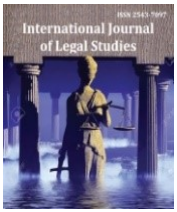

Received: 13 November 2023
Revised: 13 December 2023
Accepted: 22 December 2023
Published: 31 December 2023

THREATS TO THE FUNCTIONING OF ORGANIZATIONAL UNITS OF THE PRISON SERVICE RELATED TO NEW TECHNOLOGIES – CYBERCRIMES

ZAGROŻENIA W FUNKCJONOWANIU JEDNOSTEK ORGANIZACYJNYCH SŁUŻBY WIĘZIENNEJ ZWIĄZANE Z NOWYMI TECHNOLOGIAMI – CYBERPRZESTĘPSTWA

Mateusz Lewandowski
dr, por.; Akademia Wymiaru Sprawiedliwości
Instytut Penitencjarystyki Stosowanej, Pracownia Prawa i Porządku Publicznego
ul. Wiśniowa 50, 02-520 Warszawa, Polska
ORCID: https://orcid.org/0000-0002-5039-5528
* *Corresponding author:* e-mail: mateusz.lewandowski@aws.edu.pl

Abstract
The subject of scientific reflection in the research conducted was threats to the functioning of organizational units of the Prison Service related to new technologies - cybercrimes. A non-reactive content analysis method was used to conduct them. As a result of scientific investigations, the theoretical aspects of cybercrime and their types were presented. Cyber threats to the Ministry of Justice were diagnosed and issues regarding the penalization of acts in cyberspace under Polish law were discussed. The final effect of the research in question are recommendations.
Keywords: Prison Service, threats, cybercrime, criminalization of acts in cyberspace

Streszczenie
Przedmiotem naukowej refleksji w przeprowadzonych badaniach uczyniono zagrożenia w funkcjonowaniu jednostek organizacyjnych Służby Więziennej związane z nowymi technologiami - cyberprzestępstwa. Do ich przeprowadzenia wykorzystano niereaktywną metodę analizy treści. W wyniku naukowych dociekań przybliżono teoretyczne aspekty cyberprzestępczości i ich rodzaje. Zdiagnozowano cyberzagrożenia dla resortu wymiaru sprawiedliwości oraz omówiono kwestie dotyczące penalizacji czynów w cyberprzestrzeni na gruncie polskiego prawa. Efekt finalny przedmiotowych badań stanowią rekomendacje.
Słowa kluczowe: Służba Więzienna, zagrożenia, cyberprzestępczość, penalizacja czynów w cyberprzestrzeni

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

Główny zarys problemu i jego związku z ważnymi kwestiami naukowymi i praktycznymi

Współczesne społeczeństwa podlegają wielokierunkowym, przyspieszonym zmianom, które nazywa się postmodernizmem, trzecią falą, globalną transformacją, społeczeństwem informacyjnym, społeczeństwem sieci lub społeczeństwem ryzyka [1]. Zdaniem autora niniejszego opracowania dorobek oraz kierunek rozwoju nauk o bezpieczeństwie wskazują na największą zasadność stosowania ostatniego z wymienionych określeń. Współcześnie stwierdza się bowiem zwielokrotnienie liczby zagrożeń dla podmiotów bezpieczeństwa oraz wzrost ryzyka ich wystąpienia, a przecież bezpieczeństwo w wąsko rozumianym ujęciu (tzw. definicja negatywna/antonimiczna) zawężającym bezpieczeństwo do antonimów wobec zagrożeń [2] to *brak zagrożenia fizycznego albo ochrona przed nim, ochrona przed niebezpieczeństwami i pewność rozwoju* [3]. W XXI w. bezpieczeństwo przedmiotowe odnosi się do różnorodnych aspektów funkcjonowania podmiotów, a nie wyłącznie do aspektu militarnego, jak to miało miejsce w naukach wojskowych [4], z których wywodzą się nauki o bezpieczeństwie [5]. Przemiana w myśleniu o bezpieczeństwie zapoczątkowana w latach 80. XX w. przez Barrego Buzzana [6] i kontynuowana przez innych przedstawicieli szkoły kopenhaskiej jest implikacją zmian zachodzących w środowisku bezpieczeństwa podmiotów państwowych – pojawienia się nowych zagrożeń. Przedstawiciele szkoły kopenhaskiej dostrzegli znaczenie zagrożeń politycznych, ekonomicznych, społecznych oraz ekologicznych i wymieniali je na równi z zagrożeniami militarnymi. Koncepcja sektorów bezpieczeństwa Barrego Buzzana na przestrzeni lat ewoluowała, wskazane przez niego sektory nie stanowią katalogu zamkniętego. Współcześnie za sprawą pojawienia się nowych zagrożeń przedmiotem bezpieczeństwa czyni się również inne obszary działalności ludzkiej [7]. Reasumując zatem współczesna ekspansja ryzyka i kumulacji różnorodnych zagrożeń skłania do przyjęcia za Ulrichem Beckiem tezy, iż współczesne społeczeństwo jest w istocie społeczeństwem ryzyka [8]. Według niego społeczeństwa industrialne koncentrowały się w swoich wysiłkach na zdobywaniu i dystrybucji bogactwa. Społeczeństwa współczesne to społeczeństwa nie dystrybucji bogactwa, lecz ryzyka. Społeczeństwo ryzyka oznacza epokę, w której negatywne skutki i konsekwencje rozwoju i postępu technicznego zdominowały społeczną debatę, wyróżniając cztery rodzaje ryzyka [9]: 1) ryzyko ekologiczne; 2) ryzyko związane ze zdrowiem; 3) ryzyko ekonomiczne; 4) ryzyko społeczne.

W XXI wieku w debacie publicznej przeważa tematyka nowoczesnych technologii, w tym innowacyjnych rozwiązań poprawiających jakość życia człowieka, ale również cyberprzestępstw, które wpływają na funkcjonowanie całego społeczeństwa,

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

w odniesieniu do wszystkich rodzajów ryzyka zaproponowanych przez Ulricha Becka. Za sprawą cyberprzestępczości traci jednostka, grupy społeczne, instytucje, przedsiębiorstwa, organizacje sektora prywatnego i publicznego. Cyberprzestępczość uderza w gospodarkę. W rankingu Interpolu przestępczość internetowa wyprzedziła pod względem dochodowości handel narkotykami [10]. Zainteresowanie społeczeństwa cyberbezpieczeństwem znajduje również odzwierciedlenie w licznych badaniach naukowych [11]. Celem przeprowadzonej analizy literatury przedmiotu oraz aktów prawnych było włączenie się do dyskursu naukowego dot. cyberbezpieczeństwa poprzez sformułowanie i dostarczenie argumentacji przyczyniającej się do rozpoznania zagrożeń w funkcjonowaniu jednostek organizacyjnych Służby Więziennej (dalej jako: SW) związanych z nowymi technologiami. Dostrzega się bowiem pewną lukę poznawczą w kwestiach dotyczących cyberprzestępczości w kontekście funkcjonowania więziennictwa w Polsce.

Analiza najnowszych badań, aktów prawnych i literatury przedmiotu, w których podjęto omówienie podjętej problematyki

W obszarze zakreślonym tematem badaniami nad zagrożeniami związanymi z nowymi technologiami zajmowali się tacy naukowcy, jak: U. Beck (Beck U. 2002), A.A. Abd El-Latif, B. Abd El-Atty, I. Mehmood, K. Muhammad, S.E. Venegas-Andraca, J. Peng (Abd El-Latif A.A., Abd El-Atty B., Mehmood I., Muhammad K., Venegas-Andraca S.E., Peng J. 2021), K. Kim, J.S. Kim, S. Jeong, J.H. Park, H.K. Kim (Kim K., Kim J.S., Jeong S., Park J.H., Kim H.K. 2021), K.F. Cheung, M.G.H. Bell, J. Bhattacharjya (Cheung K.F., Bell M.G.H., Bhattacharjya J. 2021), D.E. Sanger (Sanger D.E. 2021), M. Conway (Conway M. 2003), D.E. Denning (Denning D.E. 2002), B. Bencsath, G. Pek, L. Buttyan, M. Felegyhazi (Bencsath B., Pek G., Buttyan L., Felegyhazi M. 2012). Zaś na gruncie krajowym wskazać należy: P. Sienkiewicza (Sienkiewicz P. 2019), S. Gwoździewicz, (Gwoździewicz S., Prokopowicz D. 2022), M. Siwickiego (Siwicki M. 2012), J. Kowalewskego, M. Kowalewskiego (Kowalewski J., Kowalewski M. 2014), J. Kosińskiego (Kosiński J. 2015), R. Białoskórskiego (Białoskórski R. 2011), D. Siemieniecką, M. Skibińską, K. Majewską (Siemieniecka D., Skibińska M., Majewska K. 2020), A. Bógdał-Brzezińską, M.F. Gawryckiego (Bógdał-Brzezińska A., Gawrycki M.F. 2003), T. Hoffmanna (Hoffmann T. 2018), S. Wojciechowską-Filipek, Z. Ciekanowskiego (Wojciechowska-Filipek S., Ciekanowski Z. 2016), A. Naruszewicz-Duchlińską (Naruszewicz-Duchlińska A. 2015), N. Andraszak (Andraszak N. 2021), C. Banasińskiego, M. Rojszczak (Banasiński C., Rojszczak M. 2020), E. Lichockiego (Lichocki E. 2009) K. Ciglic, M. Jurczyk, A. Konkel, I. Lewandowską-Wiśniewską,

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

D. Mikołajczyk, K. Podwińskiego, L. Rozenblum, J. Sordyl, M. Spychałę, Y. (Itzik) Vager, R. Żelechowskiego, D. Skokowskiego (Ciglic K., Jurczyk M., Konkel A., Lewandowska-Wiśniewska I., Mikołajczyk D., Podwiński K., Rozenblum L., Sordyl J., Spychała M., Vager Y. (Itzik), Żelechowski R., Skokowski D. 2017).

Cele i metody badawcze podjęte w analizie tematu

Celem przeprowadzonej analizy było włączenie się do dyskursu naukowego dot. cyberbezpieczeństwa poprzez sformułowanie i dostarczenie argumentacji przyczyniającej się do rozpoznania zagrożeń w funkcjonowaniu jednostek organizacyjnych Służby Więziennej związanych z nowymi technologiami. Dostrzega się bowiem pewną lukę poznawczą w kwestiach dotyczących cyberprzestępczości w kontekście funkcjonowania więziennictwa w Polsce. Do przygotowania niniejszego opracowania wykorzystano: akty prawne i literaturę przedmiotu wskazującą na występowanie zagrożeń w funkcjonowaniu jednostek organizacyjnych Służby Więziennej związanych z nowymi technologiami. Analizowane dokumenty określić można jako pisane (literatura przedmiotu), cyfrowe (materiały i opracowania statystyczne) i zastane (pierwotnie powstałe dla celów pozanaukowych), ale też oficjalne (usankcjonowane, o charakterze państwowym, urzędowym). Poddana analizie literatura dotyczyła: teoretycznych aspektów cyberprzestępczości, rodzajów cyberprzestępczości, cyberzagrożeń dla resortu wymiaru sprawiedliwości oraz penalizacji czynów w cyberprzestrzeni na gruncie polskiego prawa.

Prezentacja przeprowadzonej analizy. Dyskusja

Teoretyczne aspekty cyberprzestępczości

Przestępstwa z wykorzystaniem nowych technologii są źródłem zamieszania terminologicznego. Oprócz określenia *cyberprzestępstwo* w literaturze naukowej używa się zamiennie również: *przestępstwa internetowe*, *przestępstwa związane z technologią cyfrową*, *przestępstwa związane z technologią przetwarzania informacji*, *przestępstwa sieciowe*, *przestępstwa wirtualne*, *przestępstwa elektroniczne*, *przestępstwa związane z nowoczesnymi technologiami*, *e-przestępstwa*, czy *przestępstwa informacyjne* [12]. Na potrzeby niniejszego opracowania przyjęto definicję cyberprzestępstwa zaproponowaną przez Jakuba i Mariana Kowalewskich. Według nich cyberprzestępstwo to *wszelkiego rodzaju czyny zabronione, które zostały popełnione w cyberprzestrzeni* [13]. Posiadają one specyficzne cechy [14]:

- komputer, sieć komputerowa, urządzenie teleinformatyczne jest przedmiotem, środkiem lub celem zamachu;

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

- łatwa w obsłudze, ale zaawansowana technologia wykorzystywana przez przestępców;
- anonimowość sprawcy;
- traktowanie przez społeczeństwo przestępcy komputerowego jako człowieka nieszkodliwego;
- ofiara często nie jest świadoma, że jej system został zaatakowany;
- rzadko składane są zawiadomienia o popełnieniu przestępstwa, chyba że doszło do znacznych strat finansowych;
- krótki czas potrzebny do popełnienia przestępstwa;
- niskie koszty, duże korzyści;
- zorganizowanie i specjalizacja, często działanie na zlecenie;
- międzynarodowy zasięg, transgraniczność;
- asymetryczność zagrożeń.

Cyberprzestępczość jest zjawiskiem powszechnym, w skali roku wśród firm prowadzących działalność w Polsce przynamniej jeden incydent cyberbezpieczeństwa odnotowuje ponad połowa organizacji [15]. W 2020 r. zarejestrowano w skali kraju 10 420 cyberincydentów [16], a jak podaje Najwyższa Izba Kontroli, nieznana jest ilość i skala ataków, w przypadku których nie ujawniono informacji o ich skutecznym przeprowadzeniu [17].

Rodzaje cyberprzestępczości

Autor niniejszego opracowania zgadza się ze stwierdzeniem Roberta Białoskórskiego, iż zasadnicza trudność badawcza w obszarze cyberbezpieczeństwa wynika z braku jednolitego i powszechnie uznanego aparatu pojęciowego poszczególnych rodzajów zagrożeń w cyberprzestrzeni [18]. Na potrzeby przeprowadzonej analizy autor przyjął za Dorotą Siemieniacką, Małgorzatą Skibińską i Kamilą Majewską podział cyberprzestępstw na: szpiegostwo, cyberterroryzm, cyberagresję i hakerstwo [19].

Cyberszpiegostwo jest to *zdobywanie informacji i materiałów wywiadowczych, czyli takich, które stanowią istotną wartość z punktu widzenia zadań wywiadowczych realizowanych przez daną służbę wywiadowczą znajdujących się w cyberprzestrzeni w dyspozycji jakiegokolwiek podmiotu pozostającego w zainteresowaniu wywiadowczym z wykorzystaniem różnorodnych metod i technik wywiadowczych, w szczególności cybernetycznych* [20]. Cyberszpiegostwo za sprawą dużej dostępności, niskich kosztów oraz trudności w wykrywaniu jest zjawiskiem powszechnym. Szczególnie zaangażowane w tego typu działalność są mocarstwa światowe takie jak: Stany Zjednoczone Ameryki, Federacja Rosyjska, czy Chińska Republika Ludowa [21].

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

Uznaje się, że pojęcie *cyberterroryzmu* powstało w 1997 r. w Institute for Security and Intelligence w Californii, jednak cyberterroryzm był obiektem publicznego zainteresowania już w latach 80. XX w.[22]. Jego twórca Barry C. Collin zdefiniował cyberterroryzm jako *połączenie cybernetyki i terroryzmu* [23]. Na przestrzeni lat definicja cyberterroryzmu ewoluowała. Na potrzeby niniejszego opracowania autor przyjął za Dorothy E. Denning że *cyberterroryzm jest konwergencją cyberprzestrzeni i terroryzmu. Dotyczy nielegalnych ataków i gróźb ataków przeciwko komputerom, sieciom komputerowym i informacjom przechowywanym w nich, by zastraszyć lub wymusić na rządzie lub społeczeństwie polityczne lub społeczne cele* [24]. Literatura naukowa podaje, że pierwszy znany atak cyberterrorystyczny na rządowy system komunikacyjny został przeprowadzony w 1998 r. przez Tamilskie Tygrysy. Przedstawiciele tej organizacji terrorystycznej wykorzystując technikę e-mail bombing przez dwa tygodnie wysyłali do lankijskiej ambasady ponad 800 maili dziennie z wiadomością o treści *jesteśmy internetowymi Czarnymi Tygrysami i chcemy zniszczyć wasz system komunikacyjny* [25]. Współcześnie najczęstszy cel ataków cyberterrorystycznych stanowią firmy energetyczne [26]. Jeden z najbardziej spektakularnych z nich miał miejsce w grudniu 2015 r. w Ukrainie. Część państwa w wyniku cyberataku, w tym prawie połowa gospodarstw domowych w obwodzie iwano-frankowskim, została pozbawiona elektryczności. Zgodnie z doniesieniami medialnymi, w wyniku cyberataku poszkodowanych zostało około 700 tys. klientów jednego z głównych operatorów energii elektrycznej na Ukrainie [27]. W dyskursie medialnym i politycznym pojawiają się głosy o braku zagrożenia terrorystycznego dla Rzeczypospolitej Polskiej (dalej jako: RP) [28], a praktyka wskazuje, że jest to niezgodne z prawdą. W lipcu i październiku 2014 r. na terytorium RP miały miejsce cyberataki o znamionach terrorystycznych. Anonimowi nadawcy przesyłali informacje, że w ważnych instytucjach rządowych są podłożone ładunki wybuchowe. Po szczegółowym sprawdzeniu przez właściwe służby okazało się, że informacje były nieprawdziwe [29].

Cyberagresja *to forma prześladowania, do której należą: kłamstwa, plotki, zamieszczanie nieprzyjaznych i obraźliwych komentarzy, realizowanych poprzez czaty, pocztę elektroniczną, strony internetowe, a także zamieszczanie niechcianych zdjęć lub filmów* [30]. Jedną z jej szczególnie popularnych odmian jest *hejt*, czyli *obraźliwy lub agresywny komentarz zamieszczony w Internecie* [31]. Język hejtu opiera się na kategoryzacji my-oni, nienawiść ta jest ukierunkowana na dyskryminowanie grup [32]. Pojęcia cyberagresji i hejtu zyskały popularność głównie w kontekście zagrożeń dla bezpieczeństwa młodzieży szkolnej, ale coraz częściej cyberagresja jest skierowana przeciwko grupom dyspozycyjnym, w tym funkcjonariuszom SW. Szczególnie to

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

niekorzystne zjawisko uwidaczniało się w kontekście zwalczania przez funkcjonariuszy różnych służb skutków pandemii COVID-19 oraz stabilizowania sytuacji na granicy polsko-białoruskiej [33].

Hakerstwo to *poszukiwanie i wykorzystywanie dziur w oprogramowaniu komputerowym, pozwalające na uzyskanie dostępu do zabezpieczonych informacji. Są to działania zmierzające do dokonania zmian na stronach internetowych oraz kradzieży lub zniszczenia danych* [34]. Haker może np. włamać się do publicznego serwera instytucji rządowej i zmienić treść zamieszczonych na niej informacji na śmieszną lub obraźliwą. Tego typu atak kompromituje i podważa wizerunek instytucji [35]. Jednym z pierwszych znanych ataków w cyberprzestrzeni był Slammer, którym w 2003 r. zaatakowano systemy komputerowe. Był to wirus wykorzystujący lukę w oprogramowaniu SQL Serwer. W czasie 10-minutowego ataku za jego pomocą zainfekowano ok. 75 tys. komputerów na świecie [36].

Arsenał technik stosowanych przez cyberprzestępców jest znaczny, należą do nich m.in.[37]: backdoor, backdoor-santas, bakteria, bomba logiczna, bomba pocztowa, banner grabing, botnet, chipping, cookies, cracking, dialery, DoS/DDos, exploit, fastflux, hi jacking, inżynieria społeczna, keylogger, koń trojański, mobler, phishing, posyłanie numerów sekwencji TCP/IP, przepełnienie bufora, receptory van Ecka, robak, rootkit, sniffing, spoofing, spyware, stuxnet, wabbit, wirus, złośliwe programy, XSS, zero-day exploits. Powyższe techniki nie stanowią katalogu zamkniętego, cyberprzestępcy dokonują ich modyfikacji i nieustannie opracowują nowe bardziej skuteczne ich formy. W niniejszym opracowaniu techniki stosowane przez cyberprzestępców nie zostały szczegółowo omówione, ograniczono się wyłącznie do ich wskazania. Wynika to z ograniczenia co do objętości opracowania. Jest to jednak zagadnienie już dobrze rozpoznane w literaturze naukowej [38].

Cyberzagrożenia dla resortu wymiaru sprawiedliwości

W opinii autora niniejszego opracowania cyberprzestępstwa stanowią istotne zagrożenie dla prawidłowego funkcjonowania resortu wymiaru sprawiedliwości. Mogą implikować różnorodne problemy dla Ministerstwa Sprawiedliwości, Akademii Wymiaru Sprawiedliwości, Centralnego Zarządu Służby Więziennej, sądów, prokuratur czy jednostek penitencjarnych. W celu zobrazowania zagrożenia w dalszej części opracowania zostały przedstawione opisy rzeczywistych sytuacji, które miały miejsce w Polsce oraz innych państwach.

W kontekście cyberbezpieczeństwa szczególnie często obiekt ataków stanowią portale rządowe i mimo to, że są zazwyczaj dobrze chronione, to co jakiś czas do opinii publicznej przedostaje się informacja o skutecznym cyberataku. Dla przykładu w

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

styczniu 2009 r. hakerzy przełamali zabezpieczenia uznawanej za bardzo bezpieczną izraelskiej infrastruktury informatycznej. Atakiem objęto co najmniej 5 mln komputerów (w tym portale rządowe). Izrael obarczył odpowiedzialnością za atak organizacje przestępcze z terytorium byłego ZSRR, działające na zlecenie i opłacane przez Hamas lub Hezbollah [39]. Natomiast w lutym tego samego roku nieznani hakerzy za pomocą techniki DoS zaatakowali rządowe strony internetowe Stanów Zjednoczonych Ameryki i Republiki Korei [40]. Również na gruncie polskim zdarzają się cyberataki na portale rządowe. Najbardziej znane, szeroko opisywane w mediach i literaturze specjalistycznej to te z 2012 r., kiedy to najważniejsze strony administracji publicznej w domenie gov.pl stały się częścią kampanii protestu społecznego związanej z przygotowaniami do podpisania przez Polskę międzynarodowego porozumienia dotyczącego walki z naruszaniem własności intelektualnej ACTA. Między innymi celem ataku była strona internetowa Ministerstwa Sprawiedliwości. Działania hakerów były wówczas ukierunkowane na przeciążenie serwerów udostępniających strony www tych instytucji [41]. Bardzo medialne były również wycieki danych z adresu mailowego ministra Michała Dworczyka oraz wyciek danych (imiona i nazwiska, pesele, adresy miejsc pełnienia służby) ok. 20 tys. funkcjonariuszy m.in. Policji, Straży Granicznej, Służby Więziennej, czy Państwowej Straży Pożarnej [42].

Przykłady z Polski oraz innych państw wskazują na to, że potencjalny cel ataku cybernetycznego może stanowić Akademia Wymiaru Sprawiedliwości oraz ośrodki szkolenia i doskonalenia kadr SW. W kontekście szkolnictwa wyższego celem cyberataków są bowiem zazwyczaj uczelnie, na których kształci się kadrę wojskową oraz innych służb mundurowych. Dla przykładu w listopadzie 2006 r. hakerzy spenetrowali system informatyczny jednej z amerykańskich wojskowych szkół wyższych, w wyniku czego na okres dwóch tygodni sparaliżowano jej pracę. Drugi przykład jest z maja 2007 r., kiedy to nieznani sprawcy posługując się programem szpiegostwa przemysłowego przeprowadzili cyberatak na systemy informatyczne amerykańskiego Uniwersytetu Obrony Narodowej [43]. Również w Polsce tego typu ataki zdarzały się już w przeszłości. W kwietniu 2020 r. Krajowa Szkoła Sądownictwa i Prokuratury stała się ofiarą wycieku danych. Baza danych, która została skradziona i bezprawnie ujawniona w Internecie zawierała m.in.: imiona i nazwiska, numery telefonów, adresy e-mail, adresy zamieszkania, daty pierwszego i ostatniego logowania oraz miejsca pracy sędziów i prokuratorów [44]. Z kolei w lipcu 2019 r. podczas Spotkania Ministerialnego Poświęconego Budowaniu Pokoju i Bezpieczeństwa na Bliskim Wschodzie, które miało miejsce w Warszawie celem ataku hakerów stały się witryny internetowe czterech

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

polskich instytucji, w tym Centralnego Ośrodka Szkolenia Służby Więziennej. Atak polegał na tym, że na witrynie podmieniono treści [45].
Funkcjonariusze i pracownicy SW mogą stać się ofiarami cyberprzestępstw zarówno podczas wykonywania obowiązków służbowych jak również w czasie wolnym od służby. W strukturach administracji funkcjonuje wiele systemów informatycznych, zawierających bardzo ważne informacje dla bezpieczeństwa państwa, należą do nich m.in. Krajowy Rejestr Karny i Centralna Baza Danych Osób Pozbawionych Wolności [46]. Ich prawidłowe wykorzystywanie podczas wykonywania obowiązków służbowych, ale również ostrożność podczas aktywności w czasie wolnym od służby może gwarantować bezpieczeństwo danych. Cyberszpiedzy pozyskują informacje w różnorodnych okolicznościach. Dla przykładu w 2008 r. za pomocą wirtualnie wykreowanej postaci atrakcyjnej kobiety (Reut Zukerman), prawdopodobnie libański Hezbollah pozyskiwał w sieci Internet informacje na temat danych osobowych izraelskich żołnierzy, a nawet tajne kody i opisy baz wojskowych, w których pełnili służbę. Arabska prasa podawała natomiast, że izraelskie służby wykorzystują portale Facebook i Twitter do pozyskiwania w Strefie Gazy palestyńskich informatorów [47]. Praktyka wskazuje na to, że zdarzają się również ataki na serwisy internetowe, z których korzystają funkcjonariusze różnych formacji. W Polsce w maju 2020 r. dokonano włamania do najpopularniejszego serwisu internetowego dla policjantów. Przestępcy prawdopodobnie przejęli prywatne adresy e-mail oraz hasze haseł licznych funkcjonariuszy Policji z całego kraju [48]. Drugi przykład jest z lipca 2015 r., kiedy to dokonano ataku hakerskiego na portal związków zawodowych SW. Polegał on na umieszczeniu na stronie internetowej tunezyjskiej flagi i wizerunku zamaskowanego bojownika, a także apelu o poszanowanie islamu [49]. Zdarza się także, że funkcjonariusze i pracownicy SW stają się ofiarami cyberprzestępstw wymierzonych przeciwko ogółowi społeczeństwa. W okresie przedświątecznym popularne są oszustwa dotyczące rzekomych usług kurierskich. Przestępcy za pomocą smsów z prośbami o dopłatę drobnych kwot (ok. 4-5 zł) do przesyłek kurierskich kradną dane do logowania klientów na stronę internetową banku. Po kliknięciu w link przesłany w smsie przez cyberprzestępcę użytkownik zostaje przekierowany na fałszywą stronę internetową banku, która do złudzenia przypomina oryginał. Po dokonaniu dopłaty do rzekomej usługi kurierskiej cyberprzestępcy przejmują dane do logowania przyszłej ofiary i wykorzystują je w celu dokonania kradzieży środków z jej konta bankowego [50].

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

Penalizacja czynów w cyberprzestrzeni na gruncie polskiego prawa

Cyberprzestępstwa nie zostały ujęte w jednolity sposób we współczesnych kodyfikacjach karnych. Jest to niewątpliwy problem związany z identyfikacją zagrożenia oraz wskazaniem ram odpowiedzialności karnej za podjęte działania [51].

W polskim prawie nie istnieje jedna ustawa, która regulowałaby wszelkie przepisy dotyczące cyberprzestępczości. Odnośniki do tej kwestii można znaleźć w: 1) Ustawie z dnia 6 czerwca 1997 – *Kodeks karny* [52] (dalej jako: Kodeks Karny), 2) Ustawie z dnia 10 maja 2018 r. *o ochronie danych osobowych* [53], 3) Ustawie z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* [54], 4) Ustawie z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* [55], 5) Ustawie z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* [56]. Usystematyzowanie wskazanych kwestii jest jednak zadaniem karkołomnym ze względu na dużą różnorodność przestępstw, których można dokonać z wykorzystaniem sieci Internet. Wskazują na to chociażby zapisy Kodeksu Karnego. Zagadnienia związane z przestępstwami internetowymi zostały zawarte w kilku jego rozdziałach, m.in.:

- XVII, który dotyczy przestępstw przeciwko Rzeczypospolitej Polskiej (art. 130 - szpiegostwo, art. 132 – dezinformacja);
- XX, dotyczącym przestępstw przeciwko bezpieczeństwu powszechnemu (art. 165 – inne niebezpieczeństwa, art. 167 – niebezpieczne urządzenia lub substancje);
- XXXIII, czyli przestępstwa przeciwko ochronie informacji (art. 267 – nielegalne uzyskanie informacji, art. 268 niszczenie informacji, art. 268a – szkoda w bazach danych, art. 269 – sabotaż komputerowy, art. 269a – zakłócenie pracy w sieci, art. 269b – bezprawne wykorzystanie programów i danych);
- XXXV, który przedstawia przestępstwa przeciwko mieniu (art. 278 – kradzież, art. 287 – oszustwo komputerowe, art. 288 – naruszenie integralności rzeczy, art. 293 – paserstwo komputerowe).

Wnioski

Problematyka cyberbezpieczeństwa jest bardzo istotna zarówno z poznawczego, jak i pragmatycznego punktu widzenia. Z poznawczego punktu widzenia stanowi ona nie do końca eksplorowany obszar badawczy. Permanentne zmiany zachodzące w sposobie działania cyberprzestępców determinowane pojawianiem się coraz to nowych możliwości technicznych implikują potrzebę podejmowania badań nad cyberbezpieczeństwem. Z pragmatycznego punktu widzenia wskazane jest wykorzystywanie pozyskanej w ten sposób wiedzy teoretycznej do rozwiązywania problemów

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

praktycznych. Pomimo tego, że przestępstwa z wykorzystaniem nowych technologii występują powszechnie, to są zjawiskami słabo rozpoznanymi. Wiedza na ich temat jest rozproszona, brakuje nawet konsensusu w sprawach tak podstawowych jak kwestie definicyjne i kategoryzacyjne. Przyjęty na potrzeby badań podział cyberprzestępstw na: szpiegostwo, cyberterroryzm, cyberagresją i hakerstwo jest co zaznaczono wcześniej tylko przykładowym. Te oraz inne cyberprzestępstwa niewątpliwie stanowią wyzwanie dla resortu wymiaru sprawiedliwości. Szczególne cyberzagrożenie dla resortu wymiaru sprawiedliwości stanowią ataki na portale internetowe poszczególnych jednostek organizacyjnych (w tym Akademii Wymiaru Sprawiedliwości, ośrodków szkolenia i doskonalenia kadr) Służby Więziennej, wycieki danych z adresów mailowych funkcjonariuszy i pracowników jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Sprawiedliwości, a także próby wyłudzenia od funkcjonariuszy i pracowników Służby Więziennej ważnych danych.
Przeprowadzona analiza może posłużyć lepszemu zrozumieniu specyfiki zagrożeń związanych z nowymi technologiami oraz dostarczyć argumentacji na rzecz podjęcia działań mających na celu podniesienie poziomu cyberbezpieczeństwa resortu wymiaru sprawiedliwości, w tym jednostek organizacyjnych SW. Przedstawione wnioski z analizy literatury przedmiotu oraz aktów prawnych mogą także stanowić introdukcję do bardziej pogłębionych badań jakościowych w tej materii.

Bibliografia

1. Sienkiewicz P., *Analiza systemowa zagrożeń bezpieczeństwa rozwoju społeczeństwa informacyjnego,* [w:] Jaroszyńska M., Moch N., Stochaj J. (red.), *Bezpieczeństwo narodowe Polski w erze społeczeństwa informacyjnego*, Wojskowa Akademia Techniczna, Warszawa 2019, s. 7.
2. Stańczyk J., *Formułowanie kategorii pojęciowej bezpieczeństwa*, FNCE, Poznań 2017, s. 90.
3. Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych,* [w:] Bobrow D.B., Haliżak E., Zięba R. (red.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX w*., Scholar, Warszawa 1997, s. 3.
4. Szulc B., Mazurek Z., *Podstawy tożsamości metodologicznej nauk wojskowych: praca naukowo-badawcza*, Akademia Obrony Narodowej, Warszawa 2010; Wiśniewski E., *Metodyka wojskowych badań naukowych*, Akademia Sztabu Generalnego Wojska Polskiego, Warszawa 1988; Kulińczyk B., *Współczesna nauka wojenna*, Akademia Sztabu Generalnego im. generała broni Karola Świerczewskiego, Warszawa 1973.

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

5. Gierszewski J., Pieczywok A., *Metodologiczne podstawy badania problemów bezpieczeństwa*, Difin, Warszawa 2020, s. 24.
6. Buzan B., *People, states and fear. The national security problem in international relations*, Wheatsheaf Book LTD, Brighton 1983.
7. Zięba R., *Kategoria bezpieczeństwa w nauce o stosunkach międzynarodowych,* [w:] Bobrow D.B., Haliżak E., Zięba R. (red.), *Bezpieczeństwo narodowe i międzynarodowe u schyłku XX w*., Scholar, Warszawa 1997, s. 6-7; Cieślarczyk M., *Metody i techniki badawcze stosowane w badaniach problemów bezpieczeństwa*, [w:] Czupryński A., Wiśniewski B., Zboina J. (red.), *Bezpieczeństwo. Teoria – badania – praktyka*, CNBOP-PIB, Józefów 2015, s. 59; Zając J., *Bezpieczeństwo państwa,* [w:] Wojtaszczyk K.A., Materska-Sosnowska A., *Bezpieczeństwo państwa. Wybrane problemy*, Oficyna Wydawnicza ASPRA-JR, Warszawa 2009, s. 19; Nowakowski Z., Pomykała M., Rajchel J., Rajchel K., Tokarski H., *Administracja bezpieczeństwa i porządku publicznego*, TNP, Warszawa 2009, s. 38-39; Paździor M., Szmulik B. (red.), *Instytucje bezpieczeństwa narodowego*, C.H.Beck, Warszawa 2012, s. 7.
8. Beck U., *Społeczeństwo ryzyka*, Scholar, Warszawa 2002.
9. Sienkiewicz P., *Analiza systemowa zagrożeń bezpieczeństwa rozwoju społeczeństwa informacyjnego,* [w:] Jaroszyńska M., Moch N., Stochaj J. (red.), *Bezpieczeństwo narodowe Polski w erze społeczeństwa informacyjnego*, Wojskowa Akademia Techniczna, Warszawa 2019, s. 15.
10. *Masz taki telefon? Jesteś na celowniku hakerów*, https://www.fakt.pl/facet/technologie/posiadacze-smartfonow-na-celeowniku-hakerow/jdsqewr (dostęp w dniu: 28.11.2023 r.).
11. Abd El-Latif A.A., Abd El-Atty B., Mehmood I., Muhammad K., Venegas-Andraca S.E., Peng J., *Quantum-Inspired Blockchain-Based Cybersecurity: Securing Smart Edge Utilities in IoT-Based Smart Cities*, „Information Processing and Management" 2021, no 4(58); Kim K., Kim J.S., Jeong S., Park J.H., Kim H.K., *Cybersecurity for autonomous vehicles: Review of attacks and defense*, „Computers and Security" 2021, no 103; Cheung K.F., Bell M.G.H., Bhattacharjya J., *Cybersecurity in logistics and supply chain management: An overview and future research directions*, „Transportation Research Part E: Logistics and Transportation Review" 2021, no 146; Gwoździewicz S., Prokopowicz D., *Determinants of electronic data interchange security in the context of big data and cloud computing technology development. Sentiment analysis conducted for cybercrime issues occurred in the period from may 2017 to february 2019,* „ International Journal of New Economics and Social Sciences " 2022, nr 1(15); Ciglic K., Jurczyk M., Konkel A., Lewandowska-Wiśniewska I., Mikołajczyk D., Podwiński K., Rozenblum L., Sordyl J., Spychała M., Vager Y. (Itzik), Żelechowski R., Skokowski D. (red.), *Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny*, Instytut Kościuszki, Kraków 2017; Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, FNCE, Poznań 2018.

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

12. Siwicki M., *Podział i definicja cyberprzestępstw*, „Prokuratura i Prawo" 2012, nr 7-8, s. 246-256.
13. Kowalewski J., Kowalewski M., *Cyberterroryzm szczególnym zagrożeniem bezpieczeństwa państwa*, „Telekomunikacja i Techniki Informacyjne" 2014, nr 1-2, s. 24.
14. Kosiński J., *Paradygmaty cyberprzestępczości*, Warszawa 2015, s. 46.
15. *Barometr cyberbezpieczeństwa. W kierunku rozwiązań chmurowych*, KPMG, Warszawa 2020, s. 5, https://assets.kpmg/content/dam/kpmg/pl/pdf/2020/06/pl-raport-kpmg-barometr-cyberbezpieczenstwa-2020-w-kierunku-rozwiazan-chmurowych.pdf (dostęp w dniu: 29.11.2023 r.).
16. *Krajobraz bezpieczeństwa polskiego Internetu. Raport roczny z działalności CERT Polska*, CERT/NASK, Warszawa 2020, https://cert.pl/uploads/docs/Raport_CP_2020.pdf (dostęp w dniu: 29.11.2023 r.).
17. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Najwyższa Izba Kontroli, Warszawa 2015, s. 21., https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf (dostęp w dniu: 29.11.2023 r.).
18. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 79.
19. Siemieniecka D., Skibińska M., Majewska K., *Cyberagresja. Zjawisko, skutki, zapobieganie*, Uniwersytet Mikołaja Kopernika, Toruń 2020, s. 10.
20. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 79.
21. Sanger D.E., *Cyberbroń - broń doskonała. Wojny, akty terroryzmu i zarządzanie strachem w epoce komputerów*, Helion, Gliwice 2021.
22. Conway M., *Cyberterrorism: The story so far*, „Journal of Information Warfare" 2003, no 2(2), p. 36.
23. Kopczewski M., *Elementy infrastruktury krytycznej państwa/organizacji – jako obiekty narażone na ataki cyberterrorystyczne*, „Zarządzanie Przedsiębiorstwem" 2011, http://www.ptzp.org.pl/files/konferencje/kzz/artyk_pdf_2011/054.pdf (dostęp w dniu: 29.11.2023 r.).
24. Denning D.E., *Wojna informacyjna i bezpieczeństwo informacji*, Wydawnictwo Naukowo-Techniczne, Warszawa 2002.
25. Bógdał-Brzezińska A., Gawrycki M.F., *Cyberterroryzm i problemy bezpieczeństwa informacyjnego we współczesnym świecie*, ASPRA-JR, Warszawa 2003, s. 154.
26. Ciglic K., Jurczyk M., Konkel A., Lewandowska-Wiśniewska I., Mikołajczyk D., Podwiński K., Rozenblum L., Sordyl J., Spychała M., Vager Y. (Itzik), Żelechowski R., Skokowski D. (red.), *Cyberbezpieczeństwo polskiego przemysłu. Sektor energetyczny*, Instytut Kościuszki, Kraków 2017
27. https://pulaski.pl/komentarz-blackout-w-zachodniej-ukrainie-cyber-atak-o-wymiarze-miedzynarodowym/ (dostęp w dniu: 29.11.2023 r.).

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

28. *Czy Polska jest narażona na atak terrorystów?*, https://www.rmf24.pl/fakty/polska/news-czy-polska-jest-narazona-na-atak-terrorystow,nId,1504590#crp_state=1 (dostęp w dniu: 11.11.2023 r.).
29. Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, FNCE, Poznań 2018, s. 73.
30. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki-organizacji-państwa*, CeDeWu, Warszawa 2016, s. 205.
31. *Hejt*, https://sjp.pwn.pl/szukaj/hejt.html (dostęp w dniu: 06.09.2023 r.).
32. Naruszewicz-Duchlińska A., *Nienawiść w czasach Internetu*, Novae Res, Gdynia 2015, s. 21.
33. Andraszak N., *Hejt wobec funkcjonariuszy Policji w dobie pandemii COVID-19. Jego wpływ na poziom zaangażowania w organizację policjantów*, „Policja. Kwartalnik kadry kierowniczej Policji" 2021, nr 2; *Hejt w stronę Straży Granicznej. Gen. Praga: robimy to, do czego zostaliśmy powołani, bronimy ojczyzny*, https://www.polskieradio24.pl/5/1222/Artykul/2843258,Zolnierzy-bedzie-tylu-ilu-bedzie-trzeba-Szef-MON-o-sytuacji-na-granicy-z-Bialorusia (dostęp w dniu: 13.12.2021 r.).
34. Forlicz S., *Informacja w biznesie*, PWE, Warszawa 2008, s. 174.
35. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki-organizacji-państwa*, CeDeWu, Warszawa 2016, s. 216.
36. Hoffmann T., *Wybrane aspekty cyberbezpieczeństwa w Polsce*, FNCE, Poznań 2018, s. 71.
37. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 80-88.
38. Bencsath B., Pek G., Buttyan L., Felegyhazi M., *The cousins of Stuxnet: Duqu, Flame, and Gauss*, „Future Internet" 2012, no 4(4); Banasiński C., Rojszczak M. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwer, Warszawa 2020, s. 115-124; Siemieniecka D., Skibińska M., Majewska K., *Cyberagresja. Zjawisko, skutki, zapobieganie*, Uniwersytet Mikołaja Kopernika, Toruń 2020, s. 153-159; Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 80-88; Lichocki E., *Model systemu zarządzania kryzysowego w warunkach zagrożeń cyberterrorystycznych dla bezpieczeństwa informacyjnego Sił Zbrojnych RP* (rozprawa doktorska), Akademia Obrony Narodowej, Warszawa 2009, s. 62-63.
39. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 92.
40. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 94.
41. *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, Najwyższa Izba Kontroli, Warszawa 2015, s. 20, https://www.nik.gov.pl/plik/id,8764,vp,10895.pdf (dostęp w dniu: 29.11.2023 r.).

ISSN 2543-7097 / E-ISSN 2544-9478

© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691

42. *Sprawą włamania na skrzynkę mailową Michała Dworczyka zajmuje się ABW*, https://www.infosecurity24.pl/zaryn-sluzby-specjalne-analizuja-opisane-przez-ministra-dworczyka-wydarzenia (dostęp w dniu: 02.12.2021 r.).
43. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 90.
44. *Dane dziesiątek tysięcy sędziów i prokuratorów wyciekły z KSSIP i ciągle wiszą w sieci*, https://niebezpiecznik.pl/post/dane-dziesiatek-tysiecy-sedziow-i-prokuratorow-wyciekly-z--kssip-i-ciagle-wisza-w-sieci/ (dostęp w dniu: 30.11.2021 r.).
45. *Hakerzy zaatakowali polskie witryny podczas konferencji bliskowschodniej w Warszawie*, https://zaufanatrzeciastrona.pl/post/hakerzy-zaatakowali-polskie-witryny-podczas-konferencji-bliskowschodniej-w-warszawie/ (dostęp w dniu: 06.12.2021 r.).
46. Wojciechowska-Filipek S., Ciekanowski Z., *Bezpieczeństwo funkcjonowania w cyberprzestrzeni jednostki-organizacji-państwa*, CeDeWu, Warszawa 2016, s. 217-218.
47. Białoskórski R., *Cyberzagrożenia w środowisku bezpieczeństwa XXI wieku. Zarys problematyki*, Wyższa Szkoła Cła i Logistyki, Warszawa 2011, s. 75.
48. *Kto stoi za atakiem na Internetowe Forum Policyjne*, https://zaufanatrzeciastrona.pl/post/kto-stoi-za-atakiem-na-internetowe-forum-policyjne/ (dostęp w dniu: 30.11.2021 r.).
49. *Atak hakerski na portal związków zawodowych Służby Więziennej. Stoją za nim islamiści?*, https://www.wprost.pl/514625/atak-hakerski-na-portal-zwiazkow-zawodowych-sluzby-wieziennej-st.html (dostęp w dniu: 05.12.2021 r.).
50. *Uwaga na groźne SMS-y dotyczące przesyłek*, https://niebezpiecznik.pl/post/uwaga-na-grozne-sms-y-dotyczace-przesylek/ (dostęp w dniu: 17.12.2021 r.).
51. Banasiński C., Rojszczak M. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Wolters Kluwer, Warszawa 2020, s. 449.
52. Ustawa z dnia 6 czerwca 1997 – *Kodeks karny* (Dz.U. z 2022 r. poz. 1138).
53. Ustawa z dnia 10 maja 2018 r. *o ochronie danych osobowych* (Dz.U. z 2019 r. poz. 1781).
54. Ustawa z dnia 4 lutego 1994 r. *o prawie autorskim i prawach pokrewnych* (Dz.U. z 2022 r. poz. 2509).
55. Ustawa z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz.U. z 2023 r. poz. 913).
56. Ustawa z dnia 18 lipca 2002 r. *o świadczeniu usług drogą elektroniczną* (Dz.U. z 2020 r. poz. 344).

ISSN 2543-7097 / E-ISSN 2544-9478
© 2023 / Wydawca: Międzynarodowy Instytut Innowacji Nauka-Edukacja-Rozwój w Warszawie, Polska

This is an open access article
under the CC BY-NC license (http://creativecommons.org/licenses/by-nc/4.0/)

Lewandowski M.,(2023). Zagrożenia w Funkcjonowaniu Jednostek Organizacyjnych Służby Więziennej Związane z Nowymi Technologiami – Cyberprzestępstwa
International Journal of Legal Studies, 2(14)2023: 51 - 65
DOI 10.5604/01.3001.0054.2691