0000-0002-3450-8377
artur.gruszczak@uj.edu.pl

Recenzent
dr hab. Daniel Boćkowski, prof. UwB

Opracowanie redakcyjne
Magdalena Gibiec

Projekt okładki
Marta Jaszczuk

ISBN 978-83-8138-880-1
https://doi.org/10.12797/9788381388801

Autor zdjęcia na okładce: Yarohork (Adobe Stock)
Publikacja dofinansowana przez Instytut Nauk Politycznych i Stosunków Międzynarodowych UJ

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl
https://akademicka.pl

SPIS TREŚCI

CZĘŚĆ II
SKUTKI KONFLIKTU W UKRAINIE DLA BEZPIECZEŃSTWA POLSKI

THE WAR MUST GO ON. Dynamika wojny w Ukrainie
i jej reperkusje dla bezpieczeństwa Polski, s. 43-52
https://doi.org/10.12797/9788381388801.04

DOMINIKA DZIWISZ
BŁAŻEJ SAJDUK

ROSYJSKA INWAZJA NA UKRAINĘ A PRZYSZŁOŚĆ CYBERWOJNY – WNIOSKI W ROCZNICĘ „SPECJALNEJ OPERACJI WOJSKOWEJ"

Abstrakt

W rozdziale opisane zostały sposoby wykorzystania cyberprzestrzeni przez Rosję przeciwko Ukrainie w okresie bezpośrednio poprzedzającym wybuch wojny do 1 lutego 2023 r. Celem jest przedstawienie skomplikowanej natury działań w cyberprzestrzeni oraz próba wyjaśnienia rosyjskich założeń strategicznych w tej domenie wojny. Ponadto uwzględniono element prognostyczny obejmujący ewentualne konsekwencje rosyjskiej wojny w cyberprzestrzeni dla bezpieczeństwa Polski.

Słowa kluczowe: cyberbezpieczeństwo, cyberwojna, strategia, Ukraina, Rosja

Abstract

The Russian Invasion of Ukraine and the Future of Cyber Warfare – Conclusions on the Anniversary of the "Special Military Operation"

This chapter describes the ways how Russia has been using cyberspace against Ukraine, in the period immediately preceding the outbreak of the war until February 1, 2023. The aim is to present the complicated nature of activities in cyberspace and to try to explain Russian strategic assumptions in this domain of war. In addition, a prognostic

element was taken into consideration, including the possible consequences of the Russian war in cyberspace for the security of Poland.

Keywords: cybersecurity, cyberwar, strategy, Ukraine, Russia

Wprowadzenie

Od czasu inwazji Ukraina stoi w obliczu intensywnych rosyjskich ofensywnych operacji w cyberprzestrzeni, ale niewiele wskazuje na to, żeby przyczyniły się one do całościowego wysiłku wojennego Rosjan. Mimo różnic w wielu kwestiach autorzy analiz publikowanych w ciągu ostatnich 12 miesięcy są zgodni co do tego jednego aspektu. Jak pisze James Lewis z Center for Strategic and International Studies, „w dotychczasowej nieudolnej rosyjskiej inwazji, cyberoperacje przyniosły niewielkie korzyści"[1]. Jon Bateman z Carnegie Endowment for International Peace dodaje, że „rosyjskie operacje cybernetyczne w Ukrainie nie miały większego wpływu militarnego", a nawet, że jest to „upokarzającym doświadczeniem Rosji"[2]. Z kolei John Hultquist z Mandiant zwraca uwagę, że „wiele z przeprowadzonych ataków miało na celu wywarcie wpływu na ludność cywilną, a nie na cele wojskowe"[3]. Marcusa Willetta z International Institute for Strategic Studies zaskoczyło, że „rosyjskiej inwazji na Ukrainę w 2022 r. nie towarzyszyły od początku rosyjskie operacje cybernetyczne mające na celu znaczne wyłączenie infrastruktury krytycznej Ukrainy"[4]. Microsoft pisze o „ograniczonym wpływie" cyberoperacji oraz o gwałtownym spadku ich intensywności i tempa już na początku marca 2022 r.[5]

Na początku marca ubiegłego roku „The Washington Post" skatalogował kilkanaście możliwych wyjaśnień ograniczonego sukcesu operacji cybernetycznych, które towarzyszyły rosyjskiej inwazji. Na liście znalazły się: brak elastyczności zarządzania armią, unikanie ryzyka związanego z niekontrolowalnym rozprzestrzenianiem się

---

1 J.A. Lewis, *Cyber War and Ukraine*, Center for Strategic and International Studies, 16 VI 2022, [online] http://bit.ly/40v9GpR, 1 II 2023.

2 J. Bateman, *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Carnegie Endowment for International Peace, 16 XII 2022, [online] https://cutt.ly/I90pxsb, 25 I 2023.

3 M. Miller, *Russia's Cyberattacks Aim to „Terrorize" Ukrainians*, 11 I 2023, [online] http://bit.ly/3X4qy3N, 25 I 2023.

4 M. Willett, *The Cyber Dimension of the Russia–Ukraine War*, International Institute for Strategic Studies, 6 X 2022, [online] http://bit.ly/40u853y, 28 I 2023.

5 Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, 22 VI 2022, [online] https://bit.ly/3Y0OPZS, 11 I 2023, s. 5.

ataków na inne państwa czy też plan szybkiego zwycięstwa w pierwszych tygodniach wojny bez konieczności wykorzystania cyberzdolności[6]. Obecnie, na podstawie wiedzy z ostatnich miesięcy, listę tych czynników można ograniczyć. Jednym z tych, na które coraz częściej wskazują eksperci, jest brak koordynacji działań cybernetycznych z kinetycznymi. Rosyjscy stratedzy wojskowi zbyt wysoko ustawili poprzeczkę dla cyberoperacji, ponieważ oparli swoje planowanie na obserwacjach wojen toczonych w latach 90. XX w. i początku obecnego stulecia, a nie dostosowali ich do warunków wojny totalnej. Zabrakło pomysłu (i mocy przerobowych lub zdolności) na koordynację działań w różnych domenach prowadzenia wojny. Pomimo podejmowania takich prób w pierwszych tygodniach inwazji obecnie można zaobserwować wyłącznie niezależne od siebie wykorzystanie rosyjskiego potencjału[7]. Eksperci znajdują dwa wytłumaczenia. Jednym z nich jest brak możliwości tak dynamicznej koordynacji wynikający z rosyjskiego systemu dowodzenia. Jednakże nie można wykluczyć, że powodem braku koordynacji są różnice w celach rosyjskiej inwazji cybernetycznej i kinetycznej. Rosyjska strategia prowadzenia wojny może zakładać, że domena cybernetyczna służy głównie do wojny informacyjnej, a kinetyczna do przejmowania terytorium. Brak wykorzystania cyberzdolności do ataków na infrastrukturę krytyczną byłby więc rezultatem innych priorytetów, a nie braku umiejętności.

Warto pamiętać też o tym, że niszczycielskie skutki cyberataków mogą być odroczone, co sprawia, że oceny ich skuteczności nie można dokonać w czasie rzeczywistym. Niewykluczone, że dopiero w przyszłości dowiemy się, że przeprowadzono efektywne cyberataki, ale były one zbyt subtelne, by zostały wykryte na czas. Dlatego też brak spektakularnych i widocznych sukcesów Rosjan w cyberprzestrzeni nie może uśpić czujności Ukrainy i jej sojuszników, przede wszystkim państw sąsiadujących.

Na przestrzeni ostatnich miesięcy można wyróżnić kilka dających się wyodrębnić faz cyberoperacji, które często rozwijały się w zaskakującym dla analityków kierunku. W tym rozdziale przedstawione zostaną próby implementacji różnych strategii wykorzystania cyberprzestrzeni testowanych przez Rosjan w Ukrainie od okresu bezpośrednio poprzedzającego wojnę do dzisiaj (stan na dzień 1 lutego 2023 r.). Celem jest przedstawienie skomplikowanej natury działań w cyberprzestrzeni oraz próba wyjaśnienia rosyjskich założeń strategicznych w tej domenie wojny. Dodatkowo zarysowane zostaną ewentualne konsekwencje rosyjskiej wojny w cyberprzestrzeni dla bezpieczeństwa Polski.

---

[6] J. Marks, *11 Reasons We Haven't Seen Big Russian Cyberattacks Yet*, „The Washington Post", 3 III 2022, [online] https://tinyurl.com/32d5thsp, 16 I 2023.

[7] Microsoft, *Defending Ukraine…*

Strategia substytucji wojny

Istniejące teorie cyberkonfliktów zakładają różne możliwe bezpośrednie powiązania między działaniami w cyberprzestrzeni a działaniami kinetycznymi. Jeszcze przed wybuchem wojny szczególną popularność zyskała teoria substytucji[8]. W dużym skrócie sprowadza się ona do optymistycznego założenia, że poprzez działania w szarej strefie państwa mogą osiągnąć podobne efekty, co za pomocą siły kinetycznej. Zgodnie z nią, utrzymując swoje wrogie działania poniżej pewnego progu, państwa mogą intencjonalnie utrudniać ich interpretację na gruncie prawa międzynarodowego, aby przeszkodzić społeczności międzynarodowej w przypisywaniu odpowiedzialności sprawcy[9]. Jeszcze przed rozpoczęciem rosyjskiej inwazji zwolennicy tej teorii, jak Keir Giles z Chatham House, argumentowali, że „niszczycielski atak cybernetyczny może być wycelowany w wojskowe systemy dowodzenia i kontroli lub cywilną infrastrukturę krytyczną, i zmusić Kijów do ustępstw, a jego przyjaciół za granicą do spełnienia żądań Rosji"[10]. Między 2014 a 2022 r. Rosja próbowała implementować strategię substytucji. Cybernarzędzia z szarej strefy, w tym trwająca dezinformacja, propaganda informacyjna, ingerencja w wybory w 2014 r., cyberataki na infrastrukturę krytyczną w 2015 r. oraz cyberataki na ukraińskie ministerstwa i banki w lutym 2022 r., były formą ograniczonej rywalizacji wojskowej, która utrzymywała działania poniżej progu agresji. Najwyraźniej nie wystarczyło to, aby osiągnąć założone cele strategiczne i Kreml uznał, że jedyną opcją jest rozpoczęcie kampanii wojskowej[11].

Możliwe jest również, że Rosjanie od samego początku postrzegali cyberprzestrzeń jako najbardziej przydatną do realizacji celów informacyjnych, takich jak gromadzenie danych wywiadowczych w celu uzyskania lepszego wglądu w prowadzenie wojny, kradzież technologii, wpływanie na opinię publiczną, tworzenie i dostarczanie dezinformacji czy szerzenie chaosu. Jeśli tak, to rosyjscy hakerzy mogli zadowalająco

---

8 N. Kostyuk, E. Gartzke, *Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine*, „Texas National Security Review" 2022, t. 5, nr 3, s. 113-126, [online] bit.ly/3Hxk47Q, 20 I 2023.

9 D. Dziwisz, *Cyber Pearl Harbor Is Not Coming: US Politics Between War and Peace*, „Politeja" 2022, t. 19, nr 4(79), s. 95-109, [online] https://journals.akademicka.pl/politeja/article/view/4783, 21 XII 2022.

10 K. Giles, *Putin Does Not Need to Invade Ukraine to Get His Way*, Chatham House, 6 XII 2021, [online] https://cutt.ly/F90pR1l, 12 I 2023.

11 Brak skuteczności strategii substytucji w przypadku Rosji nie oznacza, że ta strategia nie może się sprawdzić w innych sytuacjach. Atak robaka komputerowego Stuxnet z 2010 r. jest przykładem udanego wykorzystania cyberkonfliktów jako substytutu wojny. Stuxnet zniszczył wirówki w irańskim obiekcie jądrowym Natanz, opóźniając w ten sposób program nuklearny. Atakujący nie musieli używać siły zbrojnej, ponieważ cyberataki osiągnęły podobne cele.

zrealizować cele stawiane przed nimi przez dowództwo, a rozczarowanie zachodnich analityków jest jedynie wynikiem ich braku znajomości rozkazów.

Doświadczenia z czasu pokoju i działań w szarej strefie pokazują, że cyberoperacje mogą być potężnym narzędziem szpiegowskim i propagandowym. Sprawdza się to również w czasie wojny[12]. Cyberoperacje mogą wspierać planowanie strategiczne, np. pomagając wybrać odpowiedni moment do rozpoczęcia inwazji. Mogą również wspierać działania okupacyjne, np. dezinformacji, tłumienia lokalnego oporu, identyfikowania Ukraińców powiązanych z działalnością partyzancką, śledzenia, aresztowania lub zabójstwa wybranych osób, weryfikacji rozpoznania sytuacyjnego, jakie Moskwa otrzymuje ze swoich źródeł HUMINT (wywiad agenturalny). W cyberprzestrzeni Rosjanie przeprowadzają także operacje wywierania wpływu, np. poprzez dyskredytowanie ważnych polityków ukraińskich i rozpowszechnianie fałszywych informacji.

Pełny zakres wpływów działań wywiadowczych, propagandowych i dezinformacyjnych w Ukrainie w czasie wojny bez wątpienia jest ogromny, ale także trudny do oceny ze względu na brak dostępności informacji niejawnych. Jeśli gromadzenie danych wywiadowczych było zasadniczym celem rosyjskich działań w cyberprzestrzeni, to nadal nie przyniosły one znaczących korzyści militarnych. Jon Bateman jest zdania, że „wiele potrzeb wywiadu wojskowego Moskwy może być łatwiej zaspokojonych przez źródła inne niż cybernetyczne. Mówiąc bardziej zasadniczo, ogólne podejście Rosji do wojny – od planowania kampanii po okupację zajętego terytorium – sugeruje, że kluczowe decyzje wojskowe nie są podejmowane na podstawie danych ze wszystkich źródeł”[13].

Strategia koordynacji

Nie ulega wątpliwości, że w pierwszych tygodniach wojny Rosja testowała uzupełnianie działań wojennych w klasycznych domenach operacjami w cyberprzestrzeni, dostosowując taktykę do realiów „gorącego konfliktu”. Natomiast wciąż nie ma przekonujących dowodów na to, że ofensywne działania w cyberprzestrzeni były koordynowane z konkretnymi operacjami kinetycznymi w takim stopniu, w jakim np. ostrzały rakietowe i artyleryjskie poprzedzają atak wojsk lądowych. Próby takiej synchronizacji

[12] J. Bateman, *Russia's Wartime…*
[13] *Tamże*.

sygnalizują m.in. raporty Microsoft z kwietnia i czerwca 2022 r.[14] Tezę taką stawiają też przedstawicie ukraińskiego rządu[15]. Jednakże istnieje również inne wyjaśnienie.

Niewykluczone, że masowa skala cyberataków z początku wojny spowodowała, że część z nich faktycznie współwystępowała z atakami kinetycznymi. Nawet jeśli Rosjanom udało się zsynchronizować ataki cybernetyczne z kinetycznymi, to efekt ofensywnego użycia cyberbroni dla końcowego przebiegu konfliktu pozostał nieznaczny. Dobrą ilustrację tego faktu stanowią cyberataki skierowane przeciw ukraińskim portalom informacyjnym (głównie przy użyciu wipera DesertBlade) oraz następujący po nich atak rakietowy na wieżę telewizyjną w Kijowie 1 marca 2022 r.[16] Cyberatak spowodował jedynie krótkotrwałe ograniczenie możliwości przekazywania informacji przez stronę ukraińską. Dopiero zniszczenie fizycznie istniejącej infrastruktury realnie osłabiło ukraińskie zdolności do oddziaływania informacyjnego.

Mniejszy wpływ rosyjskich cyberataków na losy wojny wynikać może także z tego, iż po pierwszych miesiącach inwazji ich wyrafinowanie i liczba wyraźnie spadły[17]. Miejsce wiperów wymazujących dane zajęły nieskomplikowane ataki phishingowe i DDoS[18]. Po przerwie operacyjnej początek roku 2023 przyniósł wzmożenie rosyjskich działań w cyberprzestrzeni, o czym informowała m.in. słowacka firma ESET, ustalając pojawienie się nowego wipera[19] stworzonego przez grupę Sandworm. Ponadto ukraiński CERT (Computer Emergency Response Team of Ukraine) podał, iż ukraińska agencja prasowa (Ukrinform) została zaatakowana przez mieszankę pięciu wiperów[20]. To, czy Rosja ponownie zintensyfikuje działania w cyberprzestrzeni, nie jest jeszcze przesądzone. Jednakże można oczekiwać, że skupi się na intensyfikacji działań dezinformacyjnych i wywiadowczych, zwłaszcza tych skierowanych przeciwko państwom i społeczeństwom wspierającym Ukrainę.

---

[14] Microsoft, *Special Report: Ukraine*, 27 IV 2022, [online] https://aka.ms/ukrainespecialreport, 27 I 2023; Microsoft, *Defending Ukraine*…

[15] State Service of Special Communication and Information Protection of Ukraine, *Cyber Attacks, Artillery, Propaganda. General Overview of The Dimensions of Russian Aggression*, 17 I 2023, [online] http://bit.ly/40tcGCP, 27 I 2023.

[16] Microsoft, *Special Report*…, s. 12.

[17] D.B. Johnson, *The Russia–Ukraine War Has Some Rrethinking the Role of Offensive Cyber Operations in Armed Conflict*, SC Media, 9 I 2023, [online] http://bit.ly/3l5ON4c, 27 I 2023.

[18] D. Kapur, T. Shloman, R. Venal, J. Fokker, *Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity*, Trellix, 24 I 2023, [online] http://bit.ly/3Y4jPIe, 27 I 2023.

[19] ESET, *SwiftSlicer: New Destructive Wiper Malware Strikes Ukraine*, WeLiveSecurity, 27 I 2023, [online] http://bit.ly/3RugiAs, 27 I 2023.

[20] C. Watts, *Preparing for a Russian Cyber Offensive Against Ukraine this Winter*, Microsoft, 3 XII 2022, [online] http://bit.ly/3kXvlqc, 27 I 2023.

Wnioski i prognoza dla Polski

Doświadczenia pierwszego roku rosyjskiej inwazji pozwalają na sformułowanie kilku wniosków dotyczących prób koordynacji działań w cyberprzestrzeni z operacjami kinetycznymi w miesiącach po rozpoczęciu działań wojennych.

Po pierwsze, w Federacji Rosyjskiej wciąż oficjalnie nie funkcjonuje centralne cyberdowództwo mogące nadzorować cyberoperacje realizowane przez rosyjskie służby i współpracujące z nimi podmioty prywatne. Może to być jeden z powodów, dla którego nie zaobserwowano znaczącego stopnia koordynacji działań w domenie cyber z operacjami kinetycznymi.

Po drugie, na podstawie analizowanych raportów można wysunąć wniosek, że dotychczas Rosjanie nie wykorzystali żadnej przełomowej cyberbroni[21] i prawdopodobnie żałują, że w chwili obecnej nie mogą powtórzyć cyberataków na ukraińskie elektrownie, takich jak te z 2015 i 2016 r. czy ataku NotPetya z 2017 r. Najpowszechniej stosowanymi formami ataku są wipery, a także phishing i DDoS.

Po trzecie, działania w cyberprzestrzeni mające na celu zakłócenie lub uszkodzenie wrogich systemów komunikacyjnych są czasochłonne, bo wymagają znalezienia dostępu do systemu. Co więcej, po wykryciu podatności, luki, które umożliwiły przeprowadzenie ataku, są szybko łatane i nie można ich ponownie wykorzystać. Dlatego cyberbroń, odwrotnie niż broń konwencjonalna, zwykle jest jednorazowego użytku. W rezultacie ze względu na bardzo różny charakter obu rodzajów broni koordynacja ich działań na polu walki jest niezwykle trudna.

Po czwarte, cyberprzestrzeń jest najbardziej przydatna w realizacji celów informacyjnych. W rosyjskim myśleniu cyberbroń nie wystarczy, by pokonać naród, i najlepiej wykorzystać ją do rywalizacji w sferze informacyjnej do zdobywania celów politycznych. Natomiast, kiedy celem jest zajęcie terytorium, siły kinetyczne są bardziej przewidywalne.

Po piąte, tocząca się wojna potwierdza, iż bezsprzeczne korzyści cyberoperacji w trakcie konfliktu znajdującego się pod progiem agresji tracą na znaczeniu, gdy konflikt staje się „gorący". Kluczowa zaleta cyberdziałań, czyli problem atrybucji – jednoznacznego wskazania podmiotu atakującego w cyberprzestrzeni – traci na znaczeniu, gdy obie strony znajdują się już w fazie fizycznej konfrontacji i ich wzajemne intencje są jasne. Druga z zalet prowadzenia wrogich działań w cyberprzestrzeni – łatwość w dezorganizowaniu wymiany informacji przeciwnika – może być efektywniej osiągnięta np. atakami rakietowymi na elementy infrastruktury teleinformatycznej. Trzecia z zalet

[21] J. Bateman, *Russia's Wartime*…, Figure 1, s. 12.

cyberoperacji – aterytorialność, czyli możliwość ich realizacji z dowolnego miejsca na Ziemi – traci na znaczeniu w sytuacji, kiedy można atakować cele kinetycznie na całym terytorium wroga (tak jak robią to Rosjanie, atakując cele w Ukrainie).

W aktualnej fazie wojny Rosja kontynuuje wykorzystanie cyberprzestrzeni do prowadzenia działań w szarej strefie w stosunku do państw wspierających Ukrainę. Z tego powodu można spodziewać się rosnącej intensyfikacji działań dezinformacyjnych oraz wywiadowczych. Świadczą o tym m.in. opinie ekspertów Microsoft, którzy wskazują, że rosyjskie wrogie działania wymierzone w państwa wspierające Ukrainę mają głównie charakter wywiadowczy, w tym np. te wymierzone w polskie podmioty miały na celu nie tyle uszkodzenie systemów, a zdobywanie informacji o procesie logistycznym związanym z przekazywaniem pomocy Ukrainie. Na duże możliwości dezinformacyjne Kremla zwraca także uwagę gen. Karol Molenda, dowódca Wojsk Obrony Cyberprzestrzeni. Głównym celem Rosji jest przecież podważenie koalicji, które są niezbędne dla odporności Ukrainy, w tym przepływu pomocy humanitarnej i wojskowej[22]. Rosyjska machina propagandowa była szczególnie aktywna, gdy amerykańska agencja informacyjna Associated Press zaczęła rozpowszechniać informację, że rosyjskie rakiety spadły na polską wieś Przewodów w pobliżu granicy z Ukrainą, zabijając dwie osoby. Moskwa oskarżyła wtedy Ukrainę o celowy atak na Polskę i NATO. Można przewidywać, że każda podobnie niejednoznaczna sytuacja zostanie wykorzystana do wbicia klina w stosunki polsko-ukraińskie. Analizując dotychczasowe sukcesy i porażki rosyjskich operacji cybernetycznych w Polsce, można również założyć, że na razie operacje informacyjne i psychologiczne wydają się być pierwszą opcją rosyjską. Biorąc to pod uwagę, konieczne jest zwrócenie uwagi na szczególnie ważną rolę, jaką odgrywają w Polsce państwowe media publiczne. Powinny być one obiektywne, bezstronne i informacyjne. Nade wszystko publiczne programy i kanały informacyjne powinny cieszyć się zaufaniem odbiorców, a w przypadku Polski występuje tu niestety spory deficyt[23].

Powyższe wnioski oczywiście nie wykluczają podejmowania prób cyberataków na infrastrukturę krytyczną, zwłaszcza, że w swoim arsenale Rosja nie posiada narzędzi pozwalających na symetryczną odpowiedź w stosunku do zachodnich sankcji gospodarczych. Wraz z wybuchem wojny w Ukrainie nastąpił gwałtowny wzrost liczby cyberataków na elementy infrastruktury krytycznej w Polsce. Dlatego Polska powinna być przygotowana na możliwość przeprowadzenia przez Rosję ataku ransomware.

---

[22] B. Lewicki, *Polski dowódca: Wszyscy spodziewali się swoistego „cyber Pearl Harbor". Ukraina była jednak przygotowana*, Dziennik.pl, 9 VI 2022, [online] http://bit.ly/3JFnTKQ, 2 II 2023.

[23] D. Dziwisz, B. Sajduk, *To War or not to War? Russia's Cyber Strategies in Ukraine 2014–22*, „New Eastern Europe" (w trakcie procesu wydawniczego).

Szczególnie zagrożone są państwa i firmy zaopatrujące Ukrainę w niezbędne łańcuchy dostaw pomocy i broni. W związku z tym, a także biorąc pod uwagę cyberpotencjał, jakim dysponuje nasze państwo, i ograniczone możliwości ofensywy w cyberprzestrzeni, uzasadnione wydaje się, aby w rozwoju polskich Wojsk Obrony Cyberprzestrzeni szczególnie duży nacisk kłaść na rozwijanie zdolności pozwalających zwalczać dezinformację, a także możliwości obronnych i wywiadowczych.

Bibliografia

Bateman J., *Russia's Wartime Cyber Operations in Ukraine: Military Impacts, Influences, and Implications*, Carnegie Endowment for International Peace, 16 XII 2022, [online] https://cutt.ly/I90pxsb.

Dziwisz D., *Cyber Pearl Harbor Is Not Coming: US Politics Between War and Peace*, „Politeja" 2022, t. 19, nr 4(79), s. 95-109, https://doi.org/10.12797/Politeja.19.2022.79.07.

Dziwisz D., Sajduk B., *To War or not to War? Russia's Cyber Strategies in Ukraine 2014-22*, „New Eastern Europe" (w trakcie procesu wydawniczego).

ESET, *SwiftSlicer: New Destructive Wiper Malware Strikes Ukraine*, WeLiveSecurity, 27 I 2023, [online] http://bit.ly/3RugiAs.

Giles K., *Putin Does Not Need to Invade Ukraine to Get His Way*, Chatham House, 6 XII 2021, [online] https://cutt.ly/F90pR1l.

Johnson D.B., *The Russia–Ukraine War Has Some Rethinking the Role of Offensive Cyber Operations in Armed Conflict*, SC Media, 9 I 2023, [online] http://bit.ly/3l5ON4c.

Kapur D., Shloman T., Venal R., Fokker J., *Cyberattacks Targeting Ukraine Increase 20-fold at End of 2022 Fueled by Russia-linked Gamaredon Activity*, Trellix, 24 I 2023, [online] http://bit.ly/3Y4jPIe.

Kostyuk N., Gartzke E., *Why Cyber Dogs Have Yet to Bark Loudly in Russia's Invasion of Ukraine*, „Texas National Security Review" 2022, t. 5, nr 3, s. 113-126, http://dx.doi.org/10.26153/tsw/42073.

Lewicki B., *Polski dowódca: Wszyscy spodziewali się swoistego „cyber Pearl Harbor". Ukraina była jednak przygotowana*, Dziennik.pl, 9 VI 2022, [online] http://bit.ly/3JFnTKQ.

Lewis J. A., *Cyber War and Ukraine*, Center for Strategic and International Studies, 16 VI 2022, [online] http://bit.ly/40v9GpR.

Marks J., *11 Reasons We Haven't Seen Big Russian Cyberattacks Yet*, „The Washington Post", 3 III 2022, [online] https://tinyurl.com/32d5thsp.

Microsoft, *Defending Ukraine: Early Lessons from the Cyber War*, 22 VI 2022, [online] https://bit.ly/3Y0OPZS.

Microsoft, *Special Report: Ukraine*, 27 IV 2022, [online] https://aka.ms/ukrainespecialreport.

Miller M., *Russia's Cyberattacks Aim to „Terrorize" Ukrainians*, 11 I 2023, [online] http://bit.ly/3X4qy3N.

State Service of Special Communication and Information Protection of Ukraine, *Cyber Attacks, Artillery, Propaganda. General Overview of the Dimensions of Russian Aggression*, 17 I 2023, [online] http://bit.ly/40tcGCP.

Watts C., *Preparing for a Russian Cyber Offensive Against Ukraine this Winter*, Microsoft, 3 XII 2022, [online] http://bit.ly/3kXvlqc, 27 I 2023.

Willett M., *The Cyber Dimension of the Russia–Ukraine War*, International Institute for Strategic Studies, 6 X 2022, [online] http://bit.ly/40u853y.

Minął rok od brutalnej napaści zbrojnej Federacji Rosyjskiej na Ukrainę. Rosyjska agresja była ciosem w chwiejący się liberalny porządek międzynarodowy łączony z uniwersalnymi – jak się wydawało – wartościami i zasadami, takimi jak praworządność, suwerenność, pokój czy współpraca. Była również brutalnym aktem podważenia zrębów pozimnowojennego systemu bezpieczeństwa międzynarodowego, kwestionującym jego logikę oraz rewidującym mechanizmy utrzymujące go w stanie względnej równowagi.

Wybuch wojny w Ukrainie wstrząsnął fundamentami porządku międzynarodowego i wyzwolił energię, która podsyca działania zbrojne oraz odsuwa perspektywę pokojowego zakończenia wojny w odległą przyszłość. Ma to istotne konsekwencje nie tylko dla bezpośrednich stron konfliktu, tj. Rosji i Ukrainy, lecz także dla państw graniczących z obydwoma krajami, w tym Polski.

Niniejsza książka zawiera zestaw krótkich artykułów analityczno-prognostycznych napisanych przez naukowców z Katedry Bezpieczeństwa Narodowego, odnoszących się do zasadniczych aspektów wojny w Ukrainie i jej różnorodnych reperkusji, w szczególności skutków dla bezpieczeństwa Polski.

WYDAWNICTWO
KSIĘGARNIA AKADEMICKA

https://akademicka.pl

ISBN 978-83-8138-880-1
9 788381 388801