FOLIA 414

Annales Universitatis Paedagogicae Cracoviensis

Studia de Securitate 14(2) (2024)

ISSN 2657-8549

DOI 10.24917/26578549.14.2.13

Joanna Kowalska
Akademia Sztuki Wojennej
ORCID 0009-0002-7748-1861

Współczesne cyberzagrożenia wyzwaniem dla bezpieczeństwa Rzeczypospolitej Polskiej

Contemporary Cyber Threats as a Challenge to the Security of the Republic of Poland

Abstrakt

Celem niniejszego opracowania jest analiza i ocena współczesnych wyzwań i zagrożeń w obszarze cyberbezpieczeństwa Rzeczypospolitej Polskiej. Główny problem badawczy stanowi próba odpowiedzi na pytanie: jakie ryzyka i zagrożenia stoją przed państwem polskim w obliczu dynamicznego wykorzystywania cyberprzestrzeni?

Znalezienie odpowiedzi na powyższą kwestię jest możliwe dzięki analizie i porównaniu raportów o stanie bezpieczeństwa w cyberprzestrzeni. W artykule przyjęto hipotezę, iż cyberzagrożenia stanowić będą jeden z głównych problemów dla bezpieczeństwa narodowego Polski w przyszłości, dlatego należy formułować efektywne prognozy polegające na wskazywaniu, z jakimi zagrożeniami i ryzykiem przyjdzie nam się zmierzyć. Metodyka badań oparta została o krytyczną analizę literatury. Wielowymiarowość rozpatrywanych wyzwań wymagała zastosowania wielu metod badawczych, takich jak: analiza dokumentów strategicznych, literatury oraz dostępnych materiałów dydaktycznych dotyczących tematyki cyberzagrożeń, a także syntezy dostępnej wiedzy, analogii, wnioskowania.

Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń, cyberatak, wyzwanie, zagrożenia, bezpieczeństwo RP.

Abstract

The purpose of this study is to analyze and assess contemporary challenges and threats in the area of cybersecurity facing the Republic of Poland. The central research question addresses what risks and threats the Polish State encounters amid the dynamic use of cyberspace. Answering this question involves analyzing and comparing available reports on the current state of security

in cyberspace. The article assumes the hypothesis that cyber threats will constitute one of the main challenges to Poland's national security in the future. Consequently, it is necessary to formulate effective forecasts by identifying potential threats and risks. The research methodology is based on a critical analysis of the literature. The multidimensionality of the challenges under consideration requires the use of several research methods, such as the analysis of strategic documents, academic literature, and available educational materials related to cyber threats, as well as synthesis, analogy, and inference.

Keywords: cybersecurity, cyberspace, cyberattack, challenge, threats, security

Wprowadzenie

Rozważania zacząć warto od przypomnienia początków narzędzia, jakim jest internet, bez którego trudno już sobie wyobrazić współczesny świat. Dzięki inicjatywie prezydenta Stanów Zjednoczonych Dwighta Eisenhowera (dokładnie w 1958 roku) rozpoczęła działalność organizacja ARPA (Advanced Research Project Agency). Początkowo jej celem było prowadzenie projektów skierowanych głównie do walki przeciwko zagrożeniu ze strony Związku Socjalistycznych Republik Radzieckich. Oficjalnie sieć powstała 1 stycznia 1983 roku, a więc istnieje dopiero od 41 lat.

Dynamiczny rozwój internetu oraz jego komercjalizację obserwuje się w latach 90. XX wieku. Pojawiają się wtedy pierwsze fora społecznościowe, poczta elektroniczna, komunikatory, strony internetowe. W 1991 roku w Polsce została wysłana pierwsza wiadomość mailowa[1].

Internet jest bez wątpienia jednym z najważniejszych narzędzi rozwoju cywilizacji. Szacuje się, iż obecnie na świecie występuje ponad pięć bilionów miliardów aktywnych użytkowników; jest to zatem około 66% populacji świata. Statystyki potwierdzają, że ta liczba będzie cały czas wzrastać, by w 2029 roku osiągnąć wartość blisko osiem miliardów. Tym samym oczekuje się, iż w zaledwie pięć lat liczba odbiorców wzrośnie o prawie połowę. Warto przyjrzeć się populacjom online na całym świecie – od 2023 roku Chiny pozostają wiodącym rynkiem pod względem liczby odbiorców internetu na świecie, następne w kolejności są Indie i USA.

Dostęp do sieci oraz populacja cyfrowa wyraźnie rosną, jednocześnie w wielu częściach świata proces ten znacząco się różni. W zależności od regionu nadal istnieją obszary, w których łączność z internetem pozostaje znacznie niższa niż średnia światowa. Afryka miała najniższą liczbę użytkowników stacjonarnego internetu szerokopasmowego w 2022 roku, podczas gdy Azja i Pacyfik przodują w rankingu. Istnieją regiony, gdzie dostęp do internetu dla ogółu społeczeństwa jest bardzo ograniczony przez rząd, a jego odbiór jest możliwy tylko za specjalnym zezwoleniem.

Interesujący jest fakt, iż możliwości internetu wciąż ewoluują, a co za tym idzie populacja, która korzysta z jego dobrodziejstw, jest w coraz większym stopniu narażona

[1] D. Duda (2023). *Cyberzagrożenia wyzwaniem dla państwa i społeczeństwa*. W: R. Szynowski (red.). *Wybrane problemy badań bezpieczeństwa z perspektywy młodych naukowców.* Wydawnictwo Naukowe Akademii WSB. Dąbrowa Górnicza, s. 115.

na cyberzagrożenia. Internet stale podlega modernizacji, by nadążyć za zmieniającym sie życiem użytkowników, w następstwie czego powstają kolejne zagrożenia. Średnio w sieci użytkownik spędza 6,5 godziny dziennie. Ilość czasu spędzanego w sieci różni się w zależności od grupy wiekowej: młodzież w wieku od 16 do 24 lat spędza 2,5 godziny więcej niż osoby w wieku od 55 do 64 lat. Równie ciekawa rysuje się demografia internautów: w kwietniu 2024 roku około 70% męskiej populacji na świecie korzystało z internetu, dla porównania wśród kobiet to 64%. Ta dysproporcja zauważalna jest w prawie wszystkich regionach świata, w większej mierze występuje w krajach najsłabiej rozwiniętych.

Statystyki z działalności w sieci są imponujące: każdego dnia publikowanych jest 7,5 miliona wpisów na blogach, a 5,04 miliarda ludzi używa mediów społecznościowych. Miejsca te stają się jednocześnie skarbnicą wiedzy o osobach korzystających z nich, jednocześnie będąc ogromnym zasobem wiedzy dla cyberprzestępców. Zwiększone korzystanie z internetu to zagrożenia cybernetyczne i obawy dotyczące bezpieczeństwa. Po drugiej stronie znajdują się miliardy osób, które czerpią korzyści z korzystania z sieci, zaś ich praca i wartości ewoluują wraz z dynamiczną transformacją cyfrową.

Niezaprzeczalnie dostęp do sieci stał się łatwiejszy niż kiedykolwiek, większość ludzi ma go w zasięgu swojej dłoni i praktycznie zawsze przy sobie (smartfony). Internet oferuje użytkownikom wachlarz możliwości i wszechstronny sposób interakcji z zasobami i usługami, niezależnie od tego, czy mowa o pracy, szkole czy spędzaniu wolnego czasu.

Wiele narzędzi, które znacząco uprościły życie populacji cyfrowej poprzez m.in. stosowanie elektronicznych podpisów czy prowadzenie kont bankowych w sieci, firm internetowych, ogólnoświatową wymianę, przyczyniło się także do rozwijania środowiska hakerów oraz szkodliwego oprogramowania. Często użytkownicy nie są świadomi, jakie zagrożenia niesie za sobą nierozważne i nieumiejętne korzystanie z nowoczesnych technologii. Poważna w skutkach może okazać się m.in. utrata wrażliwych danych (np. bankowych).

Niestety, podczas gdy cyberprzestrzeń stała się obrazem rzeczywistości, pojawiło się wiele zagrożeń stanowiących wyzwanie dla państwa polskiego. Są to m.in.: cyberprzestępczość, cyberdemonstracje, cyberszpiegostwo, cyberprzemoc, kradzież danych, kradzież tożsamości.

Podsumowując powyższe rozważania, stwierdzić należy, iż pomimo wielu zalet, które wynikają z rozwoju cyberprzestrzeni, można też wyodrębnić szereg zagrożeń, a także związanych z nimi wyzwań, które stanowią interesujący przedmiot naukowej eksploracji.

Ocena aktualnego stanu wiedzy

Nieustanny rozwój techniki i technologii informacyjnych tworzy idealne pole do budowania sieci zależności między użytkownikami, zmniejsza odległości, ułatwia dostęp do wiedzy, kontaktów międzynarodowych, jednocześnie będąc miejscem do powstawania nowych zagrożeń i konfliktów. Cyberprzestrzeń jest hybrydą dającą milionom ludzi

niesamowite możliwości działania, tym samym niosąc ze sobą duże niebezpieczeństwo. Państwa, jak i indywidualni użytkownicy są narażeni na różnego rodzaju ataki, zaś największą trudność sprawia identyfikacja agresorów, ponieważ mają oni po swojej stronie potężne narzędzie, jakim jest anonimowość. Za szczególnie ważne dla cyberbezpieczeństwa uznaje się ataki w kierunku infrastruktury krytycznej państwa. Co istotne, naruszenie jednego składnika tej infrastruktury przez jej powiązania systemowe ma zazwyczaj negatywny wpływ na pozostałe urządzenia. Finalnie skutki takiego ataku mogą być odczuwalne dla całego państwa, w tym jego gospodarki.

Zdaniem autora punktem wspólnym jest przeświadczenie o istocie tych zagrożeń w obszarze bezpieczeństwa narodowego państwa. Ryzyko, jakie niesie za sobą użytkowanie cyberprzestrzeni, będzie ewoluować, gdyż liczba incydentów w sieci ma tendencję wzrostową[2].

Istotną pozycją w literaturze przedmiotu jest publikacja C. Banasińskiego[3], który podaje prawne podstawy cyberbezpieczeństwa oraz specyfikę zagrożeń w cyberprzestrzeni. Wartą uwagi pozycją jest „Cyberbezpieczeństwo dzieci i młodzieży – realny i wirtualny problem polityki bezpieczeństwa" pod red. M. Górki[4]. Autorzy dotykają problemów facebookowego dzieciństwa, cyberprzemocy, jak również postępu technologicznego będącego źródłem ryzyka. Zetknięcie się z cyberświatem od najmłodszych lat przybliża „Uczeń bezpieczny w cyberprzestrzeni" pod red. D. Szeligiewicz-Urban[5]. Kolejnym przydatnym źródłem informacji dla niniejszej pracy i rozważań stanowi praca pod red. T. Dębowskiego „Cyberbezpieczeństwo wyzwaniem XXI wieku"[6].

Jednym z najistotniejszych źródeł wiedzy na temat cyberzagrożeń stanowią raporty cyberbezpieczeństwa zawierające statystyki zagrożeń dla instytucji, podmiotów oraz organizacji pokazujących ryzyko występujące w cyberprzestrzeni z podziałem na poszczególne kategorie. Opracowania zostały stworzone przez m.in. właściwe zespoły CSIRT (ABW, NASK)[7].

---

[2] Por. CSIRT GOV (2023). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2023 roku*. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp 14.10.2024].

[3] C. Banasiński (red.). (2018). *Cyberbezpieczeństwo. Zarys wykładu.* Wydawnictwo Wolters Kluwer Polska. Warszawa.

[4] M. Górka (red.). (2017). *Cyberbezpieczeństwo dzieci i młodzieży – realny i wirtualny problem polityki bezpieczeństwa*. Wydawnictwo Difin. Warszawa.

[5] D. Szeligiewicz-Urban (red.). (2012). *Uczeń bezpieczny w cyberprzestrzeni*. Wydawnictwo Humanitas. Sosnowiec.

[6] T. Dębowski (red.). (2018). *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Wydawnictwo ArchaeGraph. Wrocław.

[7] CSIRT GOV (2023). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2023 roku*. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp 14.10.2024]; PIB NASK (2024). *SECURE 2024*. https://www.nask.pl/pl/aktualnosci/5377,SECURE-2024-wyznaczamy-horyzont-cyberbezpieczenstwa.html [dostęp 17.10.2024].

Metodologia badania

Celem niniejszego artykułu jest analiza i ocena współczesnych wyzwań i zagrożeń w obszarze cyberbezpieczeństwa Rzeczypospolitej Polskiej. Głównym problemem badawczym jest próba odpowiedzi na pytanie: jakie ryzyka i zagrożenia stoją przed państwem polskim w obliczu dynamicznego wykorzystywania cyberprzestrzeni? Hipoteza badawcza postawiona w pracy stanowi, iż cyberzagrożenia są jednym z głównych problemów dla bezpieczeństwa narodowego Polski w przyszłości, dlatego należy jasno formułować efektywne prognozy polegające na wskazywaniu, z jakimi zagrożeniami przyjdzie państwu się zmierzyć. Złożoność rozpatrywanych problemów wymagała zastosowania wielu metod badawczych, takich jak: analiza i porównanie najważniejszych dokumentów wydanych w obszarze cyberzagrożeń.

Metodyka badań przyjęta w artykule to przede wszystkim analiza materiałów prasowych oraz literatury naukowej odnoszącej się do cyberataków i ryzyka związanego z działalnością w internecie. W artykule wykorzystano m.in. materiały opublikowane na stronach internetowych, jak i dostępne raporty służb, w tym Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT (Computer Security Incident Response Team). Wykorzystano także dane pochodzące z oficjalnych stron krajowych agencji prasowych.

Wyniki badań

Zgodnie z „Raportem o stanie bezpieczeństwa Cyberprzestrzeni RP w 2023 roku" miniony rok przyniósł kolejną falę zagrożeń w cyberprzestrzeni, naznaczonych sytuacją na wschodniej granicy RP. W roku 2023 CSIRT odnotował łącznie 43 785 faktycznych incydentów dotyczących bezpieczeństwa teleinformatycznego[8].

Polska, jako członek Unii Europejskiej oraz Paktu Północnoatlantyckiego, mierzy się z zagrożeniami ze strony grup cyberprzestępczych, haktywistycznych czy grup typu *state-sponsored*. Co najbardziej niepokojące, szczególnym zainteresowaniem cieszą się czołowe organy państwowe, np. ministerstwa, organy administracji rządowej, służby oraz infrastruktura krytyczna, w szczególności w sektorze energii oraz transportu. Najczęściej wykrywane zagrożenia dotyczą przede wszystkim ataków powodujących zakłócenia dostępności stron internetowych czy usług elektronicznych, próby włamań do systemów teleinformatycznych, infrastruktury sieciowej czy wtargnięć na poczty elektroniczne.

Podsumowując rok 2023, trzeba zauważyć, że Polska jako państwo członkowskie NATO stanowiła jeden z głównych celów ataków grup haktywistycznych. Prowadzą one wzmożone działania wobec krajów uznawanych za sprzeciwiające się polityce Federacji Rosyjskiej, starając się doprowadzić do dezinformacji oraz zakłócania możliwości sprawnego funkcjonowania państwa. Działalność tych organizacji służy celom propagandowym, często jest też szeroko nagłaśniana na prowadzonych przez tego typu zespoły kanałach społecznościowych. Widoczny wzrost poziomu zagrożeń i incydentów

[8] CSIRT GOV (2023). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2023 roku*. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp 14.10.2024].

cyberprzestrzeni RP, które mogą prowadzić do działań o charakterze terrorystycznym, podyktowany jest przede wszystkim sytuacją w Ukrainie. Efektem tego jest wprowadzenie w 2022 roku pierwotnie stopnia alarmowego ALFA-CRP, a następnie stopnia CHARLIE-CRP (obowiązuje w 2024 roku)[9].

Mając na względzie predykcję cyberzagrożeń, cyberataki w obszarze bezpieczeństwa RP będą stale przybierać na sile. Należy pamiętać, że trwający konflikt zbrojny w Ukrainie i związana z nim obecna sytuacja geopolityczna, będzie pogłębiać liczbę cyberataków. Podsumowując skalę i rodzaje zagrożeń wykrytych w przeciągu ostatnich dwóch lat, należy przyjąć, iż ich zaawansowany poziom podlega dalszej intensywności w zakresie np. kampanii socjotechnicznych. Większe zagrożenie najprawdopodobniej będzie dotyczyć także ataków na poczty elektroniczne z uwagi na ich powszechne użycie. Zagrożenia te wymagają w rezultacie konieczności realizacji działań prewencyjnych w zakresie stałego monitorowania bezpieczeństwa infrastruktury przez zespoły odpowiedzialne za cyberbezpieczeństwo systemów i sieci teleinformatycznych administracji rządowej oraz operatorów infrastruktury krytycznej.

Warte analizy treści poruszyła debata podczas SECURE 2024, podczas której przedstawiono sztuczną inteligencję jako kolejne narzędzie w kontekście cyberzagrożeń. Cyberbezpieczeństwo technologii wykorzystujących AI wydaje się nowym, jeszcze nie do końca zbadanym obszarem ryzyka dla bezpieczeństwa państwa; przyszłe innowacje bez wątpienia mogą wpłynąć na nowy krajobraz cyberzagrożeń[10].

Jak podaje CERT Polska (Computer Emergency Response Team), historycznie pierwszy w Polsce zespół reagowania na incydenty w internecie, 2023 rok należy uznać za rekordowy, jeśli wziąć pod uwagę skalę i rodzaj incydentów. Obraz, jaki rysuje się ze statystyk, należy uznać za mocno niepokojący. Lawinowy wzrost sytuacji niebezpiecznych w cyberprzestrzeni obrazuje poniższy wykres[11].

Należy jednak zauważyć, że wzrastająca liczba zgłoszeń incydentów to także efekt działań promocyjnych i uruchomienia nowego, bezpłatnego numeru 8080 do zgłaszania podejrzanych wiadomości SMS. Dzięki takim działaniom rośnie wśród społeczeństwa świadomość dotycząca cyberzagrożeń, w rezultacie rośnie też liczba zgłoszeń. Najlepszą bronią w walce z cyberoszustwami jest bez wątpienia właśnie wiedza w zakresie cyberprzestępstw[12].

---

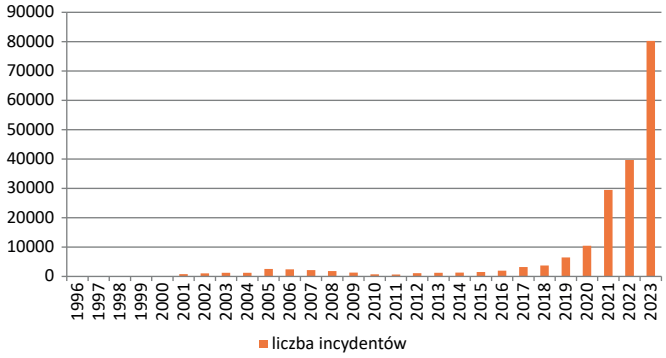
[9] ALFA-CRP to pierwszy stopień alarmowy, który można wprowadzić w przypadku uzyskania informacji o możliwości wystąpienia zdarzenia o charakterze terrorystycznym, którego rodzaj i zakres jest trudny do przewidzenia. CHARLIE-CRP to trzeci stopień alarmowy – można go wprowadzić w przypadku wystąpienia zdarzenia potwierdzającego prawdopodobny cel ataku o charakterze terrorystycznym. Ministerstwo Spraw Wewnętrznych i Administracji. *Rodzaje stopni alarmowych*. https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych [dostęp 05.05.2025].

[10] PIB NASK (2024). *SECURE 2024*. https://www.nask.pl/pl/aktualnosci/5377,SECURE-2024--wyznaczamy-horyzont-cyberbezpieczenstwa.html [dostęp 17.10.2024].

[11] CERT (2023). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2023 roku*. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp 17.10.2024].

[12] CERT (2023). *Raport bezpieczeństwa w cyberprzestrzeni w 2023 roku*. https://cert.pl/uploads/docs/Raport_CP_2023.pdf [dostęp 14.10.2024].

Wykres 1. Historyczne porównanie liczby incydentów



Źródło: Opracowanie własne na podstawie *Raportu o Stanie bezpieczeństwa Cyberprzestrzeni RP w 2023 roku*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf (dostęp 14.10.2024).

Powinno się wciąż proaktywnie poszukiwać odpowiedzi na pytanie: jak rozwiązywać kolejne nowe wyzwania, które stoją przed instytucjami publicznymi? Na pewno obserwując trendy w cyberprzestrzeni, prowadząc statystyki, skutecznie informować i ostrzegać, by zachować bezpieczeństwo państwa na stabilnym poziomie

Wyzwania dla bezpieczeństwa narodowego RP

Jednym z największych wyzwań dla bezpieczeństwa narodowego RP są ataki na jej infrastrukturę krytyczną. Obecny minister cyfryzacji Krzysztof Gawkowski podaje, że Polska jest regularnie atakowana przez cyberadwersarzy. Potwierdzają to oficjalne statystyki. Najczęściej ataki w infrastrukturę krytyczną kierowane są w tzw. miękkie podbrzusze państwa, czyli administrację rządową i samorządową[13]. Wrogie działania celowane w infrastrukturę krytyczną są niebezpieczne dla naszego państwa, dlatego w pełni muszą skupiać uwagę władz i ekspertów. Wzrost cyberzagrożeń nasila się w szczególnie w momentach ważnych i wrażliwych dla kraju i wspólnoty UE, jak np. podczas wyborów do Parlamentu Europejskiego czy szczytów unijnych. Podmiotom zewnętrznym zależy na zakłócaniu i destabilizacji takich wydarzeń na różne sposoby. Minister cyfryzacji podkreślił, że niejednokrotnie cel cyberataków jest czysto polityczny; chodzi o „doprowadzenie do przesilenia, w którym zyskiwać mają siły skrajne, mogące doprowadzić do rozbijania Unii", co jest jednym z nadrzędnych celów Kremla. Mają przyczynić się do destabilizacji państw europejskich i całego regionu. Jedną z gwarancji bezpieczeństwa państwa polskiego jest jej stabilność polityczna i obecność w NATO i UE, dlatego zwalczanie takich ataków jest niezwykle ważne.

[13] CYBERDEFENCE24 (2024). *Kolejne ataki na infrastrukturę krytyczną w Polsce*. https://CyberDefence24.pl [dostęp 15.10.2024].

Zapewnienie dostępności, integralności i poufności przetwarzanych danych w systemach teleinformatycznych zwłaszcza w administracji publicznej stanowi jeden z najważniejszych filarów bezpieczeństwa państwa polskiego. W Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 wskazano wagę zapewnienia bezpieczeństwa finansowego państwa i jego ochrony przed cyberprzestępczością. Zauważono, że coraz więcej przestępstw gospodarczych popełnianych jest w cyberprzestrzeni za pomocą nowoczesnych technologii. Podkreślono konieczność budowy systemów finansowych i bankowych w oparciu najnowszych technologiach oraz dostosowania przepisów prawa w taki sposób, by cyberhakerzy nie mieli możliwości wykorzystania luk w prawie, by uniknąć odpowiedzialności[14].

Poważnym wyzwaniem dla bezpieczeństwa narodowego Polski w przyszłości z pewnością będzie zapewnienie gwarancji swobody przepływu informacji pomiędzy poszczególnymi organami administracji publicznej i instytucjami, czyli m.in. zapewnienie bezpieczeństwa informacyjnego. Jednym z głównych cyberzagrożeń jest właśnie dezinformacja, burząca sprawną możliwość komunikacji i wymiany kluczowych informacji istotnych dla prowadzenia skutecznej polityki przez państwo.

Obecny konflikt w Ukrainie pokazuje, jak ataki na cybernetyczną infrastrukturę bezpieczeństwa państwa są niebezpieczne i jakie daleko idące konsekwencje mogą nieść za sobą. Całkowicie realnym zdaje się scenariusz zmasowanego cyberataku na systemy teleinformatyczne państwa, na co wskazuje podwyższenie wcześniej wspomnianego stopnia alarmowego w cyberprzestrzeni naszego kraju. W celu sparaliżowania działania polskiego aparatu państwowego Rosja może dokonać ataku na systemy teleinformatyczne, wywołując zamieszanie w całej przestrzeni społecznej, a nawet gospodarczej. Przewiduje sie więc, że zagwarantowanie bezpieczeństwa informacyjnego będzie jednym z największych wyzwań dla Polski[15]. Dezinformacja jako jedna z metod walki nieregularnej jest szczególnie dużym zagrożeniem połączonym z cyberprzestrzenią – za jej pomocą wróg może realizować swoje cele strategiczne, m.in. poprzez ukazywanie komfortowego dla siebie obrazu wojny (np. ukazując wojnę w Ukrainie jako operację specjalną, a nie agresję ze strony Rosji, rozmywając obraz zbrodni, jaka się tam dokonuje). Należy prowadzić skuteczne działania informacyjne dotyczące zjawiska dezinformacji, a nawet uruchomić specjalne komórki do zwalczania tego typu zjawiska, gdyż bagatelizowanie siły przekłamanej informacji funkcjonującej w przestrzeni internetowej może nieść za sobą szereg znaczących implikacji.

Innym zidentyfikowanym ryzykiem może być wykorzystywanie cyberprzestrzeni w strategii wojny hybrydowej. Biorąc pod uwagę obecną sytuacje geopolityczną, trzeba zakładać najbardziej niepojące scenariusze, m.in. cyberwojna w kontekście działań hybrydowych. Popularyzacja terminu wojny hybrydowej nastąpiła wskutek trwającego konfliktu rosyjsko-ukraińskiego, pokazując, że współczesne konflikty zbrojne

[14] P. Swoboda, A. Żebrowski (2020). *Elementy bezpieczeństwa narodowego Rzeczypospolitej Polskiej*. Wydawnictwo Avalon. Warszawa, s. 89.

[15] A.M. Dyner (2023). *Rosyjskie cyberzagrożenia dla państw NATO*. „Biuletyn PISM", 172, s. 1–2.

przybierają różne formy i znacznie odbiegają od wojen tzw. wcześniejszej generacji[16]. Obserwując współczesne konflikty można zauważyć współwystępowanie różnych elementów walki, "mieszanie" się ich; w efekcie powstaje hybryda ryzyka i różnych ataków, którą trudno przewidzieć i z którą ciężej walczyć. Tak jest dokładnie z cyberzagrożeniami. Mnogość incydentów i możliwości, jakie daje sieć, sprawia, że cyberataki świetnie wpisują się w element wojny hybrydowej. Działania niemilitarne przeplatają się z militarnymi, wspierając je i dając ostateczną przewagę w konflikcie.

Cyberwojnę można uznać za prowadzenie wojny bez jej formalnego wypowiedzenia, cel stanowić może realizacja interesów politycznych agresora, destabilizacja przeciwnika. Wykorzystanie cyberprzestrzeni w walce hybrydowej może zmaksymalizować efekt synergii z innymi działaniami niekonwencjonalnymi, takimi jak: walka psychologiczna i informacyjna czy izolacja polityczna i ekonomiczna. Współczesne konflikty występują nie tylko na płaszczyźnie terytorialnej, ale i wirtualnej, można nawet zaryzykować stwierdzenie, że przede wszystkim na tej drugiej, gdyż większość systemów obrony czy ataku znajduje się obecnie w szeroko pojmowanej sieci.

Sieć daje możliwość uniezależnienia się od ograniczeń geograficznych, prowadzone operacje mogą mieć charakter aterytorialny i niematerialny, za pomocą cyberprzestrzeni działania wymierzone przeciw jakiemuś państwu prowadzone są z dowolnego miejsca na świecie, niejednokrotnie gwarantując dużą anonimowość, dlatego cyberzagrożenia są tak niebezpieczne i trudne do wykrywania. Dla całego świata, w tym Polski, cyberprzestrzeń obok lądu, powietrza, morza, stała się kolejną przestrzenią do walki.

Polska, rozumiejąc istotę zagrożeń w cyberprzestrzeni, stworzyła szereg rekomendacji, m.in. uznając konieczność określenia ram systemu ochrony cyberprzestrzeni RP, który ma zapewnić ochronę interesu narodowego, akcentując przy tym ponadgraniczny charakter zagrożeń. Tworzone systemy mają dynamicznie dostosowywać się do zmieniających się potrzeb i wyzwań, tak więc muszą być efektywne w praktyce. Ponadto, należy precyzyjnie zdefiniować obowiązki poszczególnych elementów w mechanizmie ochrony cyberprzestrzeni, by obrona była spójna i wzajemnie sie uzupełniała. Dla efektywnego przeciwdziałania zagrożeniom należy uwzględniać i maksymalnie wykorzystywać zdobyte doświadczenie, istniejące dokonania i potencjał w dziedzinie cyberbezpieczeństwa, a w odpowiednich sytuacjach również doświadczenia innych krajów. Bezwzględnie powinno dążyć się do zapewnienia i przeznaczenia odpowiednich zasobów (finansowych, technicznych, osobowych) w celu należytej realizacji zadań służących cybernetycznej ochronie państwa[17]. Ze względu na obecną sytuację geopolityczną, autor artykułu koncentruje się na analizie wykorzystania cyberprzestrzeni przez Federację Rosyjską w trwającym konflikcie rosyjsko-ukraińskim.

---

[16] F. Bryjka (2015). *Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej*. W: T. Grabińska, Z. Kuźniar (red.). *Bezpieczeństwo personalne a bezpieczeństwo strukturalne III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego.* Wydawnictwo WSO WL. Wrocław, s. 115–131.

[17] CERT (2023). *Raport roczny z działalności CERT Polska w 2023 roku.* https://nask.pl/magazyn/raport-roczny-z-dzialalnosci-cert-polska-w-2023-roku-2 [dostęp 17.10.2024].

Rodzaje cyberzagrożeń

Niezaprzeczalnie współczesne społeczeństwo coraz bardziej staje się zależne od rozwoju technologii cyfrowych. Im większy dostęp, tym szybciej równolegle rozwijają sie narzędzia i metody cyberprzestępców. Co niepokojące, cyberprzemoc dotyczy już nie administracji, dużych firm czy instytucji, ale na to zagrożenie narażone mogą być także najmniejsze firmy czy po prostu internauci. Poniżej przedstawione zostaną najczęściej występujące ataki w cyberprzestrzeni.

Phishing to niezmiennie od wielu lat najpopularniejszy typ zgłaszanego incydentu, czyli wyłudzenie danych. Metoda ta wykorzystuje błąd, naiwność lub właśnie brak świadomości użytkownika. Sprawcy posługują się metodą opartą na socjotechnice, czyli takiej która ma skłonić potencjale ofiary do określonego działania, np. przez kliknięcie w dany link i podanie swoich danych wrażliwych. Najpopularniejszymi kampaniami phishingowymi były m.in. te wykorzystujące wizerunek serwisu aukcyjnego Allegro, społecznościowego Facebook czy sprzedażowego OLX.

Oszustwa komputerowe to kolejny popularny typ incydentów. Wśród nich można wyróżnić m.in. fałszywe sklepy internetowe, oszustwa finansowe, podawanie się za różnego rodzaju koncerny paliwowo-energetyczne.

Kolejnym szeroko występującym cyberzagrożeniem jest szkodliwe oprogramowanie, obejmuje ono infekcje całych systemów czy szkodliwe kampanie spamowe. Złośliwe oprogramowanie szyfrujące ważne pliki na komputerze ofiary ma doprowadzić do zgarnięcia pieniędzy m.in. poprzez żądanie okupu w zamian za ich odblokowanie. Jest to bardzo opłacalny atak dla cyberprzestępców, sprowadzający się często do szantażu firm i użytkowników.

Niezwykle uciążliwe i niebezpieczne są ataki DDoS (Distributed Denial of Service) polegające na przeciążaniu zasobów systemowych m.in. serwerów, sieci za pomocą ogromnej liczby zapytań i ruchu z wielu komputerów[18]. Konsekwencją tego działania jest zablokowanie dostępu do usług i stron internetowych. Często takie ataki przeprowadzane są na witryny rządowe i wiążą się z utratą własności intelektualnej i koniecznością odzyskiwania danych. Działania związane z przywracaniem danych wrażliwych są bardzo kosztowne.

Prognozuje się, że hakerzy będą sięgać po coraz nowsze techniki ataku lub też rozpoczną modyfikację aktualnie stosowanych metod. Według ENISA (Agencja Unii Europejskiej ds. Cyberbezpieczeństwa) w niedalekiej przyszłości, czyli do 2030 roku, do najbardziej istotnych cyberzagrożeń będą się zaliczać:

- ataki złośliwego oprogramowania łańcuchu dostaw,
- zaawansowane kampanie dezinformacyjne,
- utrata prywatności w cyberprzestrzeni inwigilacja cyfrowa,
- zużytkowanie starszych systemów w ekosystemach cyberfizycznych, błędy ludzkie,
- ataki z wykorzystaniem danych pochodzących z inteligentnych urządzeń,

[18] Cyfrowa Polska (2023). *Raport cyberbezpieczeństwo urządzeń końcowych*. https://cyfrowapolska.org/wp-content/uploads/2023/09/Raport_Cyberbezpieczenstwo-urzadzen-koncowych_2023.pdf [dostęp 17.10.2024].

- zagrożenia dla infrastruktury kosmicznej przez brak właściwych zabezpieczeń,
- stworzenie zaawansowanych zagrożeń hybrydowych pomiędzy światem online i offline,
- ataki hakerskie na organizacje, braku umiejętności i kompetencji w ich odpieraniu,
- cyberataki na dostawy transgraniczne skutkujące niedostępnością infrastruktury krytycznej,
- nadużywanie i nieumiejętne wykorzystywanie sztucznej inteligencji i manipulowanie algorytmami AI[19].

Analizując kwestie cyberzagrożeń nie sposób nie dotknąć pojęcia cyberterroryzmu jako świadomego, pozaprawnego i zaplanowanego działania; takie ataki mogą być prowadzone przez konspiratorskich agentów. Celem cyberterroryzmu jest wywołanie paniki, paraliżu społecznego, strachu, niepokoju przez działania o destruktywnym charakterze, m.in. poprzez blokadę działania systemów zinformatyzowanych, które mogą wywoływać katastrofy transportowe, doprowadzając do ofiar śmiertelnych[20]. Przy pomocy narzędzi teleinformatycznych cyberterroryści dążą do osiągnięcia konkretnych celów, często politycznych, co łatwiej osiągnąć przez kontrolowane i zastraszone społeczeństwo.

Podsumowując rozważania na temat obecnych i przyszłych cyberzagrożeń, zauważyć można ich znaczący wzrost w obszarze cybeprzestrzeni, dlatego tak ważnym jest osiągnięcie możliwie wysokiego poziomu cyberbezpieczeństwa poprzez skoordynowane wysiłki państwa.

Implikacje dla bezpieczeństwa państwa polskiego związane z naruszeniem cyberbezpieczeństwa RP

Niepodważalne jest, że rozwój cyberświata to nie tylko ułatwienie codziennego życia, rozwój technologii nie skutkuje jedynie powstawaniem „idealnego" świata bez granic, cyberprzestrzeń to także źródło wielu zagrożeń. Poczucie anonimowości w sieci sprzyja naruszeniom barier między działaniami zgodnymi z prawem a bezprawnymi, granice w świecie wirtualnym zacierają się bardzo łatwo, a przekonanie o bezkarności sprzyja rozwojowi cyberprzestępczości. Prawodawstwo polskie nie posiada jednej definicji tego pojęcia, jednak posiadają one część wspólną określającą cyberprzestępstwo jako przestępstwo spowodowane użyciem internetu i komputera. Podkreślić należy, że cyberprzestępstwa stanowią część cyberkonfliktów, które to dzielą się na aktywizm (czynności wspierające kampanie za pomocą internetu), cyberterroryzm i haktywizm[21], i mają negatywny wpływ na bezpieczeństwo RP. Wszystkie te aktywności to przemyślane i zaplanowane działanie przy użyciu systemu informacyjnego i sieci

[19] ENISA (2023). *Foresight Cybersecurity Threats for 2030 – raport ENISA – Cyberpolicy NASK*. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030 [dostęp 17.10.2024].

[20] K. Przestrzelska (2022). *Security in Cyberspace*. https://sbn.wat.edu.pl/pdf-151907-92591?filename=BEZPIECZENSTWO%20W.pdf [dostęp 17.10.2024].

[21] K. Liedel, P. Piasecka (2011). *Wojna cybernetyczna – wyzwanie XXI wieku*. Wydawnictwo Difin. Warszawa, s. 17.

komputerowej mające na celu destabilizację i osłabienie państwa polskiego. Może ono uderzać w pojedynczych użytkowników, administrację rządową czy infrastrukturę krytyczną, powodując poważne szkody materialne i osłabienie wizerunku Polski na arenie międzynarodowej; niebagatelne skutki to pozbawienie życia i zniszczenie infrastruktury gospodarczej. Przemoc stosowana wobec ludzi to kluczowa cecha cybernetycznych aktów, tak jak i wyrządzenie zniszczeń w celu wywołania poczucia strachu, np. przez zablokowanie e-bankowości, wywołanie katastrof transportowych.

Można stwierdzić, że cyberzagrożenie to jedno z głównych niebezpieczeństw dla świata w XXI wieku, gdyż wpływa na wszystkie systemy – społeczny, polityczny i gospodarczy – państwa. To co czyni cyberzagrożenia tak niebezpiecznymi to fakt, że jest to stosunkowo nowe zjawisko, a jednocześnie rozwijające się bardzo szybko jako forma przestępczości transgranicznej. Niezależnie od tego, czy ataki mają motyw polityczny, religijny czy społeczny, mogą przybrać charakter o zagrożeniu globalnym.

Dodatkowo postępująca globalizacja, w której dzielenie się informacją i danymi jest coraz bardziej powszechne, przyczynia się do rozprzestrzeniania się zagrożeń w cyberprzestrzeni[22]. Współczesne bezpieczeństwo ma charakter zintegrowany, brak stabilizacji w jednym państwie automatycznie ma swoje reperkusje w pozostałych. Obecna niestabilna sytuacja, np. polityczna, w naszym regionie wpływa bardzo negatywnie na środowisko bezpieczeństwa w państwie.

Cybernetyczne złowrogie ataki przenoszą spory międzynarodowe na inną płaszczyznę, a szkody cyberprzestępczości sięgają wielorakich gałęzi, na których oparte jest prawidłowe funkcjonowanie państwa. Cyberataki destrukcyjnie wpływają na kontakty między państwami, dlatego znaczenie bezpieczeństwa informacyjnego jest priorytetem dla utrzymania prawidłowego poziomu bezpieczeństwa narodowego.

Jednym z głównych elementów bezpieczeństwa narodowego jest ochrona infrastruktury krytycznej, gdyż jest ona niezbędna do prawidłowego funkcjonowania państwa i jego rozwoju gospodarczego. Popyt na wodę, energię, surowce energetyczne, paliwa, łączność, ochrona zdrowia to obszary, które są szczególnie narażone na cyberataki, ale przeniesienie ich w sferę cyberprzesterzni było nieuniknione i już się dokonało. W przypadku uszkodzenia sieci któregoś z elementów tej infrastruktury może nastąpić efekt domina, prowadząc do załamania bezpieczeństwa państwa.

Walka z zagrożeniami cybernetycznymi będzie coraz bardziej wymagająca. Cyberterroryzm, cyberprzestępczość to problemy, które będą dynamicznie rosnąć; cyberataki zmusiły państwa do budowy nowego rodzaju działań związanych z cyberbezpieczeństwem. Cel ten spełnia m.in. Strategia Cyberbezpieczeństwa RP na lata 2019–2024, która określa strategiczne cele, środki polityczne i regulacje mające na celu uodpornienie systemu informacyjnego czy operatorów infrastruktury krytycznej na cyberzagrożenia, by zwiększyć poziom bezpieczeństwa narodowego w sektorze publicznym, militarnym i prywatnym[23]. Jednym z ważnych celów szczegółowych strategii jest budowanie silnej

[22] ABW (2023). *Konkurs Szefa ABW*. https://www.abw.gov.pl/ftp/foto/Wydawnictwo/PBW/pbw27/19__przeglad_prac_konkursowych_-_S__Woszek [dostęp 18.10.2024].

[23] Ministerstwo Cyfryzacji (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 [dostęp 18.10.2024].

pozycji RP w obszarze cyberbezpieczeństwa jako kompetentnego i silnego partnera w walce z cyberatakami.

Jednym z narzędzi podnoszenia odporności państwa na cyberzgrożenia jest tworzenie aktów o cyberbezpieczeństwie, które wprowadzają certyfikacje produktów i usług w sieci komputerowej (m.in. powołanie Krajowego Organu ds. Certyfikacji Cyberbezpieczeństwa – KOCC)[24]. Należy dążyć do osiągnięcia pełnego spektrum działań przeciw cyberzagrożeniom przy zachowaniu „suwerenności cyfrowej". Muszą współistnieć z partycypowaniem w nich obywateli, którzy są świadomi i edukowani w kierunku bezpiecznego korzystania z cybeprzestrzeni. W tym celu na początku sierpnia 2024 roku powstała nowa usługa w aplikacji mObywatel o nazwie „Bezpiecznie w sieci"[25]. Dzięki niej każdy użytkownik będzie mógł jeszcze szybciej zgłosić oszustwo w internecie, w prosty sposób nielegalne treści będą odnalezione i unieszkodliwione. Zgłoszeniami zajmować się będzie specjalny zespół reagowania.

Dyskusja i wnioski

Obecna rzeczywistość połączona jest z powszechnym korzystaniem z internetu. Przyszłość opierać się będzie w głównej mierze na zasobach cyfrowych.

Trudno jest wyobrazić sobie funkcjonowanie bez serwisów, portali, usług komunikacyjnych, stron internetowych czy instytucji działających *online* i e-bankowości. Drastyczny wzrost technologii sprawił, że cyberprzestrzeń jest wręcz niemożliwa do odpowiedniego zabezpieczenia. Specjaliści ds. hakingu z łatwością są w stanie odnajdywać luki w systemach, czego skutkiem jest pozaprawne przechwytywanie danych. Poczucie bezpieczeństwa w cyberprzestrzeni jest niezwykle trudnym zadaniem, m.in. dlatego że sprawcy są niemal niemożliwi do zidentyfikowania. Ich poczucie bezkarności sprawia, że coraz więcej osób śmielej działa na granicy prawa lub łamie to prawo w cyberprzestrzeni.

Zapewnienie właściwego poziomu wiedzy użytkowników oraz administratorów, właściwe zabezpieczenie zasobów i utrzymywanie kopii zapasowych własnych danych to niezbędne działania, które pozwalają na ograniczenie skutków ataków bądź ich wyeliminowanie.

Rozwijające się środowisko cyberprzestrzeni stanowi idealne dla hakerów i przestępców miejsce. Cyberprzestrzeń jest również źródłem wielu zagrożeń dla bezpieczeństwa zewnętrznego i wewnętrznego państwa. Biorąc pod uwagę skalę problemu związaną z cyberatakimi, przeciwdziałanie takim zagrożeniom jest priorytetem. Celem zwiększenia bezpieczeństwa w cyberprzestrzeni Polska powinna zwiększyć nacisk na podstawowe zasady bezpiecznego korzystania z sieci i stale uświadamiać społeczeństwo w kwestii zagrożeń występujących w sieci. Szkolenie większej liczby specjalistów

[24] PIB NASK (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. https://cyberpolicy.nask.pl/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024/ [dostęp 18.10.2024].

[25] Ministerstwo Cyfryzacji (2024). *Bezpiecznie w sieci – nowa usługa do walki z cyberzagrożeniami dostępna w mObywatelu*. https://www.gov.pl/web/baza-wiedzy/bezpiecznie-w-sieci--nowa-usluga-do-walki-z-cyberzagrozeniami-dostepna-w-mobywatelu [dostęp 18.10.2024].

zajmujących się bezpieczeństwem teleinformatycznym jest priorytetem, ponieważ to oni będą w stanie rozpoznawać nowe rodzaje zagrożeń i z nimi walczyć. Warto również zadbać o ochronę kluczowych systemów teleinformatycznych oraz przeprowadzać ćwiczenia sprawdzające trwałość i odporność infrastruktury na ataki cybernetyczne. Z uwagi na globalny charakter sieci niezbędne jest stworzenie dokumentu regulującego aspekty prawne cyberbezpieczeństwa na całym świecie w myśl zasady *need to share*, nie zaś *need to know*, który ujednoliciłby sposoby zapobiegania, reagowania i wiele innych kwestii związanych z zagrożeniami w cyberprzestrzeni w taki sposób, aby wszystkie kraje respektujące regulacje były w stanie współpracować i prowadzić aktywną politykę przeciwko tego typu zagrożeniom w przyszłości. Działania, które mają na celu zapewnienie bezpieczeństwa w cyberprzestrzeni, muszą być redefiniowane i aktualizowane, tak by państwo zawsze było w stanie zapobiec zagrożeniom bądź – w razie ich wystąpienia – przeciwdziałać im.

Zasadnym jest przeanalizowanie strategii cyberbezpieczeństwa oraz skuteczne praktyki w obszarze zwalczania zagrożeń. Stąd również ważna jest edukacja użytkowników, która – sądząc po danych CERT NASK dotyczących zgłoszeń incydentów – przynosi już pozytywne skutki (wzrost zgłoszeń o 178%), choć jeszcze nadal stanowi znaczne wyzwanie. Zwłaszcza że zawsze to człowiek stanowi najsłabsze ogniwo w procesie cyberochrony. Potrzebne są zatem działania edukujące[26], w tym treści kształcenia np. przedmiotu edukacja dla bezpieczeństwa[27].

Ochrona cyberprzestrzeni i infrastruktury krytycznej musi być priorytetem administracji państwowej i wpływać na zacieśnienie współpracy z branżą technologiczną. Warto mieć na uwadze istotę wspólnych wysiłków w ramach zapobiegania, reagowania, ale także odbudowy po atakach cybernetycznych. Szczególną rolę przypisać można organizacjom międzynarodowym, jak np. NATO czy UE, dla których cyberprzestrzeń jest priorytetem i stanowi kolejną domenę operacyjną w prowadzeniu walki o wpływy na arenie międzynarodowej.

Bibliografia

ABW (2023). *Konkurs Szefa ABW*. https://www.abw.gov.pl/ftp/foto/Wydawnictwo/PBW/pbw27/19__przeglad_prac_konkursowych_-_S__Woszek [dostęp 18.10.2024].

Banasiński C. (red.). (2018). *Cyberbezpieczeństwo. Zarys wykładu.* Wydawnictwo Wolters Kluwer Polska. Warszawa.

Bryjka F. (2015). Cyberprzestrzeń w strategii wojny hybrydowej Federacji Rosyjskiej. W: T. Grabińska, Z. Kuźniar (red.). *Bezpieczeństwo personalne a bezpieczeństwo strukturalne III. Czynniki antropologiczne i społeczne bezpieczeństwa personalnego*. Wydawnictwo WSO WL. Wrocław.

[26] I. Urych, A. Orzyłowska (2020). *Wiedza o bezpieczeństwie w praktyce pedagogicznej.* Wydawnictwo Akademii Sztuki Wojennej. Warszawa, s. 148–154.

[27] I. Urych (2019). *On Security Education in Poland. The Essence and Content of the Subject of Education*. "Scientific and Technical Journal Safety and Defense", 5(2), s. 22–27. https://doi.org/10.37105/sd.52 [dostęp 01.10.2024].

CERT (2023). *Raport bezpieczeństwa w cyberprzestrzeni w 2023 roku*. https://cert.pl/uploads/docs/Raport_CP_2023.pdf [dostęp 14.10.2024].

CERT (2023). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2023 roku*. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi [dostęp 17.10.2024].

CERT (2023). *Raport roczny z działalności CERT Polska w 2023 roku*. https://nask.pl/magazyn/raport-roczny-z-dzialalnosci-cert-polska-w-2023-roku-2 [dostęp 17.10.2024].

CSIRT GOV (2023). *Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2023 roku*. https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/980,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2023-roku.html [dostęp 14.10.2024].

CYBERDEFENCE24 (2024). *Kolejne ataki na infrastrukturę krytyczną w Polsce*. https://CyberDefence24.pl [dostęp 15.10.2024].

Cyfrowa Polska (2023). *Raport cyberbezpieczeństwo urządzeń końcowych*. https://cyfrowapolska.org/wp-content/uploads/2023/09/Raport_Cyberbezpieczenstwo-urzadzen--koncowych_2023.pdf [dostęp 17.10.2024].

Dębowski T. (red.). (2018). *Cyberbezpieczeństwo wyzwaniem XXI wieku*. Wydawnictwo ArchaeGraph. Wrocław.

Duda D. (2023). Cyberzagrożenia wyzwaniem dla państwa i społeczeństwa. W: R. Szynowski (red.). *Wybrane problemy badań bezpieczeństwa z perspektywy młodych naukowców.* Wydawnictwo Naukowe Akademii WSB. Dąbrowa Górnicza.

Dyner A.M. (2023). *Rosyjskie cyberzagrożenia dla państw NATO*. „Biuletyn PISM", 172, 1–2.

ENISA (2023). *Foresight Cybersecurity Threats for 2030 – raport ENISA – Cyberpolicy NASK*. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats--for-2030 [dostęp 17.10.2024].

Górka M. (red.). (2017). *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*. Wydawnictwo Difin. Warszawa.

Liedel K., Piasecka P. (2011). *Wojna cybernetyczna – wyzwanie XXI wieku*. Wydawnictwo Difin. Warszawa.

Ministerstwo Cyfryzacji (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa--rzeczypospolitej-polskiej-na-lata-2019–2024 [dostęp 18.10.2024].

Ministerstwo Cyfryzacji (2024). *Bezpiecznie w sieci – nowa usługa do walki z cyberzagrożeniami dostępna w mObywatelu*. https://www.gov.pl/web/baza-wiedzy/bezpiecznie-w--sieci--nowa-usluga-do-walki-z-cyberzagrozeniami-dostepna-w-mobywatelu [dostęp 18.10.2024].

Ministerstwo Spraw Wewnętrznych i Administracji. *Rodzaje stopni alarmowych*, https://www.gov.pl/web/mswia/rodzaje-stopni-alarmowych [dostęp 05.05.2025].

PIB NASK (2019). *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*. https://cyberpolicy.nask.pl/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej--na-lata-2019–2024/ [dostęp 18.10.2024].

PIB NASK (2024). *SECURE 2024*. https://www.nask.pl/pl/aktualnosci/5377,SECURE-2024--wyznaczamy-horyzont-cyberbezpieczenstwa.html [dostęp 17.10.2024].

Przestrzelska K. (2022). *Security in Cyberspace*. https://sbn.wat.edu.pl/pdf-151907-92591?filename=BEZPIECZENSTWO%20W.pdf [dostęp 17.10.2024].

Swoboda P., Żebrowski A. (2020). *Elementy bezpieczeństwa narodowego Rzeczypospolitej Polskiej*. Wydawnictwo Avalon. Warszawa.

Szeligiewicz-Urban D. (red.). (2012). *Uczeń bezpieczny w cyberprzestrzeni*. Wydawnictwo Humanitas. Sosnowiec.

Urych I. (2019). *On Security Education in Poland. The Essence and Content of the Subject of Education*. "Scientific and Technical Journal Safety and Defense", 5(2). https://doi.org/10.37105/sd.52.

Urych I., Orzyłowska A. (2020). *Wiedza o bezpieczeństwie w praktyce pedagogicznej.* Wydawnictwo Akademii Sztuki Wojennej. Warszawa.