Marcin Kiestrzyn

# Ocena poziomu wydatków publicznych na funkcjonowanie systemu cyberbezpieczeństwa w Polsce na tle Unii Europejskiej

**Assessment of the level of public expenditure on the functioning of the cybersecurity system in Poland compared to the European Union**

The main purpose of the article is to present and assess the changes in the directions of expenditure on cybersecurity in Poland from the state budget and their impact on the assessment of technological advancement in comparison with the EU. The formal and legal regulations that came into force over the last years in the EU and in Poland in this area are reviewed as well. The first part of the article focuses on the evolution of definitions and regulations regarding cyberspace, cybercrime and cybersecurity. It also highlights the entities involved in the cybersecurity system and their role in preventing threats in cyberspace. Next, the author briefly examines main threats in the digital space of the European Union and Poland. The final section assesses directions of financing cybersecurity in Poland versus the EU. The author argues that as the use of technology increases, it will be necessary to increase public spending on cybersecurity in order to maintain the level of security.

| | |
|---|---|
| **DOI** | https://doi.org/10.31268/StudiaBAS.2020.25 |
| **Słowa kluczowe** | cyberbezpieczeństwo, zagrożenia w cyberprzestrzeni, wydatki na cyberbezpieczeństwo w Unii Europejskiej, wydatki na cyberbezpieczeństwo w Polsce |
| **Keywords** | cybersecurity, threats in cyberspace, EU expenditure on cybersecurity, expenditure on cybersecurity in Poland |
| **O autorze** | doktorant w Katedrze Finansów Zrównoważonych i Rynków Kapitałowych w Instytucie Ekonomii i Finansów Uniwersytetu Szczecińskiego • ✉ mkiestrzyn@gmail.com • ORCID 0000-0003-1188-0691 |

## Wstęp

We współczesnym świecie wraz z postępem technologii, cyfryzacji gospodarki oraz szybkiego rozwoju niemalże każdej sfery życia społecznego zmienia się także profil, rodzaj oraz skala obecnych cyberzagrożeń. Odpowiednia cyberochrona staje się w ostatnich latach priorytetem wielu rządów, w tym także polskiego.

Cyberprzestępczość skutkuje zaburzeniami funkcjonowania społeczeństwa oraz podważa poczucie bezpieczeństwa zarówno życia, jak i prowadzenia biznesu. Pojawia się problem sprawnego działania instytucji publicznych i prywatnych. Zagrożenia w cyberprzestrzeni zakłócają również przebieg procesów produkcyjnych i usługowych, a tym samym negatywnie oddziałują na wzrost gospodarczy i bezpieczeństwo publiczne. Zapewnienie cyberbezpieczeństwa staje się nie tylko obowiązkiem, lecz także obiektywną koniecznością. Według raportu Centrum Studiów Strategicznych i Międzynarodowych (Center for Strategic and International Studies – CSIS) i McAfee cyberprzestępczość kosztowała świat prawie 600 miliardów dolarów, czyli 0,8% glo-

balnego PKB[1]. Masowe ataki cybernetyczne zostały wskazane jako jedno z większych zagrożeń dla państw i współczesnych społeczeństw[2]. Cyberataki dotyczą praktycznie wszystkich sfer działalności: od rządu, poprzez przedsiębiorstwa prywatne i państwowe, aż po obywateli.

Unia Europejska (w tym Polska) przyjęła dokumenty kierunkowe oraz ramy prawne, dzięki czemu nakreśliła konkretne cele i działania w zakresie cyberbezpieczeństwa. Działania te wymagają zapewnienia nie tylko struktur, lecz także odpowiedniego zaplecza finansowego.

Celem artykułu jest ukazanie i ocena zmian w kierunkach ponoszenia wydatków publicznych na cyberbezpieczeństwo w Polsce z budżetu państwa i ich wpływu na ocenę stanu zaawansowania technologicznego na tle UE. Zaprezentowane zostaną zagadnienia związane z ewolucją podejścia do cyberbezpieczeństwa oraz regulacje formalno-prawne obowiązujące w UE i w Polsce w tym zakresie. W artykule zostaną przedstawione w formie opisowej i graficznej – na podstawie raportów z Polski i UE – najbardziej popularne metody wykorzystywane przez cyberprzestępców. Celem analizy jest wskazanie dylematów, problemów i potencjalnych kierunków zmian w finansowaniu cyberbezpieczeństwa. Dla dokładniejszego zobrazowania kierunków zmian w finasowaniu cyberbezpieczeństwa w Polsce w artykule zostanie przybliżona dynamika w grupie wskaźników służących do oceny poziomu nakładów z budżetu państwa na cyberbezpieczeństwo w Polsce i w Unii Europejskiej w latach 2013–2018. W ostatniej części zostaną oszacowane przyszłe wydatki publiczne na cyberbezpieczeństwo w oparciu o wydatki z budżetu państwa.

## Cyberbezpieczeństwo jako zjawisko implikujące działania ze strony państwa – zarys problemu

Nowoczesne technologie informacyjne integrują ludzkość w skali globalnej i jednocześnie powodują decentralizację społeczeństw, instytucji oraz miejsc pracy. W cyberprzestrzeni są tworzone i kształtowane relacje społeczne, a internet stał się narzędziem wpływania na zachowania grup społecznych, a także oddziaływania w płaszczyźnie politycznej[3]. Instytucje publiczne coraz mocniej wchodzą w sferę realizacji usług publicznych w oparciu o technologie cyfrowe, np. Program Polska Cyfrowa (e-Obywatel, digitalizacja i udostępnianie rejestrów i zasobów, elektronizacja sądów). Również doświadczenia w okresie pandemii COVID-19 pokazały konieczność przyspieszenia zmian w zakresie cyfryzacji gospodarki i życia społecznego. W cyberprzestrzeni, tak jak w środowisku rzeczywistym, powstają i rozwijają się liczne zagrożenia. Wraz z rozwojem

1 McAfee, *The Economic Impact of Cybercrime – No Slowing Down*, February 2018, s. 1, https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf. [dostęp: 1 czerwca 2020 r.].

2 Komisja Europejska, *Biała księga w sprawie przyszłości Europy. Refleksje i scenariusze dotyczące przyszłości UE-27 do 2025 r.*, Bruksela 2017, s. 9, https://ec.europa.eu/commission/sites/beta-political/files/biala_ksiega_w_sprawie_przyszlosci_europy_pl.pdf. [dostęp: 1 czerwca 2020 r.].

3 Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017, s. 4, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109 [dostęp: 2 października 2020 r.].

technologii krajowe normy prawne powinny być sukcesywnie dostosowywane do regulacji międzynarodowych, a w szczególności do prawa unijnego, w zakresie zwalczania cyberprzestępstw i zapewnienia odpowiedniego poziomu cyberbezpieczeństwa[4].

W ramach podstawowych pojęć związanych z zagrożeniami w zinformatyzowanym świecie można wyróżnić:

- cyberprzestrzeń,
- cyberprzestępczość,
- cyberbezpieczeństwo.

Cyberprzestrzeń jako przestrzeń wirtualna bez fizycznych granic definiowana jest na wiele sposobów[5]. Wybrane definicje cyberprzestrzeni przedstawiono w tabeli 1.

Jak ukazano w tabeli 1, definicja cyberprzestrzeni zmieniała się w czasie praktycznie od koncepcji zarysowanych w literaturze[6], przez podejście praktyczne, do regulacji prawnych. Cechą wspólną zaprezentowanych definicji jest charakter wirtualny przestrzeni bez granic oparty na łączności systemów informatycznych i ich użytkowników oraz tworzonych relacji. Cyberprzestrzeń pozbawiona jest wszelkich fizycznych atrybutów czyjejś obecności, takich jak: odciski palców, głos, wizerunek[7]. Powszechne bowiem zastosowanie nowoczesnych rozwiązań teleinformatycznych – głównie komputerów oraz sieci komputerowych – wytworzyło specyficzną cyfrową przestrzeń do podejmowania różnych rodzajów czynności, zarówno tych istotnych wyłącznie obyczajowo i społecznie, jak i prawnych[8]. Od strony technicznej fundamentem tej domeny jest oczywiście globalna sieć internet[9].

Nie ma precyzyjnej i jednolitej definicji pojęcia „cyberprzestępczość"[10], jednakże odnosi się ono do przestępstw popełnianych za pomocą komputera z użyciem internetu. Wybrane sposoby rozumienia przestępstw w cyberprzestrzeni przedstawiono w tabeli 2.

Zaprezentowane w tabeli 2 definicje, choć literalnie różne, odnoszą się do tego samego problemu przestępstw popełnianych za pomocą komputera z użyciem internetu. Ich uzupełnieniem, a wręcz doprecyzowaniem pozwalającym na poznanie stanowiska w zakresie pojęcia

4 *Prawne i społeczne aspekty cyberbezpieczeństwa*, red. S. Gwoździewicz, K. Tomaszycki, Międzynarodowy Instytut Innowacji, Warszawa 2017, s. 7, https://instytutinnowacji.edu.pl/wp-content/uploads/2016/11/PISAC_Druk.pdf [dostęp: 1 czerwca 2020 r.].

5 Według F.D Kramera istnieje przynajmniej 28 definicji cyberprzestrzeni. Zob. F.D. Kramer, *Cyberpower and National Security: Policy Recommendations for a Strategic Framework* [w:] *Cyberpower and National Security*, red. F.D. Kramer, S.H. Starr, L.K. Wentz, National Defense University Press, Washington, D.C. 2009.

6 Zob. I.A. Jaroszewska, *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017, s. 6–13.

7 R. Jedlińska, *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, nr 1(126), t. 2, s. 185, https://doi.org/10.18276/epu.2017.126/2-19.

8 J. Janowski, *Technological Destabilization of Law* [w:] *Information Technology and Law*, W. Cyrul, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014, s. 15 i n., 21 i n.

9 J. Wasilewski, *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 225, https://www.abw.gov.pl/download/1/1284/Segregator13.pdf. [dostęp: 1 czerwca 2020 r.].

10 Zob. np. J. Wasilewski, *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 149–173, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-5c76c983-d00f-431d-9e16-6fa0ed5a9f75 [dostęp: 1 czerwca 2020 r.].

**Tabela 1. Wybrane definicje cyberprzestrzeni**

| Lp. | Autor/Źródło | Rok | Definicja cyberprzestrzeni |
|---|---|---|---|
| 1 | W. Gibson[a] | 1984 | Konsensualna halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników we wszystkich krajach, przez dzieci nauczane pojęć matematycznych (...). Graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Niewyobrażalna złożoność (...). Świetlne linie przebiegały bezprzestrzeń umysłu, skupiska i konstelacje danych. |
| 2 | R. Ottis, P. Lorents[b] | 2010 | Cyberprzestrzeń to zależny od czasu zestaw połączonych ze sobą systemów informatycznych i użytkowników, którzy wchodzą w interakcje z tymi systemami. |
| 3 | Dyrektywa Parlamentu Europejskiego i Rady[c] | 2016 | „Sieci i systemy informatyczne" oznaczają:<br>a) sieci łączności elektronicznej w rozumieniu art. 2 lit. a/ dyrektywy 2002/21/WE;<br>b) wszelkie urządzenia lub grupy wzajemnie połączonych lub powiązanych urządzeń, z których jedno lub większa ich liczba, wykonując program, dokonuje automatycznego przetwarzania danych cyfrowych; lub<br>c) dane cyfrowe przechowywane, przetwarzane, odzyskiwane lub przekazywane przez elementy określone w lit. a/ i b/ w celu ich eksploatacji, użycia, ochrony i utrzymania. |
| 4 | Krajowe Ramy Polityki Cyberbezpieczeństwa Polski[d] | 2017 | Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami. |

[a] Fragment książki Williama Gibsona *Neuromancer* w tłumaczeniu Piotra W. Cholewy, Książnica, Katowice 2009, s. 59.

[b] R. Ottis, P. Lorents, *Cyberspace: Definition and Implications* [w:] *Proceedings of the 5th International Conference on Information Warfare and Security 2010, Dayton, Ohio, USA, 8–9 April 2010*, Academic Conferences Limited, Reading, s. 1, https://www.ccdcoe.org/library/publications/cyberspace-definition-and-implications/ [dostęp: 1 czerwca 2020 r.].

[c] Art. 4 pkt 1 dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 2016.194.1).

[d] Ministerstwo Cyfryzacji, *Krajowe Ramy...*

Źródło: Opracowanie własne na podstawie wskazanych pozycji.

„cyberprzestępstwo", jest wypowiedź Komisji Wspólnot Europejskich, która wyróżnia następujące rodzaje przestępstw występujących w cyberprzestrzeni[11]:

- tradycyjne formy przestępstw, takie jak oszustwo czy fałszerstwo, jednak w kontekście cyberprzestępczości odnoszące się konkretnie do przestępstw popełnionych z użyciem elektronicznych sieci informatycznych i systemów informatycznych (dalej: sieci łączności elektronicznej);
- publikacja nielegalnych treści w mediach elektronicznych (np. materiałów związanych z seksualnym wykorzystywaniem dzieci czy nawoływaniem do nienawiści rasowej);

11 Komisja Wspólnot Europejskich, Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości, 2007, s. 2; w literaturze przedmiotu dyskusję na ten temat rozszerza: R. Jedlińska, *op. cit.*, s. 185–194.

**Tabela 2. Wybrane sposoby rozumienia pojęcia „cyberprzestępczość"**

| Lp. | Autor/Źródło | Rok | Definicja |
|---|---|---|---|
| 1 | Komisja Wspólnot Europejskich[a] | 2007 | Czyny przestępcze dokonane przy użyciu sieci łączności elektronicznej i systemów informatycznych lub skierowane przeciwko takich sieciom i systemom. |
| 2 | Ministerstwo Cyfryzacji, Agencja Bezpieczeństwa Wewnętrznego[b] | 2013 | Czyn zabroniony popełniony w obszarze cyberprzestrzeni. |
| 3 | Interpol[c] | 2020 | Przestępstwa przeciwko komputerom i systemom informatycznym, których celem jest uzyskanie nieautoryzowanego dostępu do urządzenia lub odmowa dostępu dla legalnego użytkownika. |

[a] Komisja Wspólnot Europejskich, Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości, 2007, s. 2.
[b] Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa, 25 czerwca 2013 r., s. 5, https://bip.malopolska.pl/e,pobierz,get.html?id=1223287 [dostęp: 1 czerwca 2020 r.].
[c] Interpol, w oryginale: 'Pure cybercrime' refers to crimes against computers and information systems, where the aim is to gain unauthorized access to a device or deny access to a legitimate user, https://websites.fraunhofer.de/CIPedia/index.php/Cybercrime#Interpol [dostęp: 2 października 2020 r.].
Źródło: Opracowanie własne na podstawie wskazanych pozycji.

- przestępstwa typowe dla sieci łączności elektronicznej, tj. ataki przeciwko systemom informatycznym, ataki typu „denial of service" oraz hakerstwo.

W ogólnym ujęciu czyny określane jako cyberprzestępstwa polegają na posługiwaniu się sieciami telekomunikacyjnymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne[12]. Przestępstwa te nie znają granic fizycznych ani wirtualnych, powodują poważne szkody i stanowią bardzo realne zagrożenie dla ofiar na całym świecie[13].

Cyberbezpieczeństwo jest skorelowane z omówionymi wyżej pojęciami i również nie posiada jednej, precyzyjnej, międzynarodowej definicji[14]. W kategoriach językowych pojęcie „cyberbezpieczeństwo" lub „bezpieczeństwo cybernetyczne" – w zależności od organizacji i przyjętego sposobu nazywania – jest raczej nowym terminem, pochodzącym od słowa „cyberprzestrzeń". Termin „cyberbezpieczeństwo" został stworzony i wykorzystany przez specjalistów IT, konsultantów, lobbystów i polityków w celu odniesienia się do obaw związanych z bezpieczeństwem w cyberprzestrzeni[15]. Bezpieczeństwo cybernetyczne polega na działaniach mających na celu

12 M. Siwicki, *Cyberprzestępczość*, Wydawnictwo C.H. Beck, Warszawa 2013, s. 19.
13 Interpol, *Cyberattacks know no borders and evolve at a rapid pace*, https://www.interpol.int/Crimes/Cybercrime [dostęp: 1 czerwca 2020 r.].
14 Zob. np. European Union Agency for Network and Information Security, *Definition of Cybersecurity: Gaps and overlaps in standardisation*, December 2015, s. 13–19, https://www.enisa.europa.eu/publications/definition-of-cybersecurity [dostęp: 1 czerwca 2020 r.].
15 *Ibidem*, s. 8, w oryginale: *In language terms 'Cybersecurity' or 'cyber security', depending on the organization and the spelling of the word within its context, is a rather young term. Originated on the term 'Cyber Space',*

zachowanie dostępności i integralności sieci i infrastruktury oraz zachowanie poufności zawartych w nich informacji[16]. Analiza wybranych obowiązujących przepisów prawnych w Unii Europejskiej i w Polsce pokazuje, że różnice w definicjach cyberbezpieczeństwa są prawie niezauważalne, co ujęto na rysunku 1.

**Rysunek 1. Wybrane definicje pojęcia „cyberbezpieczeństwo"**

| Cyberbezpieczeństwo – Unia Europejska |
| --- |
| „Bezpieczeństwo sieci i systemów informatycznych" oznacza odporność sieci i systemów informatycznych, przy danym poziomie zaufania, na wszelkie działania naruszające dostępność, autentyczność, integralność lub poufność przechowywanych lub przekazywanych, lub przetwarzanych danych lub związanych z nimi usług oferowanych lub dostępnych poprzez te sieci i systemy informatyczne. |
| **Cyberbezpieczeństwo - Polska** |
| Odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. |

Źródło: Opracowanie własne na podstawie: dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 2016.194.1); Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109 [dostęp: 2 października 2020 r.].

Wraz z rozwojem cyberprzestępczości rośnie zainteresowanie rządów, w tym polskiego, problematyką zabezpieczenia sieci i urządzeń przed dostępem osób niepowołanych. Zagadnienia te zajmują szczególne miejsce pośród realizowanych przez państwa zadań, a państwa członkowskie UE dostrzegają konieczność prowadzenia wspólnej polityki i ujednolicania podejść do kwestii cyberprzestępczości i cyberbezpieczeństwa. Bezpieczeństwo jest uznawane za dobro publiczne; tym samym zapewnienie cyberbezpieczeństwa na poziomie poszczególnych państw i wspólnot uważa się za dobro publiczne[17].

Ewolucja pojęcia „cyberbezpieczeństwo", w ramach przepisów Unii Europejskiej, jest związana z przyjęciem w 1997 r. przez Parlament Europejski oraz Radę Unii Europejskiej dyrektywy w sprawie przetwarzania danych osobowych i ochrony prywatnych danych w sektorze łączności elektronicznej[18]. Świadoma rosnącej potrzeby unormowania cyberbezpieczeństwa w ramach

*the term 'Cybersecurity' was crafted and used by IT professionals, consultants, lobbyists and politics to address security concerns in the 'Cyber Space'.*

16 Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, nr 2(10), s. 108, https://ssl-kolegia.sgh.waw.pl/pl/KES/czasopisma/kwartalnik_szpp/Documents/2(10)%202016/066_05_Chmielewski.pdf. [dostęp: 1 czerwca 2020 r.].

17 M. Leszczyński, *Bezpieczeństwo jako dobro publiczne w społeczeństwie ryzyka*, „Nierówności Społeczne a Wzrost Gospodarczy" 2020, nr 61(1), s. 117–125, https://doi.org/10.15584/nsawg.2020.1.8.

18 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 2002.201.37).

swoich działań Komisja Europejska opracowała strategię bezpieczeństwa cybernetycznego Unii Europejskiej pod hasłem „Otwarta, bezpieczna i chroniona cyberprzestrzeń”[19]. W uzupełnieniu do tej strategii, w celu standaryzacji pojęć związanych z cyberbezpieczeństwem, European Union Agency for Network and Information Security (ENISA) sporządziła dokument uszczegółowiający problematykę cyberbezpieczeństwa, w którym omawianą tematykę połączono z obszarami działań w samej cyberprzestrzeni, jak i z wpływem tych działań na realne zdarzenia polityczne, wojskowe oraz infrastrukturę (tabela 3)[20].

**Tabela 3. Rodzaje cyberbezpieczeństwa**

| Lp. | Rodzaj cyberbezpieczeństwa | Definicja |
|---|---|---|
| 1 | Bezpieczeństwo komunikacyjne | Ochrona przed zagrożeniem dla infrastruktury technicznej systemu cybernetycznego, które może prowadzić do zmiany jego właściwości w celu wykonywania czynności, które nie były zamierzone przez jego właścicieli, projektantów lub użytkowników. |
| 2 | Bezpieczeństwo operacyjne | Ochrona przed zamierzonym uszkodzeniem procedur lub przepływów pracy, które przyniesie skutki niezamierzone przez właścicieli, projektantów lub użytkowników. |
| 3 | Bezpieczeństwo informacyjne | Ochrona przed zagrożeniem kradzieży, usunięcia lub zmiany przechowywanych lub przesyłanych danych w systemie cybernetycznym. |
| 4 | Bezpieczeństwo fizyczne | Ochrona przed zagrożeniami fizycznymi, które mogą wpływać na stan systemu cybernetycznego. |
| 5 | Bezpieczeństwo narodowe | Ochrona przed zagrożeniem, które pochodzi z cyberprzestrzeni, ale może zagrozić zasobom fizycznym lub cybernetycznym w sposób, który przyniesie atakującemu korzyści polityczne, wojskowe lub strategiczne. |

Źródło: Opracowanie własne na podstawie: European Union Agency for Network and Information Security, *Definition of Cybersecurity: Gaps and overlaps in standardisation*, December 2015, https://www.enisa.europa.eu/publications/definition-of-cybersecurity [dostęp: 1 czerwca 2020 r.].

Przedstawione w tabeli 3 obszary cyberbezpieczeństwa wskazują na konieczne działania w celu wyeliminowania zagrożeń w cyberprzestrzeni. Jak widać, działania te mają charakter zarówno wirtualny (działania bezpośrednio w sieci), jak i fizyczny (działania zapobiegawcze związane z samą siecią).

W celu dostosowania działań dla poprawy cyberbezpieczeństwa w Unii Europejskiej do postępu technologicznego wprowadzono obecnie obowiązującą dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (dalej: dyrektywa NIS). W dyrektywie wskazano m.in. kluczowe podmioty systemu cyberbezpieczeństwa dla państw członkowskich:

19 European Commission, *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, Brussels, 7.02.2013, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667 [dostęp: 1 czerwca 2020 r.].

20 Szerzej: European Union Agency for Network and Information Security, *Definition of Cybersecurity...*, s. 11–12.

- grupa współpracy – wspiera i ułatwia strategiczną współpracę i wymianę informacji między państwami członkowskimi oraz rozwija wśród nich zaufanie i pewność; składa się z przedstawicieli państw członkowskich, Komisji i ENISA;
- sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT) – przyczynia się do rozwijania zaufania i pewności między państwami członkowskimi oraz promuje szybką i skuteczną współpracę operacyjną;
- właściwe organy krajowe – monitorują stosowanie dyrektywy na poziomie krajowym;
- pojedynczy punkt kontaktowy – pełni funkcję łącznikową w celu zapewnienia transgranicznej współpracy organów państw członkowskich oraz współpracy z odpowiednimi organami w innych państwach członkowskich, a także z grupą współpracy;
- operatorzy usług kluczowych – podmioty świadczące usługi w sektorach uznanych za kluczowe dla funkcjonowania kraju, tzn. w sektorach: energetycznym, transportowym, bankowym i infrastruktury rynków finansowych, ochrony zdrowia, zaopatrzenia w wodę pitną (wraz z dystrybucją), infrastruktury cyfrowej;
- dostawcy usług cyfrowych – każda osoba prawna, która świadczy usługi cyfrowe.

Każde państwo członkowskie przyjęło, na podstawie dyrektywy, krajową strategię bezpieczeństwa sieci i systemów informatycznych, w której określono również kluczowe podmioty.

Krajowy system cyberbezpieczeństwa w Polsce został zdefiniowany w ustawie z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[21], która weszła w życie 28 sierpnia 2018 r. Celem systemu jest „zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów"[22]. W ramach działań związanych z zapewnieniem funkcjonowania krajowego systemu cyberbezpieczeństwa w Polsce na podstawie dyrektywy NIS szczegółowo określono podmioty podejmujące działania w zakresie zapewnienia cyberbezpieczeństwa (tabela 4).

Poza podmiotami wskazanymi bezpośrednio w dyrektywie NIS krajowy system cyberbezpieczeństwa w Polsce objął również podmioty wskazane w poz. 6–9 tabeli 4. Ustawa o krajowym systemie cyberbezpieczeństwa przypisała im zadania i miejsce w systemie:

- Pełnomocnik Rządu ds. Cyberbezpieczeństwa – odpowiada za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa; Pełnomocnik podlega Radzie Ministrów i jest w randze sekretarza stanu albo podsekretarza stanu;
- Kolegium ds. Cyberbezpieczeństwa – organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego i organów właściwych do spraw cyberbezpieczeństwa; Kolegium działa przy Radzie Ministrów;
- podmioty publiczne – zobligowane są do zgłaszania incydentów, które powodują lub mogą spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego wykonywanego przez dany podmiot publiczny; są to organy władzy publicznej, jednostki budżetowe,

21 Dz.U. 2018, poz. 1560; tekst jednolity: Dz.U. 2020, poz. 1369.

22 Tamże, art. 3.

**Tabela 4. Podmioty podejmujące działania w zakresie zapewnienia cyberbezpieczeństwa w Polsce, zaadaptowane na podstawie dyrektywy NIS**

| Lp. | Podmioty określone w dyrektywie NIS | Podmioty określone w Polsce |
|---|---|---|
| 1 | Sieć zespołów reagowania na incydenty bezpieczeństwa komputerowego (sieć CSIRT) | CSIRT NASK (CERT Polska) – prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;<br>CSIRT GOV – prowadzony przez Agencję Bezpieczeństwa Wewnętrznego;<br>CSIRT MON – prowadzony przez Ministerstwo Obrony Narodowej;<br>Sektorowe zespoły cyberbezpieczeństwa. |
| 2 | Właściwe organy krajowe | Ministerstwa odpowiedzialne za poszczególne działy gospodarki uznane za sektory kluczowe dla funkcjonowania państwa. |
| 3 | Pojedynczy punkt kontaktowy | Pojedynczy Punkt Kontaktowy prowadzony przez ministra właściwego do spraw informatyzacji |
| 4 | Operatorzy usług kluczowych | Operatorzy usług kluczowych |
| 5 | Dostawcy usług cyfrowych | Dostawcy usług cyfrowych |
| 6 | | Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa |
| 7 | | Kolegium do Spraw Cyberbezpieczeństwa |
| 8 | | Podmioty publiczne |
| 9 | | Podmioty świadczące usługi z zakresu cyberbezpieczeństwa |

Źródło: Opracowanie własne na podstawie: ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; materiały ze strony internetowej Ministerstwa Cyfryzacji: https://www.gov.pl/web/cyfryzacja/cyberbezpieczenstwo.

samorządowe zakłady budżetowe, agencje wykonawcze, instytucje gospodarki budżetowej, uczelnie publiczne i Polska Akademia Nauk, Zakład Ubezpieczeń Społecznych, Kasa Rolniczego Ubezpieczenia Społecznego, Narodowy Fundusz Zdrowia, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polska Agencja Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej;

- podmioty świadczące usługi cyberbezpieczeństwa – podmioty, które mogą zawierać umowy z operatorami usług kluczowych w zakresie zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej; w takim przypadku stanowią całość lub część wewnętrznych struktur powołanych przez operatora usługi kluczowej odpowiedzialnych za cyberbezpieczeństwo.

Role i zadania wyżej wymienionych podmiotów stanowią uzupełnienie krajowego systemu cyberbezpieczeństwa o elementy związane z koordynacją i planowaniem państwa (Pełnomocnik Rządu ds. Cyberbezpieczeństwa oraz Kolegium ds. Cyberbezpieczeństwa), jak i ze zwiększeniem nadzoru nad systemem i wsparciem systemu przez podmioty publiczne i podmioty świadczące usługi cyberbezpieczeństwa.

Podsumowując: pojęcia, takie jak cyberprzestrzeń, cyberprzestępstwo, cyberbezpieczeństwo, choć w dzisiejszym zdigitalizowanym świecie są szeroko spopularyzowane, są różnie definiowane zarówno w literaturze jak i przepisach. Unia Europejska podjęła działania w celu standaryzacji definicji[23]. Polska, wdrażając przepisy UE, wprowadziła ustawę o krajowym systemie cyberbezpieczeństwa, a w niej uregulowania prawne w zakresie funkcjonowania tego systemu i podmiotów nim objętych. Zapewnianie cyberbezpieczeństwa w Polsce i budowanie odpornego systemu to nieustanny proces, jednakże podjęte działania legislacyjne są oceniane jako mogące przyspieszyć wypracowanie odpowiednich mechanizmów zapewniających cyberbezpieczeństwo w Polsce[24].

## Główne zagrożenia w przestrzeni cyfrowej Unii Europejskiej i Polski jako kierunki ponoszenia wydatków publicznych z budżetu państwa

Postęp w dziedzinie globalnej komunikacji, nieskrępowany dostęp do informacji oraz ich przechowywanie i wykorzystywanie spowodowały, że integralną częścią przestrzeni cyfrowej stały się przestępstwa komputerowe. Kwoty środków utraconych z powodu przestępstw popełnianych w cyberprzestrzeni – o czym dowiadujemy się ze statystyk – na każdym robią ogromne wrażenie, niezależnie od tego, czy odbiorcą tych danych jest ekspert czy zwykły obywatel[25]. W badaniu Clark School na Uniwersytecie Marylandu oszacowano prawie stały wskaźnik ataków hakerów na komputery z dostępem do internetu – średnio co 39 sekund[26]. Za atakami stoją zarówno zorganizowane grupy przestępcze czy terrorystyczne, jak i grupy finansowane przez obce państwa. Ofiarami tych przestępstw stają się instytucje rządowe, przedsiębiorstwa i osoby prywatne. Działalność przestępcza ma wpływ na wszystkie obszary działań: od strat ekonomicznych do bezpieczeństwa narodowego[27]. Uproszczony schemat relacji w zakresie cyberprzestępczości przedstawiono na rysunku 2.

---

23 European Union Agency for Network and Information Security, *Definition of Cybersecurity...*, s. 13–19.

24 M. Sławińska, *Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania*, Rządowe Centrum Bezpieczeństwa, https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/ [dostęp: 1 czerwca 2020 r.].

25 A. Kańciak, *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 109, http://www.abw.gov.pl/download/1/1719/AKanciak.pdf [dostęp: 1 czerwca 2020 r.].

26 M. Cukier, *Study: Hackers Attack Every 39 Seconds*, A.J. Clark School of Engineering, 9 lutego 2007 r., https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds [dostęp: 1 czerwca 2020 r.].

27 Zob. A. Ahmad, N. Ahmad, S. Ali, *Crime and Economic Growth in Developing Countries: Evidence from Pakistan*, „Journal of Basic and Applied Scientific Research" 2014, nr 4, s. 31, https://www.researchgate.net/profile/Sharafat_Ali3/publication/275019421_Crime_and_Economic_Growth_in_Developing_Countries_Evidence_from_Pakistan/links/552e67070cf2acd38cb93de5.pdf; C. Detotto, E. Otranto, *Does Crime Affect Economic Growth?*, "Kyklos. International Review for Social Sciences" 2010, t. 63, nr 3, s. 330, Wiley Blackwell, https://doi.org/10.1111/j.1467-6435.2010.00477.x; K. Blackburn, K.C. Neanidis, M.P. Rana, *A theory of organized crime, corruption and economic growth*, "Economic Theory Bulletin" 2017, nr 5, s. 227–245, https://doi.org/10.1007/s40505-017-0116-5.

**Rysunek 2. Uproszczony schemat relacji w cyberprzestępczości**


Źródło: Opracowanie własne na podstawie: Ministerstwo Cyfryzacji, *Krajowe Ramy...*

W ramach powyższego schematu jako „atakujący" zostały wyodrębnione dwa rodzaje grup[28]:

- grupy przestępcze kierujące się chęcią zysku lub pobudkami terrorystycznymi;
- grupy, za którymi stoją obce państwa, kierujące się chęcią pozyskania informacji, destabilizacji politycznej lub gospodarczej albo wywołania niezadowolenia społecznego.

Podział ten jest umowny, gdyż nie ma jednolitej nomenklatury w literaturze i praktyce[29] dla tego typu grup. Cyberprzestępcy tworzą grupy identyfikowane poprzez charakterystyczne działania, które ułatwiają ich rozróżnienie. Niektóre grupy mogą być identyfikowane jako działające w ten sam sposób, lecz pod innymi nazwami. Dla przykładu: organizacja non-profit MITRE[30], na podstawie zgromadzonych danych MITRE ATT&CK, wyodrębniła 94 grupy przestępcze na całym świecie.

Jak wskazano powyżej, ofiarami przestępstw w cyberprzestrzeni stają się instytucje rządowe, przedsiębiorstwa i osoby prywatne. Na wykresie 1 przedstawiono główne cele ataków.

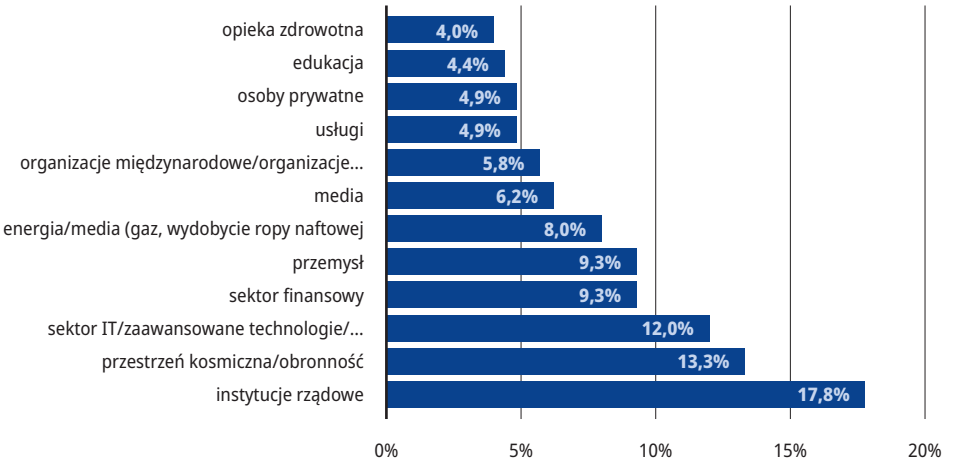
Dane przedstawione na wykresie 1 wskazują, że cyberprzestępcy najczęściej dokonują przestępstw mających na celu podważenie i obniżenie sprawności funkcjonowania instytucji sektora publicznego, przez co godzą w sfery społecznie newralgiczne. Jedną z tych sfer jest bezpieczeństwo narodowe, w tym obronność (13,3% ataków). Ma to szczególne znaczenie, gdyż odbija się na poczuciu bezpieczeństwa społecznego. Zarówno ataki na instytucje rządowe, jak i ataki wymierzone w sferę obronności przekładają się na poczucie bezpieczeństwa społeczeństwa i na sprawność funkcjonowania państwa – zwłaszcza gdy grupy przestępcze mają motywy polityczne lub geopolityczne. Kradzież cennych danych o znaczeniu strategicznym tworzy przewagę, która może zostać wykorzystana w rozgrywkach politycznych, gospodarczych czy militarnych

28 Ministerstwo Cyfryzacji, *Krajowe Ramy...*, s. 4.

29 M. Bay, *What is cybersecurity? In search of an encompassing definition for the post-Snowden era*, „French Journal For Media Research" 2016, nr 6, s. 21, https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era [dostęp: 1 czerwca 2020 r.].

30 Zob. https://attack.mitre.org/groups/ [dostęp: 1 czerwca 2020 r.]

**Wykres 1. Cel ataków grup hakerskich**




Źródło: A. Kopciuch, *Grupy cyberprzestępcze*, Fundacja Bezpieczna Cyberprzestrzeń, 12 lutego 2019 r., https://www.cybsecurity.org/pl/grupy-cyberprzestepcze/ [dostęp: 1 czerwca 2020 r.].

pomiędzy państwami[31]. Inną sferą newralgiczną narażoną na cyberataki jest bezpieczeństwo obrotu gospodarczego, w tym przebieg procesów produkcyjnych i usługowych.

Na podstawie raportu za 2018 r. dotyczącego zagrożeń w cyberprzestrzeni, opracowanego przez ENISA, można stwierdzić, że nastąpiły pewne zmiany w cyberzagrożeniach, które zostały wskazane w tabeli 5.

Głównym zagrożeniem rejestrowanym w cyberprzestrzeni Unii Europejskiej jest różnego rodzaju złośliwe oprogramowanie (*malware*), a jego czołowa pozycja w stosunku do 2017 r. nie uległa zmianie. Według autorów raportu w 2018 r. liczba ataków z użyciem wirusów miała pozostać na niezmienionym poziomie. W dalszej kolejności (poz. 2 i 3) dominują ataki internetowe lub z użyciem aplikacji internetowych. W raporcie wskazano na nasilenie trzech rodzajów ataków: ataków typu „odmowa dostępu" (*denial of service*), botnets, naruszenia danych (*data breaches*) (wzrost w rankingu w stosunku do 2017 r.). W porównaniu z 2017 r. sześć rodzajów ataków nie nasiliło się, a w odniesieniu do jednego (spam) wskazano spadek.

Dla porównania: w Polsce z *Raportu rocznego z działalności CERT Polska 2018*[32] wynika, że utrzymuje się tendencja wzrostowa w liczbie zgłoszeń incydentów. W stosunku do 2017 r. liczba zarejestrowanych incydentów była większa o 17,5% i wyniosła 3739. Trzy czwarte z nich dotyczyło osób fizycznych lub podmiotów prywatnych. Trzy najczęściej występujące typy incydentów

31 A. Kopciuch, *Grupy cyberprzestępcze*, Fundacja Bezpieczna Cyberprzestrzeń, 12 lutego 2019 r., https://www.cybsecurity.org/pl/grupy-cyberprzestepcze/ [dostęp: 1 czerwca 2020 r.].

32 NASK/CERT Polska, *Raport roczny z działalności CERT Polska 2018. Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf [dostęp: 1 czerwca 2020 r.].

**Tabela 5. Ranking najczęstszych 10 rodzajów zagrożeń w cyberprzestrzeni Unii Europejskiej w 2018 r.**

| Lp. | Rodzaje zagrożeń w cyberprzestrzeni UE w 2018 | Zmiana w rankingu do 2017 |
|---|---|---|
| 1 | Złośliwe oprogramowanie (malware) | → |
| 2 | Ataki internetowe (web based attacks) | → |
| 3 | Ataki aplikacji internetowych (web application attacks) | → |
| 4 | Wyłudzanie informacji (phishing) | → |
| 5 | Atak typu „odmowa dostępu" (denial of service) | ↑ |
| 6 | Spam | ↓ |
| 7 | Botnets | ↑ |
| 8 | Naruszenie danych (data breaches) | ↑ |
| 9 | Zagrożenia wewnętrzne (insider threat) | → |
| 10 | Zniszczenia fizyczne (physical manipulation/damage/theft/loss) | → |

Legenda: Zmiana w rankingu do 2017 r.: ↑ – wzrost; → – bez zmian; ↓ – spadek.
Źródło: Opracowanie własne na podstawie: European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2018*, January 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018 [dostęp: 1 czerwca 2020 r.].

**Tabela 6. Ranking najczęstszych 10 rodzajów zagrożeń w cyberprzestrzeni Polski w 2018 r.**

| Lp. | Rodzaje zagrożeń w cyberprzestrzeni Polski w 2018 | Zmiana w rankingu do 2017 |
|---|---|---|
| 1 | Oszustwa komputerowe (w tym phishing) | → |
| 2 | Złośliwe oprogramowanie (w tym wirusy) | → |
| 3 | Obraźliwe i nielegalne treści (w tym spam) | → |
| 4 | Próby włamań (w tym wykorzystanie znanych luk internetowych) | → |
| 5 | Włamania | ↑ |
| 6 | Gromadzenie informacji (w tym skanowanie) | ↓ |
| 7 | Podatne usługi (w tym otwarte serwisy podatne na nadużycia) | ↑ |
| 8 | Dostępność zasobów (w tym ataki denial of service) | ↓ |
| 9 | Ataki na bezpieczeństwo informacji | ↑ |
| 10 | Inne | ↓ |

Legenda: Zmiana w rankingu do 2017 r.: ↑ – wzrost; → – bez zmian; ↓ – spadek.
Źródło: Opracowanie własne na podstawie: NASK/CERT Polska, *Raport roczny z działalności CERT Polska 2018. Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf [dostęp: 1 czerwca 2020 r.]; NASK/CERT Polska, *Raport roczny z działalności CERT Polska 2017. Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/PDF/Raport_CP_2017.pdf [dostęp: 1 czerwca 2020 r.].

to oszustwa komputerowe (w tym phishing), dystrybucja złośliwego oprogramowania oraz obraźliwe i nielegalne treści (w tym spam)[33].

W tabelach 5 i 6 widać występowanie podobnego rodzaju zagrożeń w cyberprzestrzeni zarówno UE, jak i Polski. W rankingu dominują: złośliwe oprogramowanie, oszustwa komputerowe (w tym phishing) oraz obraźliwe i nielegalne treści (w tym spam). Mają one na celu wpływ na poczucie bezpieczeństwa użytkowników publicznych i prywatnych.

Podsumowując: zagrożenia cyberprzestępczością odnoszą się zarówno do sektora prywatnego, jak i do sektora publicznego. Działania cyberprzestępców są motywowane względami finansowymi, politycznymi i ideologicznymi. Według statystyk najwięcej ataków dotyczy instytucji rządowych, może to jednak też wynikać z coraz większej dostępności oraz wrażliwości danych przechowywanych przez te instytucje. Według prezentowanych raportów wzrasta aktywność grup finansowanych przez państwa, wykorzystujących inżynierię społeczną w celu wpływania na społeczeństwa. Nadal największym zagrożeniem sieci pozostaje złośliwe oprogramowanie (wirusy). Ze względu na brak granic w cyberprzestrzeni istnieją trudności w jednoznacznym określeniu kierunku ataków. Należy zaznaczyć, że ogromna liczba przestępstw komputerowych pozostaje ukryta w szarej strefie i wymyka się wszelkim statystykom, co potęguje zagrożenie[34].

## Finansowanie wydatków na cyberbezpieczeństwo w Polsce na tle UE

Finansowanie cyberbezpieczeństwa w UE i jej państwach członkowskich dokonywane jest zarówno ze środków publicznych, jak i ze środków prywatnych lub przez partnerstwo publiczno-prywatne[35]. Na rysunku 3 przedstawiono trzy główne źródła finasowania cyberbezpieczeństwa.

W pierwszej kolejności cyberbezpieczeństwo w UE jest finansowane ze środków publicznych. Dokonywane jest to bezpośrednio z budżetu Unii Europejskiej i budżetów poszczególnych państw członkowskich. Jako kolejne źródło należy wskazać środki prywatne, czyli wydatki przedsiębiorstw na bezpieczeństwo własne oraz bezpieczeństwo świadczonych usług oraz wydatki konsumentów na przeciwdziałanie atakom cyberprzestępców. Brak jest jednak jednolitego ujęcia w budżetach przedsiębiorstw, aby przeprowadzić porównania. Cyberbezpieczeństwo finansowane jest również przez partnerstwo publiczno-prywatne. Dotyczy to przede wszystkim organizacji pozarządowych (np. European Cyber Security Organisation) działających w celu wspierania współpracy między podmiotami publicznymi i prywatnymi. W niniejszym opracowaniu zajmiemy się finansowaniem ze środków publicznych z budżetu państwa.

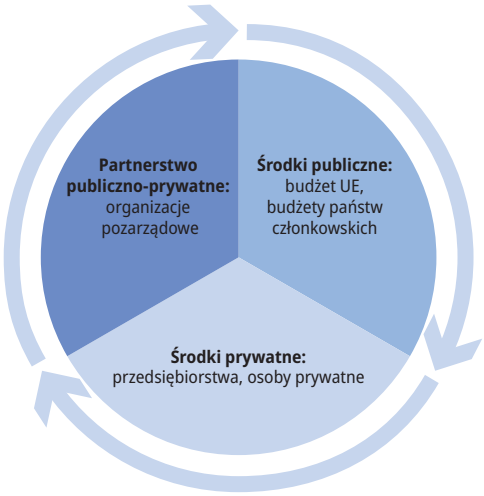
---

33 *Ibidem*, s. 6.

34 M. Kliś, *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000, http://prawo.vagla.pl/node/905 [dostęp: 1 czerwca 2020 r.].

35 Jednym z postulatów komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego oraz Komitetu Regionów, Otwarta i bezpieczna Europa: realizacja założeń (COM(2014) 154 final z 11 marca 2014 r.) jest zacieśnienie współpracy z sektorem prywatnym; za: Z. Chmielewski, *op. cit.*, s. 115.

**Rysunek 3. Finansowanie cyberbezpieczeństwa w Unii Europejskiej**




Źródło: Opracowanie własne na podstawie: Ministerstwo Cyfryzacji, *Krajowe Ramy...*

W latach 2014–2018 Komisja Europejska wydała ponad 1,4 mld euro na wdrożenie strategii pn. „Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii"[36], przy czym największa część tej kwoty przypadła na program „Horyzont 2020"[37]. W ramach tego programu zaplanowano 279 projektów dotyczących cyberbezpieczeństwa, w których zawarto umowy w okresie do września 2018 r. Na wykresie 2 przedstawiono projekty badawcze dotyczące cyberbezpieczeństwa, dla których zawarto umowy w ramach programu „Horyzont 2020" (w mln euro).

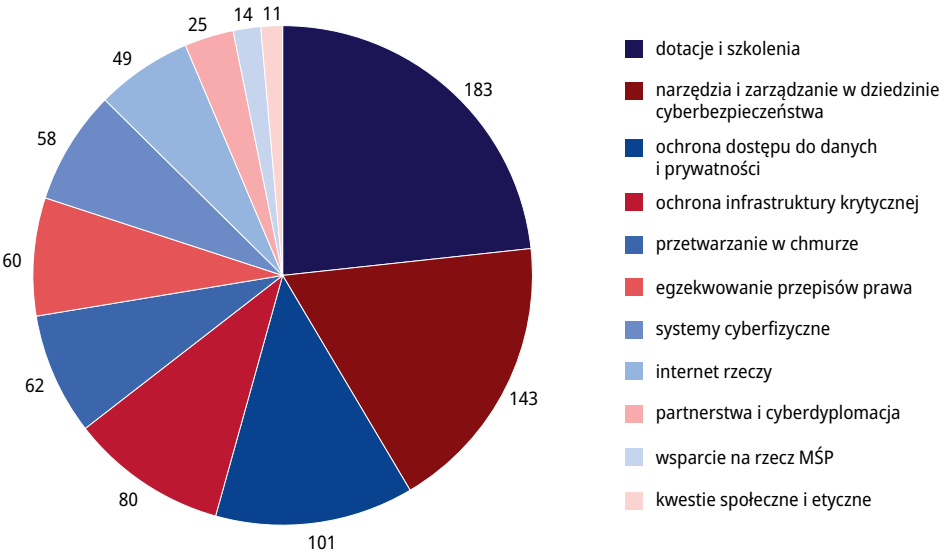
Ponadto w ramach programu „Horyzont 2020" wydatkowano kwotę 67,5 mln euro na partnerstwo publiczno-prywatne, gdzie sektor prywatny zainwestował kwotę 1 mld euro. Środki z tego programu udostępniono również w kwocie 437 mln euro na przedsięwzięcie „Podzespoły i układy elektroniczne w służbie wiodącej pozycji Europy".

Poza projektem „Horyzont 2020" zwalczanie cyberprzestępczości zostało wsparte z innych źródeł finansowania. Główne wydatki Unii Europejskiej na cyberbezpieczeństwo poza wymienionym programem przedstawiono w tabeli 7.

36 Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, COM(2017) 476 final, Bruksela, 4 października 2017 r.

37 Europejski Trybunał Obrachunkowy, *Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją. Dokument analityczny*, marzec 2019 r., https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PL.pdf [dostęp: 1 czerwca 2020 r.].

**Wykres 2. Projekty badawcze dotyczące cyberbezpieczeństwa w ramach programu „Horyzont 2020" (w mln euro)**




Źródło: Opracowanie własne na podstawie: Europejski Trybunał Obrachunkowy, *Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją. Dokument analityczny*, marzec 2019 r., https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PL.pdf [dostęp: 1 czerwca 2020 r.].

Należy podkreślić, że UE nie wykształciła jeszcze jednolitego systemu ujmowania wydatków na cyberbezpieczeństwo. Raporty z wykonania budżetu Unii Europejskiej oraz Polski wskazują brak przypisania zagregowanych wydatków na cyberbezpieczeństwo. Sytuacja ta wynika z przypisania ich do różnorodnych obszarów, takich jak technologie cyfrowe, digitalizacja, rozwój, gospodarka, nauka, bezpieczeństwo i obrona, co utrudnia dokładne określenie, w jakiej wysokości następuje finasowanie systemu cyberbezpieczeństwa. Dostępne raporty wskazują, że wydatki w UE były niskie, rozproszone, często niepoparte skoordynowanymi programami rządowymi oraz trudne do odróżnienia[38].

Ważną kwestią poznawczą dla oceny poziomu wydatków ze środków publicznych na funkcjonowanie systemu cyberbezpieczeństwa jest określenie gotowości do ponoszenia tych wydatków na podstawie wybranych danych budżetowych oraz wskaźników. Najczęściej wykorzystywane do analizy wydatków publicznych na cyberbezpieczeństwo dane budżetowe i wskaźniki przedstawia tabela 8.

38 Zob. European Court of Auditors, *Challenges to effective EU cybersecurity policy*, Briefing Paper, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf. [dostęp: 1 czerwca 2020 r.].

**Tabela 7. Wybrane źródła finansowania zwalczania cyberprzestępczości w Unii Europejskiej**

| Lp. | Źródło finansowania | Okres | Kwota wydatków | Cel |
|---|---|---|---|---|
| 1 | Fundusz Bezpieczeństwa Wewnętrznego | 2014–2017 | 62 mln euro | badania, spotkania ekspertów i działania informacyjne w ramach współpracy policyjnej |
| 2 | Dyrekcja Generalna ds. Sprawiedliwości i Konsumentów | – | 9 mln euro | wsparcie współpracy sądowej i funkcjonowania traktatów o wzajemnej pomocy prawnej |
| 3 | Instrument „Łącząc Europę" | 2016–2018 | 13 mln euro | wsparcie wdrażania wymogów dyrektywy |
| 4 | Unijny Instrument na rzecz Przyczyniania się do Stabilności i Pokoju | 2014–2018 | 50 mln euro | cyberbezpieczeństwo poza UE |
| 5 | Europejskie fundusze strukturalne i inwestycyjne | – | 400 mln euro | zwiększenie interoperacyjności i wzajemnych połączeń infrastruktury cyfrowej, identyfikacji elektronicznej, ochrony prywatności i usług zaufania |
| 6 | Europejski Bank Inwestycyjny | 2018–2020 | 6 mld euro | zwiększenie finansowania na rzecz technologii podwójnego zastosowania, cyberbezpieczeństwa i cywilnego sektora bezpieczeństwa |

Źródło: Opracowanie własne na podstawie: Europejski Trybunał Obrachunkowy, *op. cit.*

**Tabela 8. Najczęściej wykorzystywane zmienne i wskaźniki do określenia gotowości do ponoszenia wydatków na cyberbezpieczeństwo**

| Lp. | Rodzaj danych lub wskaźnika | Opis |
|---|---|---|
| 1 | Wydatki na obronność | dane dla 27 państw członkowskich Europejskiej Agencji Obrony na podstawie danych European Defence Agency |
| 2 | Wydatki na obronność jako % PKB | dane dla 27 państw członkowskich Europejskiej Agencji Obrony na podstawie danych European Defence Agency |
| 3 | Wydatki na badania i rozwój jako % wydatków na obronę | dane dla 27 państw członkowskich Europejskiej Agencji Obrony na podstawie danych European Defence Agency |
| 4 | Udział sektora ICT (sektor związany z technologiami informacyjno-komunikacyjnymi) jako % PKB | dane dla 27 państw członkowskich Europy na podstawie danych Eurostat |

Źródło: Opracowanie własne na podstawie: J. Antczak, K. Kamiński, *Cybersecurity Expenditure in the EU Member States*, New Direction, https://newdirection.online/2018-publications-pdf/CYBERSECURITY.pdf [dostęp: 1 czerwca 2020 r.].

Dynamika zaprezentowanych danych i wskaźników w tabeli 8 wskazuje pośrednio, czy występuje zależność pomiędzy wydatkami a efektami działań krajowego systemu cyberbezpieczeństwa.

Wydatki na obronność – jako jedna z głównych zmiennych finansowania walki z cyberprzestępczością w ramach Unii Europejskiej i Polski – zostały przedstawione łącznie dla 27 państw

**Tabela 9. Łączne wydatki na obronność w 27 państwach członkowskich Europejskiej Agencji Obrony w latach 2013–2018 (w euro)**

| Lp. | 27 członków Europejskiej Agencji Obrony | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|
| 1 | Łączne wydatki na obronność | 190 434 mln | 194 782 mln | 204 280 mln | 205 562 mln | 214 662 mln | 223 413 mln |
| 2 | Wydatki na obronność jako % PKB | 1,4% | 1,4% | 1,4% | 1,4% | 1,4% | 1,4% |
| 3 | Wydatki na obronność w wydatkach rządowych | 2,9% | 3,0% | 3,0% | 3,0% | 3,1% | 3,1% |
| 4 | Wydatki na obronność na 1 mieszkańca | 380 | 388 | 405 | 407 | 424 | 440 |
| 5 | Wydatki na badania i rozwój w ramach wydatków na obronność | 7579 mln | 8791 mln | 9211 mln | 7221 mln | 7789 mln | 8764 mln |
| 6 | Udział % wydatków na badania i rozwój w ramach wydatków na obronność | 4,0% | 4,5% | 4,5% | 3,5% | 3,6% | 3,9% |

Źródło: Opracowanie własne na podstawie: https://www.eda.europa.eu/info-hub/defence-data-portal [dostęp: 1 czerwca 2020 r.].

**Tabela 10. Wydatki na obronność w Polsce w latach 2013–2018 (w euro)**

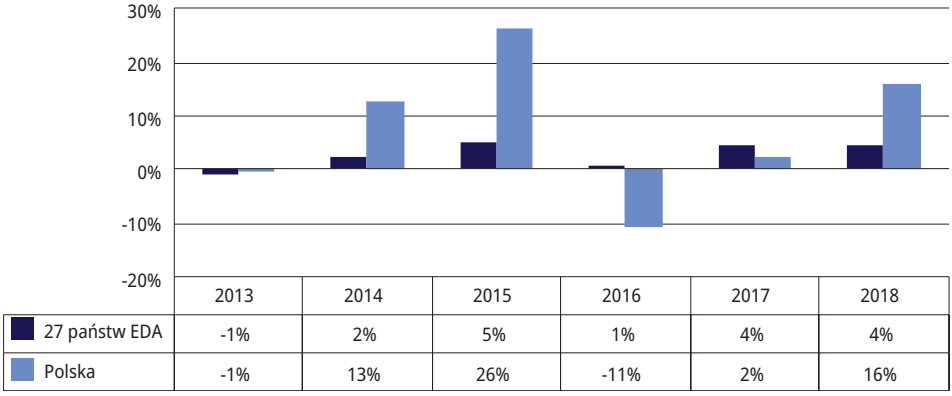
| Lp. | Polska | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|---|
| 1 | Łączne wydatki na obronność | 6720 mln | 7565 mln | 9546 mln | 8500 mln | 8683 mln | 10 052 mln |
| 2 | Wydatki na obronność jako % PKB | 1,7% | 1,8% | 2,2% | 2,0% | 1,9% | 2,0% |
| 3 | Wydatki na obronność w wydatkach rządowych | 4,0% | 4,4% | 5,3% | 4,9% | 4,5% | 4,9% |
| 4 | Wydatki na obronność na 1 mieszkańca | 175 | 197 | 248 | 221 | 226 | 262 |
| 5 | Wydatki na badania i rozwój w ramach wydatków na obronność | 94,3 mln | 217,2 mln | 156,7 mln | 138,9 mln | 259,9 mln | 248,4 mln |
| 6 | Udział % wydatków na badania i rozwój w ramach wydatków na obronność | 1,4% | 2,9% | 1,6% | 1,6% | 3,0% | 2,5% |

Źródło: Opracowanie własne na podstawie: https://www.eda.europa.eu/info-hub/defence-data-portal [dostęp: 1 czerwca 2020 r.].

członkowskich Europejskiej Agencji Obrony oraz dla Polski w latach 2013–2018 odpowiednio w tabeli 9 i tabeli 10.

Analiza wydatków na obronność w państwach UE (tabela 9) wskazuje na ich systematyczny wzrost średnio o 3% rocznie. Dynamika przyrostów rocznych (wykres 3) wahała się od spadku o 1% w 2013 r. do wzrostu rzędu 5% w 2015 r. Wydatki na obronność w państwach UE w 2018 r. były wyższe o 32 979 mln euro niż w 2013 r. Średnia wysokość wydatków na obronność w badanych latach wynosiła 205,5 mld euro. W analizowanym okresie średni udział procentowy wydatków na obronność w PKB wynosił 1,4%, a w wydatkach rządowych 3%. Przeliczając wydatki na obronność na osobę w państwach UE wyniosły one średnio 407 euro.

**Wykres 3. Dynamika wzrostu wydatków na obronność w Polsce i w państwach UE w latach 2013–2018**



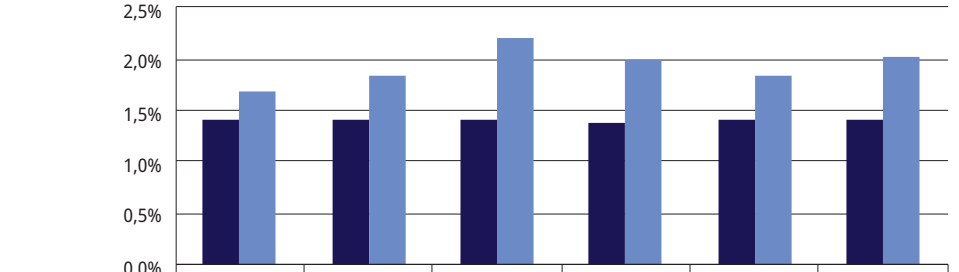

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| 27 państw EDA | -1% | 2% | 5% | 1% | 4% | 4% |
| Polska | -1% | 13% | 26% | -11% | 2% | 16% |

Źródło: Opracowanie własne na podstawie: https://www.eda.europa.eu/info-hub/defence-data-portal [dostęp: 1 czerwca 2020 r.].

W tym samym okresie (tabela 10) wydatki na obronność w Polsce rosły średnio o 8%. W porównaniu z 2013 r. w 2018 r. wydatki wzrosły o 3,3 mld euro. W badanym okresie występują jednak znaczne wahania przyrostów rocznych (wykres 3) od spadku o 11% w 2016 r. do wzrostu o 26% w 2015 r. Średnia wysokość wydatków na obronność w Polsce wynosiła 8,5 mld euro i stanowiła średnio 1,9% PKB oraz 4,7% wydatków rządowych. Wydatki na obronność w przeliczeniu na osobę wyniosły w Polsce średnio 221 euro.

Porównanie wydatków na obronność w państwach członkowskich UE i w Polsce (tabela 9 i tabela 10) ukazuje, że zarówno w UE, jak i w Polsce na przestrzeni lat 2013–2018 wydatki te rosły. Średnia roczna dynamika wzrostu wydatków w ujęciu kwotowym w Polsce była prawie trzykrotnie wyższa niż w państwach UE. Jednocześnie w państwach członkowskich Europejskiej Agencji Obrony wydatki na obronność w badanym okresie stanowiły średnio 1,4% PKB, a w Polsce 1,9% PKB. Przy tym w przypadku Polski (wykres 4) udział procentowy w PKB wahał się od 1,7% do 2,2%. Średni udział wysokości wydatków na obronność w ramach środków budżetowych

**Wykres 4. Udział wydatków na obronność w PKB w Polsce i w państwach UE**




| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| 27 państw EDA | 1,4% | 1,4% | 1,4% | 1,4% | 1,4% | 1,4% |
| Polska | 1,7% | 1,8% | 2,2% | 2,0% | 1,9% | 2,0% |

Źródło: Opracowanie własne na podstawie: https://www.eda.europa.eu/info-hub/defence-data-portal [dostęp: 1 czerwca 2020 r.].

w Polsce był wyższy od średniej państw UE o ok. 50%, kiedy jednak porównamy średnie wydatki *per capita*, to w państwach UE są one prawie dwukrotnie wyższe niż w Polsce.

W obszarze zmian w nakładach związanych z cyberbezpieczeństwem istotnym aspektem jest ewolucja wydatków na badania i rozwój w ramach wydatków na obronność. W państwach członkowskich UE stanowiły one średnio 4% wydatków na obronność, a średnia wysokość wydatków wynosiła 8,2 mld euro (tabela 9). Z wykresu 5 wynika, że dynamika wydatków rok do roku w państwach UE wahała się od – 22% do + 16% przy średniej wartości dla badanego okresu 4%.

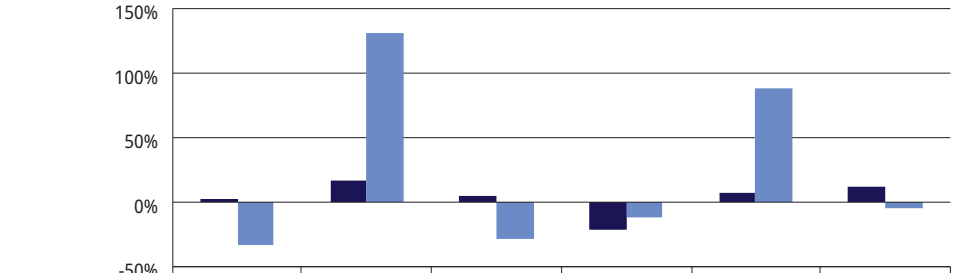
Natomiast w Polsce zgodnie z tabelą 10 udział wydatków na badania i rozwój w ramach wydatków na obronność stanowił średnio 2%, a średnia wysokość wydatków wynosiła 185,9 mln euro. Zauważalna jest też duża rozpiętość w dynamice wydatków rok do roku, bo od – 34% do + 130% przy średniej w wysokości 23%. Daje to prawie sześciokrotnie większą średnią niż w państwach UE.

Jeżeli porównać wydatki na badania i rozwój w ramach wydatków na obronność, zauważalna jest duża zmienność w relacji rok do roku zarówno w państwach UE, jak i w Polsce.

Kolejnym wskaźnikiem, pośrednio wskazującym na gotowość do ponoszenia wydatków na cyberbezpieczeństwo przez państwo, jest udział sektora ICT[39] w PKB. Sektor ten odgrywa strategiczną rolę w promowaniu wzrostu, innowacji i konkurencyjności we wszystkich gospodarkach europejskich, również w zakresie cyberbezpieczeństwa. Udział sektora ICT w latach 2013–2018 w PKB przedstawiono na wykresie 6. Ze względu na utajnienie danych przez niektóre państwa prezentacji dokonano na podstawie dostępnych danych.

39 Sektor ICT – branża gospodarki obejmująca przedsiębiorstwa, których głównym rodzajem działalności jest produkcja dóbr i usług pozwalających na elektroniczne rejestrowanie, przetwarzanie, transmitowanie, odtwarzanie lub wyświetlanie informacji; za: Główny Urząd Statystyczny, https://stat.gov.pl/metainformacje/slownik-pojec/pojecia-stosowane-w-statystyce-publicznej/1858,pojecie.html [dostęp: 1 czerwca 2020 r.].

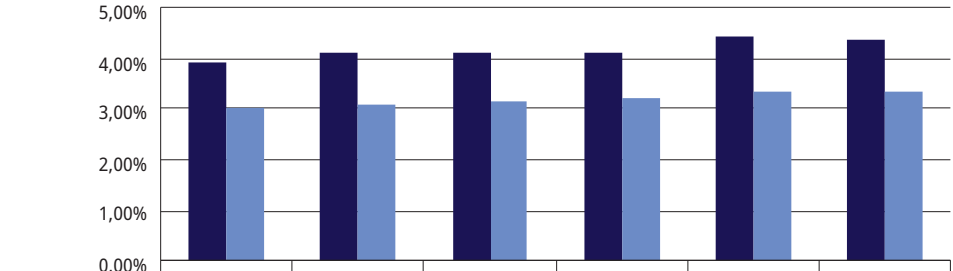
**Wykres 5. Dynamika wydatków na badania i rozwój w ramach wydatków na obronność w Polsce i w państwach UE**




| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| 27 państw EDA | 2% | 16% | 5% | -22% | 8% | 13% |
| Polska | -34% | 130% | -28% | -11% | 87% | -4% |

Źródło: Opracowanie własne na podstawie: https://www.eda.europa.eu/info-hub/defence-data-portal [dostęp: 1 czerwca 2020 r.].

**Wykres 6. Udział sektora ICT w PKB w państwach UE oraz w Polsce**



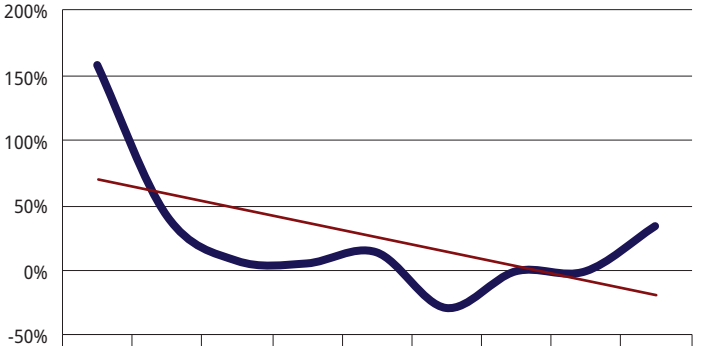

| | 2013 | 2014 | 2015 | 2016 | 2017 | 2018 |
|---|---|---|---|---|---|---|
| 27 państw UE | 3,91% | 4,09% | 4,10% | 4,11% | 4,39% | 4,35% |
| Polska | 3,01% | 3,05% | 3,15% | 3,22% | 3,33% | 3,32% |

Źródło: Opracowanie własne na podstawie: http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ag&lang=en [dostęp: 1 czerwca 2020 r.]; dane dot. 2018 r. oszacowano za pomocą funkcji liniowej na podstawie lat poprzednich.

Udział sektora ICT w PKB rośnie z roku na rok zarówno w państwach członkowskich UE, jak i w Polsce. Średni udział sektora ICT w PKB w gospodarce państw UE wyniósł 4,14% i jest prawie o 1 punkt procentowy większy niż w Polsce (3,17%).

Przedstawione zmienne i wskaźniki wskazują na zwiększanie wydatków na walkę z cyberprzestępczością w ramach budżetu Polski. Ciągle jednak mamy niższy udział sektora ICT w PKB. W zestawieniu w ramach państw Unii Europejskiej Indeksu gospodarki cyfrowej i społe-

**Wykres 7. Dynamika wydatków na cyberbezpieczeństwo w Polsce**




| | 2019 | 2020 | 2021 | 2022 | 2023 | 2024 | 2025 | 2026 | 2027 |
|---|---|---|---|---|---|---|---|---|---|
| Roczny przyrost wydatków | 158% | 42% | 8% | 6% | 15% | -28% | 0% | 0% | 35% |

Źródło: Opracowanie własne na podstawie: art. 93 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa.

czeństwa cyfrowego (DESI)[40] Polska w 2018 r. zajmowała 24. miejsce w grupie 28 państw członkowskich UE i utrzymywała pozycję z DESI 2017. Z upływem czasu czyni stałe postępy w zakresie parametrów DESI w takim samym tempie, jakie odnotowano dla całej Unii Europejskiej[41].

Kluczowe w zakresie finansowania cyberbezpieczeństwa w Polsce stało się wprowadzenie w życie ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r., na mocy której podmioty realizujące zadania publiczne są zobowiązane do ujmowania w swoich planach finansowych nakładów na cyberbezpieczeństwo. Koszty te powiększą się o nakłady przeznaczone na działania integracyjne związane z budową krajowego systemu cyberbezpieczeństwa oraz o nakłady ponoszone na realizację pozostałych przedsięwzięć planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa. Źródłami finansowania realizacji działań opisanych w dokumencie będą plany finansowe poszczególnych jednostek zaangażowanych we wdrażanie Krajowych Ram Polityki Cyberbezpieczeństwa, a także środki pochodzące z Narodowego Centrum Badań i Rozwoju oraz środki Unii Europejskiej, w miarę zaistnienia takich możliwości[42]. Ustawa o krajowym systemie cyberbezpieczeństwa jest właściwe jedynym dokumentem w Polsce określającym wprost limity wydatków na ochronę cyberprzestrzeni. Zgodnie z planem na lata 2018–2027 Polska planuje przeznaczyć 235 931 tys. zł na budowę i utrzymanie krajowego

40 Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) to złożony indeks, który podsumowuje odpowiednie wskaźniki wydajności cyfrowej Europy i śledzi ewolucję państw członkowskich UE w zakresie konkurencyjności cyfrowej.

41 Komisja Europejska, *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) 2018. Sprawozdanie krajowe dotyczące Polski*, s. 2, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52340 [dostęp: 1 czerwca 2020 r.].

42 Ministerstwo Cyfryzacji, *Krajowe Ramy...*, s. 24.

sytemu cyberbezpieczeństwa. Dynamika wydatków jest jednak znacząco różna w poszczególnych latach, co przedstawia wykres 7.

Analiza wielkości planowanych wydatków na cyberbezpieczeństwo wskazanych w art. 93 ustawy o krajowym systemie cyberbezpieczeństwa, których dynamikę przedstawia wykres 7, wykazuje ich trend malejący w latach 2019–2027. Średnia dynamika wydatków w latach 2019–2027 wynosi 5% corocznego wzrostu. Jednakże uwagę zwracają wprowadzone w ustawie o krajowym systemie cyberbezpieczeństwa mechanizmy korygujące polegające na ograniczeniu wydatków, a co za tym idzie – działań na rzecz cyberbezpieczeństwa.

Wydaje się, że w przypadku pogorszenia sytuacji budżetowej może to doprowadzić do kolejnych cięć środków, co na pewno nie przełoży się na rozwój systemu. Na ten aspekt zwróciła uwagę Polska Izba Informatyki i Telekomunikacji w petycji do Ministra Cyfryzacji o podjęcie działań zmierzających do zwiększenia środków na ochronę cyberbezpieczeństwa Polski. Postawiła też pytanie: Jaki sens ma określanie górnego pułapu wydatków na cyberbezpieczeństwo w warunkach stałego zagrożenia incydentami, a zwłaszcza przeciwdziałania incydentom krytycznym?[43]

Przedstawione powyżej prognozy wzrostu wydatków na cyberbezpieczeństwo w Polsce (5%) są o połowę mniejsze od prognozy całego rynku (10%)[44]. W świetle wprowadzonych ograniczeń wydatków budżetowych wzbudza to uzasadnione obawy co do możliwości zapewnienia przez państwo odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni w kolejnych latach.

## Podsumowanie

Można obecnie zaobserwować eksplozję rozwoju technologii informatycznych i telekomunikacyjnych, przenikających nieomal każdą dziedzinę naszego życia, dlatego cyberbezpieczeństwo stanowi krytyczny obszar z punktu widzenia państwa i obywateli[45]. Również doświadczenia pandemii COVID-19 wyraźnie wskazują na zmianę trendów w zakresie cyfryzacji gospodarki i życia społecznego. Nie zmienia się lista zagrożeń, ale zmieniają się sposoby działania, siła ataków, jak też ich waga.

W Unii Europejskiej Polska została zaliczona do grupy osiągającej niskie wyniki w ramach Indeksu gospodarki cyfrowej i społeczeństwa cyfrowego (DESI)[46], co oznacza, że nie rozwijamy się pod względem cyfrowym szybciej niż pozostali członkowie UE. Jednakże według rankingu[47] e-Governance Academy, mierzącego stopień gotowości państw do zapobiegania zagrożeniom cybernetycznym i zarządzania incydentami cybernetycznymi, a tym samym gotowości partycypacji w kosztach ponoszonych na wzmocnienie cyberbezpieczeństwa, w 2018 r. Polska

43 CyberDefence24, *Polska musi zwiększyć wydatki na cyberbezpieczeństwo*, https://www.cyberdefence24.pl/polska-musi-zwiekszyc-wydatki-na-cyberbezpieczenstwo [dostęp: 1 czerwca 2020 r.].

44 Zob. Instytut Kościuszki oraz Investin, *Europejski Rynek Cyberbezpieczeństwa. Potencjał Regionu Trójmorza*, Kraków 2018, s. 5 https://ik.org.pl/wp-content/uploads/europejski_rynek_cyberbezpieczenstwa_online.pdf [dostęp: 1 czerwca 2020 r.].

45 CyberDefence24, *op. cit.*

46 Komisja Europejska, *Indeks gospodarki cyfrowej…*, s. 2.

47 R. Rikk, *National Cyber Security Index 2018*, e-Governance Academy, Tallinn 2018, s. 9, https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf [dostęp: 1 czerwca 2020 r.].

zajmowała 15. miejsce na świecie oraz 13. w państwach członkowskich UE i osiągnęła National Cyber Security Index (NCSI) na poziomie 67,53. Autorzy raportu na podstawie porównania NCSI z Digital Development Level (DDL – Poziom Rozwoju Cyfrowego) określili, że w Polsce poziom cyberbezpieczeństwa wyprzedza nieznacznie poziom obecnego rozwoju cyfrowego[48].

Zachowanie cyberbezpieczeństwa jest dobrem publicznym, toteż jego finansowanie w UE i w jej państwach członkowskich jest dokonywane zarówno ze środków publicznych, jak i ze środków prywatnych lub przez partnerstwo publiczno-prywatne. Włączenie sektora prywatnego w finansowanie obszaru cyberbezpieczeństwa wiąże się ze współdziałaniem pomiędzy sektorem prywatnym a sektorem publicznym, lecz także ze współdziałaniem w ramach samego sektora prywatnego, np. sektora finansowego. Niezbędne jest więc uregulowanie zasad współpracy pomiędzy zaatakowanymi bankami mimo ich konkurowania ze sobą w świadczeniu usług bankowych[49]. Wydatki na cyberbezpieczeństwo rosną szybciej niż cały rynek ICT. Według szacunków przedsiębiorstw doradczych w latach 2015–2020 branża ta będzie rosnąć globalnie w tempie prawie 10% rocznie, by na koniec dekady osiągnąć wartość 170 mld dolarów, z czego na rynek europejski ma przypadać 38 mld dolarów[50]. Tylko w ramach programu „Digital Europe programme for the period 2021–2027", który ma m.in. zapewnić wdrożenie dyrektywy NIS[51], planowane są wydatki od 1 do 2 miliardów euro.

Należy zaznaczyć, że precyzyjne określenie wydatków na cyberbezpieczeństwo nie jest zadaniem prostym. Ze względu na brak jednoznacznych danych i utajnianie części działań przez państwa członkowskie konieczne jest wykorzystywanie pośrednich wskaźników. Zaprezentowana analiza jednak wskazuje, że zarówno w państwach członkowskich UE, jak i w Polsce rosną wydatki związane pośrednio z cyberbezpieczeństwem. Wydatki na obronność, w tym na badania i rozwój, cechują się przy tym bardzo dużym zróżnicowaniem pod względem dynamiki w stosunku do wzrostu sektora ICT. Przy tak dynamicznym rozwoju technologii nie wydaje się właściwe – z punktu widzenia cyberbezpieczeństwa w Polsce – umieszczenie w przepisach[52] limitów dotyczących przyszłych wydatków budżetowych na walkę z cyberprzestępczością. Może to skutkować narażeniem na ataki zewnętrzne oraz podważać poczucie bezpieczeństwa życia i prowadzenia biznesu. Dalszy zaplanowany wzrost wydatków na cyberbezpieczeństwo w ramach budżetu państwa (5%) jest mniejszy niż prognozy rynkowe[53].

Skoro nakłady na cyberbezpieczeństwo w Polsce ze strony budżetu nie odpowiadają tendencji występującej w państwach UE i na świecie, to kluczowe jest zadbanie o pozyskanie pomocowych środków zewnętrznych do wykorzystania zarówno przez organy państwowe, jak i przez sektor prywatny, tak aby stworzyć komplementarny system cyberbezpieczeństwa.

---

48 *Ibidem*. Różnica między poziomem NCSI 67,53 a poziomem DDL 66,59 wynosi 0,94.

49 M. Staszczyk, *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, „Finanse i Prawo Finansowe" 2015, t. 2, nr 1, s. 53, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.hdl_11089_9267/c/4_Staszczyk.pdf. [dostęp: 1 czerwca 2020 r.].

50 Instytut Kościuszki oraz Investin, *op. cit.*, s. 5.

51 European Court of Auditors, *op. cit.*, s. 26.

52 Art. 93 ustawy o krajowym systemie cyberbezpieczeństwa.

53 Zob. Instytut Kościuszki oraz Investin, *op. cit.*, s. 5.

## Bibliografia


Ahmad A., Ahmad N., Ali S., *Crime and Economic Growth in Developing Countries: Evidence from Pakistan*, "Journal of Basic and Applied Scientific Research" 2014, nr 4, https://www.researchgate.net/profile/Sharafat_Ali3/publication/275019421_Crime_and_Economic_Growth_in_Developing_Countries_Evidence_from_Pakistan/links/552e67070cf2acd38cb93de5.pdf.

Antczak J., Kamiński K., *Cybersecurity Expenditure in the EU Member States*, New Direction, https://newdirection.online/2018-publications-pdf/CYBERSECURITY.pdf.

Bay M., *What is cybersecurity? In search of an encompassing definition for the post-Snowden era*, "French Journal For Media Research" 2016, nr 6, https://www.researchgate.net/publication/308609163_WHAT_IS_CYBERSECURITY_In_search_of_an_encompassing_definition_for_the_post-Snowden_era.

Blackburn K., Neanidis K.C., Rana, M.P., *A theory of organized crime, corruption and economic growth*, "Economic Theory Bulletin" 2017, nr 5, https://doi.org/10.1007/s40505-017-0116-5.

Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, nr 2(10), https://ssl-kolegia.sgh.waw.pl/pl/KES/czasopisma/kwartalnik_szpp/Documents/2(10)%202016/066_05_Chmielewski.pdf.

Cukier M., *Study: Hackers Attack Every 39 Seconds*, A.J. Clark School of Engineering, 9 lutego 2007 r., https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds.

CyberDefence24, *Polska musi zwiększyć wydatki na cyberbezpieczeństwo*, https://www.cyberdefence24.pl/polska-musi-zwiekszyc-wydatki-na-cyberbezpieczenstwo.

Detotto C., Otranto E., *Does Crime Affect Economic Growth?*, "Kyklos. International Review for Social Sciences" 2010, t. 63, nr 3, Wiley Blackwell, https://doi.org/10.1111/j.1467-6435.2010.00477.x.

European Commission, *Cybersecurity Strategy of the European Union. An Open, Safe and Secure Cyberspace*, Brussels, 7.02.2013, http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667.

European Court of Auditors, *Challenges to effective EU cybersecurity policy*, Briefing Paper, March 2019, https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf.

European Union Agency for Network and Information Security, *Definition of Cybersecurity. Gaps and overlaps in standardisation*, December 2015, https://www.enisa.europa.eu/publications/definition-of-cybersecurity.

European Union Agency for Network and Information Security, *ENISA Threat Landscape Report 2018*, January 2019, https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018.

Europejski Trybunał Obrachunkowy, *Unijna polityka cyberbezpieczeństwa – wyzwania związane ze skuteczną realizacją. Dokument analityczny*, marzec 2019 r., https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PL.pdf.

Gibson W., *Neuromancer*, tłum. P.W. Cholewa, Książnica, Katowice 2009.

Instytut Kościuszki oraz Investin, *Europejski Rynek Cyberbezpieczeństwa. Potencjał Regionu Trójmorza*, Kraków 2018, https://ik.org.pl/wp-content/uploads/europejski_rynek_cyberbezpieczenstwa_online.pdf.

Interpol, *Cyberattacks know no borders and evolve at a rapid pace*, https://www.interpol.int/Crimes/Cybercrime.

Janowski J., *Technological Destabilization of Law* [w:] *Information Technology and Law*, red. W. Cyrul, Wydawnictwo Uniwersytetu Jagiellońskiego, Kraków 2014.

Jaroszewska I.A., *Wybrane aspekty przestępczości w cyberprzestrzeni. Studium prawnokarne i kryminologiczne*, Olsztyn 2017.

Jedlińska R., *Problem przestępczości elektronicznej*, „Ekonomiczne Problemy Usług" 2017, t. 2, nr 1(126), https://doi.org/10.18276/epu.2017.126/2-19.

Kańciak A., *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, http://www.abw.gov.pl/download/1/1719/AKanciak.pdf.

Kliś M., *Przestępczość w Internecie. Zagadnienia podstawowe*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2000, nr 1, Wydawnictwo Polska Akademia Umiejętności, Kraków 2000, http://prawo.vagla.pl/node/905.

Komisja Europejska, *Biała księga w sprawie przyszłości Europy. Refleksje i scenariusze dotyczące przyszłości UE-27 do 2025 r.*, Bruksela 2017, https://ec.europa.eu/commission/sites/beta-political/files/biala_ksiega_w_sprawie_przyszlosci_europy_pl.pdf.

Komisja Europejska, *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego (DESI) 2018. Sprawozdanie krajowe dotyczące Polski*, http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=52340.

Kopciuch A., *Grupy cyberprzestępcze*, Fundacja Bezpieczna Cyberprzestrzeń, 12 lutego 2019 r., https://www.cybsecurity.org/pl/grupy-cyberprzestepcze/.

Kramer F.D., *Cyberpower and National Security: Policy Recommendations for a Strategic Framework* [w:] *Cyberpower and National Security*, red. F.D. Kramer, S.H. Starr, L.K. Wentz, National Defense University Press, Washington, D.C. 2009.

Leszczyński M., *Bezpieczeństwo jako dobro publiczne w społeczeństwie ryzyka*, „Nierówności Społeczne a Wzrost Gospodarczy" 2020, nr 61(1), https://doi.org/10.15584/nsawg.2020.1.8.

McAfee, *The Economic Impact of Cybercrime – No Slowing Down*, February 2018, https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impact-cybercrime.pdf.

Ministerstwo Administracji i Cyfryzacji, *Polityka ochrony cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa, 25 czerwca 2013 r., https://bip.malopolska.pl/e,pobierz,get.html?id=1223287.

Ministerstwo Cyfryzacji, *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022*, Warszawa 2017, https://www.gov.pl/documents/31305/0/krajowe_ramy_polityki_cyberbezpieczenstwa_rzeczypospolitej_polskiej_na_lata_2017_-_2022.pdf/0bbc7a32-64df-b45e-b08c-dac59415f109.

NASK/CERT Polska, *Raport roczny z działalności CERT Polska 2017. Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/PDF/Raport_CP_2017.pdf.

NASK/CERT Polska, *Raport roczny z działalności CERT Polska 2018. Krajobraz bezpieczeństwa polskiego internetu*, https://www.cert.pl/wp-content/uploads/2019/05/Raport_CP_2018.pdf.

Ottis R., Lorents P., *Cyberspace: Definition and Implications* [w:] *Proceedings of the 5th International Conference on Information Warfare and Security 2010, Dayton, Ohio, USA, 8–9 April 2010*, Academic Conferences Limited, Reading, https://www.ccdcoe.org/library/publications/cyberspace-definition-and-implications/.

*Prawne i społeczne aspekty cyberbezpieczeństwa*, red. S. Gwoździewicz, K. Tomaszycki, Międzynarodowy Instytut Innowacji, Warszawa 2017, https://instytutinnowacji.edu.pl/wp-content/uploads/2016/11/PISAC_Druk.pdf.

Rikk R., *National Cyber Security Index 2018*, e-Governance Academy, Tallinn 2018, s. 9, https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf.

Siwicki M., *Cyberprzestępczość*, Wydawnictwo C. H. Beck, Warszawa 2013.

Sławińska M., *Rok funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa – najważniejsze postanowienia i rozwiązania*, Rządowe Centrum Bezpieczeństwa, https://rcb.gov.pl/rok-funkcjonowania-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-najwazniejsze-postanowienia-i-rozwiazania/.

Staszczyk M., *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, „Finanse i Prawo Finansowe" 2015, t. 2, nr 1, http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.hdl_11089_9267/c/4_Staszczyk.pdf.

Wasilewski J., *Przestępczość w cyberprzestrzeni – zagadnienia definicyjne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, http://yadda.icm.edu.pl/yadda/element/bwmeta1.element.desklight-5c76c983-d00f-431d-9e16--6fa0ed5a9f75.

Wasilewski J., *Zarys definicyjny cyberprzestrzeni*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, https://www.abw.gov.pl/download/1/1284/Segregator13.pdf.

## Akty prawne

Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. UE L 2002.201.37).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz.Urz. UE L 2016.194.1).

Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego i Rady: Pełne wykorzystanie potencjału bezpieczeństwa sieci i informacji – zapewnienie skutecznego wdrożenia dyrektywy (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, COM(2017) 476 final, Bruksela, 4 października 2017 r.

Komisja Wspólnot Europejskich, Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości, 2007.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2018, poz. 1560; tekst jednolity: Dz.U. 2020, poz. 1369).

## Strony internetowe

http://appsso.eurostat.ec.europa.eu/nui/show.do?dataset=isoc_bde15ag&lang=en.

https://attack.mitre.org/groups/.

https://stat.gov.pl/.

https://websites.fraunhofer.de/CIPedia/index.php/Cybercrime#Interpol.

https://www.eda.europa.eu/info-hub/defence-data-portal.

https://www.gov.pl/web/cyfryzacja.