KRAJOWA MAPA CYBERBEZPIECZEŃSTWA

RAPORT • LISTOPAD 2022



INSTYTUT PROMYKA

KRAJOWA MAPA CYBERBEZPIECZEŃSTWA

Sławomir Starzec

Instytut im. Kazimierza Promyka

ul. Obozowa 82A/19
01-434 Warszawa
www.instytutpromyka.pl
e-mail: kontakt@instytutpromyka.pl

Copyright ©
Instytut im. Kazimierza Promyka

Warszawa, Czerwiec 2022

Program Rozwoju Organizacji Obywatelskich na lata 2018–2030 PROO

Narodowy Instytut Wolności
Centrum Rozwoju Społeczeństwa Obywatelskiego

Raport powstał dzięki współfinansowaniu ze środków NIW-CRSO w ramach Programu PROO

SPIS TREŚCI

Wprowadzenie 6

Cyberbezpieczeństwo – jako obszar badań 8

Obszary występowania cyberzagrożeń 12

Krajowe dokumenty strategiczne 16

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007 17

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022 z 2013r. 18

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014 21

Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) 23

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020 25

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2013 28

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022 29

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 31

Krajowy System Cyberbezpieczeństwa 34

Wojska Obrony Cyberprzestrzeni 50

Centralne Biuro Zwalczania Cyberprzestępczości 54

Podsumowanie 56

Bibliografia 58

Netografia 61

WPROWADZENIE



Przedmiotem niniejszego opracowania jest analiza stanu krajowego cyberbezpieczeństwa, ze wskazaniem elementów jego ewolucji, zakładanych strategicznych celów dla tego obszaru oraz faktycznego potencjału rozwojowego.

Takie ujęcie tematu ma charakter nowatorski z uwagi na szereg podejmowanych w ostatnim czasie decyzji wynikających z dynamicznej sytuacji międzynarodowej – zwłaszcza sytuacji cyfrowo-konwencjonalnej wojny obronnej Ukrainy z Federacją Rosyjską i pośredniej wojny ekonomiczno-cyfrowej faktycznie toczonej z Federacją Rosyjską w zasadzie od połowy zeszłego roku.

Jeszcze zanim eskalacja tego konfliktu przyjęła formę działań konwencjonalnych na Ukrainie, miał miejsce szereg cybernetycznych ataków mających na celu z jednej strony stworzenie przedpola dla działań konwencjonalnych, z drugiej zarówno przeprowadzenie akcji wywiadowczych i dezinformacyjnych.[1]

Cyberprzestrzeń coraz bardziej staje się realnym polem walki, na którym chociaż faktycznie nie giną żołnierze i nie ma fizycznej utraty terytorium, to jednak trwa bezwzględna walka, m.in. o zasoby informacyjne, prawdziwość i pierwszeństwo przekazywanych informacji, co przekłada się na rzeczywiste bezpieczeństwo Polek i Polaków – zarówno w wymiarze tradycyjnym, jak i cyfrowym. Mając to na uwadze, 8 lutego 2022 r. powołano do życia nowe Siły Obrony Cyberprzestrzeni jako komponent Wojska Polskiego, na czele z gen. bryg. Karolem Molendą, wcześniejszym dyrektorem Narodowego Centrum Bezpieczeństwa Cyberprzestrzeni działającego w strukturze Wojska Polskiego od 2019 roku.

Ekstrapolować należy, że wraz z rosnącymi zagrożeniami cyberprzestrzeni, rozwijać się będą formy prewencyjnego, jak i bezpośredniego przeciwdziałania zarówno w sferze cywilnej jak i wojskowej.

Niniejsze opracowanie stawia sobie także za cel pewne uporządkowanie w sferze terminologicznej, jak i systemowej związanej z cyberbezpieczeństwem, ze szczególnym odniesieniem się do literatury i doktryny przedmiotu.

1 Eksperci z Check Point Research odnotowali 196-procentowy wzrost ataków w ciągu pierwszych dni wojny na ukraiński sektor rządowo-wojskowy. B. Breczko, *Wojna Rosja - Ukraina. Gigantyczny wzrost liczby ataków w internecie,* [na:] https://biznes.wprost.pl/technologie/cyberbezpieczenstwo/10640638/wojna-rosja-ukraina-gigantyczny-wzrost-liczby-atakow-w-internecie.html, dostęp: 3.08.2022.

CYBERBEZPIECZEŃSTWO – JAKO OBSZAR BADAŃ

Cyberbezpieczeństwo uznać należy za jeden z kluczowych celów strategicznych w obszarze bezpieczeństwa naszego państwa i mający na celu zapewnienie ochrony najistotniejszym sektorom gospodarki, obywatelom oraz przedsiębiorcom.[2]

Katarzyna Chałubińska-Jentkiewicz stwierdza że *„cyberbezpieczeństwo jest pojęciem odnoszącym się do zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotykają cyberprzestrzeni, jak i funkcjonowania w cyberprzestrzeni a dotyczy to zarówno sektora publicznego, jak i prywatnego oraz ich wzajemnych relacji. Na rzecz tego stanowiska przemawia również charakterystyka pojęcia cyberprzestępczości, obejmującego generalnie swoim zakresem zagrożenia, jakie pojawiają się w cyberprzestrzeni."*[3]

Autorzy Dominika Lisiak-Felicka i Maciej Szmit w swojej publikacji *„Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia"* bardzo szeroko i etymologicznie odnoszą się do pojęcia cyberbezpieczeństwa, zwracając uwagę, że stanowi ono szczegółową część nauk o bezpieczeństwie, a tym samym dotyczyć go będą także odpowiednio odnoszące się do pojęcia „bezpieczeństwa" problemy rozróżnienia subiektywnego poczucia bezpieczeństwa od obiektywnego stanu braku zagrożeń.[4]

Takie rozumienie *„cyberbezpieczeństwa"* zdaje się potwierdzać Minisłownik BBN, definiującym cyberbezpieczeństwo RP (bezpieczeństwo RP w cyberprzestrzeni) jako „transsektorowy obszar bezpieczeństwa, obejmujący proces zapewniania bezpiecznego funkcjonowania w cyberprzestrzeni państwa jako całości, jego elementów (struktur, osób fizycznych i osób prawnych, w tym przedsiębiorców i innych podmiotów nieposiadających osobowości prawnej oraz będących w ich dyspozycji systemów teleinformatycznych i zasobów informacyjnych).[5]

A z kolei bezpieczeństwo cyberprzestrzeni – utożsamiając z procesem obejmującym *„zespół przedsięwzięć organizacyjno-prawnych, technicznych, fizycznych i edukacyjnych mającym na celu zapewnienie niezakłóconego funkcjonowania cyberprzestrzeni; [lub] częścią cyberbezpieczeństwa państwa obejmującą zapewnienie bezpiecznego funkcjonowania pozostającej pod jego kontrolą teleinformatycznej infrastruktury krytycznej i wykorzystania strategicznych zasobów informacyjnych państwa"*.[6]

W USA, funkcjonuje definicja „bezpieczeństwa cybernetycznego" jako pewnej sytuacji w której „(...) systemy informacyjne lub komunikacyjne oraz informacja zawarta w nich są zabezpieczone czy chronione przed uszkodzeniem lub nieautoryzowanym użyciem, modyfikacją lub wykorzystaniem".[7] Definicja ta została zaproponowana przez Narodową Inicjatywę w zakresie Karier i Studiów w Dziedzinie Cyberbezpieczeństwa (National Initiative for Cybersecurity Careers and Studies, NICCS), tj. jednostkę zarządzaną przez wydział edukacji i świadomości cyberbezpieczeństwa znajdujący się w strukturze Departamentu Bezpieczeństwa Wewnętrznego Urzędu Cyberbezpieczeństwa i Komunikacji Rządu Federalnego USA, jako definicja o dość wąskim zakresie. Jednocześnie NICCS, proponuje także szersze rozumienie „cyberbezpieczeństwa" „jako strategii, polityki i norm dotyczących zarówno bezpieczeństwa cyberprzestrzeni, jak i działania w niej, obejmujące z jednej strony pełen zakres czynności ukierunkowanych na redukcję zagrożeń, zmniejszenie podatności na nie i odstraszanie, międzynarodowe zaangażowanie, reagowanie na zdarzenia, zaś z drugiej – elastyczną politykę prewencyjną, uwzględniającą odpowiednie operacje w sieci komputerowej, zapewnienie informacji, działania organów ścigania, dyplomacji, wojska, służb wywiadowczych, odnoszące się do bezpieczeństwa

2 *Cyberbezpieczeństwo*, [na:] https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/3284,Cyberbezpieczenstwo.html, dostęp: 3.08.2022.

3 K. Chałubińska-Jentkiewicz, *Cyberbezpieczeństwo – zagadnienia definicyjne,* „Cybersecurity and Law" Nr 2(2) 2019, s. 7.

4 D. Lisiak-Felicka, M. Szmit, *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016, s. 19.

5 http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (dostęp: 3.08.2022).

6 http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html (dostęp: 3.08.2022).

7 C. Vishik, M. Matsubara, A. Plonk, Key Concepts in Cyber Security: *Towards a Common Policy and Technology Context for Cyber Security Norms,* [w:] International Cyber Norms: Legal, Policy & Industry Perspectives, A.-M. Maria Osula, H. Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016, s. 221; Tak też: Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich,* „Studia z Polityki Publicznej" 2016/2(10), s. 108.

i stabilności globalnej infrastruktury informacyjnej i komunikacyjnej."[8]

Z kolei, nieobowiązujący już dokument Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022, w swojej części słownikowej definiował „cyberbezpieczeństwo" jako „bezpieczeństwo sieci i systemów informatycznych" lub „bezpieczeństwo teleinformatyczne" „oznaczające odporność systemów teleinformatycznych, 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".[9]

Co znamienne, zwłaszcza na poziome europejskim – UE widząc, tak znaczne rozbicie definicyjne, unika definiowania tego pojęcia, ograniczając się w tym zakresie jedynie do określenia mniej lub bardziej konkretnych celów i przedmiotu ochrony.[10] Ma to m.in. miejsce w takim dokumencie jak Strategia bezpieczeństwa cybernetycznego Unii Europejskiej „Otwarta, bezpieczna i chroniona cyberprzestrzeń"[11] zgodnie z którą, cyberprzestrzeń należy chronić przed incydentami, szkodliwymi działaniami i nadużyciami; celem zaś ochrony jest cyberprzestrzeni powinno być: zapewnienie dostępu i otwartości, poszanowania i ochrony praw podstawowych w Internecie oraz utrzymanie niezawodności i interoperacyjności Internetu."[12]

Wśród tak wielu definicji i ujęć, ważny pogląd o charakterze synkretycznym wyraża C. Banasiński, który finalnie uznaje, że pojęcie „cyberbezpieczeństwa" można sprowadzić do „sposobu wolnego od zakłóceń gromadzenia, przetwarzania i wymiany informacji utrwalonych i przetworzonych w sposób cyfrowy"[13] przez co można odróżnić samo „cyberbezpieczeństwo" od „bezpieczeństwa informacyjnego" traktowanego „jako możliwość pozyskania jakościowo dobrej informacji przez jakiś podmiot oraz ochrony posiadanej informacji przed jej utratą, niezależnie od sposobu jej gromadzenia, przesyłania i przetwarzania."[14]

Liczne próby zdefiniowania „cyberprzestrzeni" czy „cyberbezpieczeństwa" wyraźnie pokazują, że mamy do czynienia w zasadzie ze zjawiskiem relatywnie (społecznie) nowym, w którym jeszcze zarówno przedmiot badań jak i jego metodologia ostatecznie jeszcze się nie sformułowały. Przywoływany C. Banasiński – słusznie zauważa, że sama „cyberprzestrzeń" niesie ze sobą wiele istotnych zagrożeń zarówno dla poszczególnych osób, całych społeczności a nawet instytucji i państw,[15] a te ostatnie stanowią, nowy ważny element ładu międzynarodowego. Generalnie jednak, należy podzielić stanowisko, zgodnie z którym „bezpieczeństwo w cyberprzestrzeni" jest elementem nowej dyscypliny naukowej – securitologii, która obszarem swojego zainteresowania obejmuje wieloaspektowe badania odnoszące się do istnienia, rozwoju i funkcjonowania człowieka.[16] Takie ujęcie przedmiotu generować będzie konieczność multi- i interdyscyplinarnego spojrzenia na naturę securitologii, co w efekcie będzie się przekładać na konieczność korzystania z dorobku teoretycznego i warsztatu metodologicznego innych dyscyplin naukowych z jednej strony, z drugiej zaś wymuszać będzie podejście holistyczne i systemowe.[17]

---

8 C. Vishik, M. Matsubara, A. Plonk, *Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms,* [w:] International Cyber Norms: Legal, Policy & Industry Perspectives, A.-M. Maria Osula, H. Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016, s. 221-222; Tak też: Z. Chmielewski, *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich,* „Studia z Polityki Publicznej" 2016/2(10), s. 108.

9 *Słowniczek „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022",* Warszawa 2017, s. 28.

10 C. Banasiński (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018, s. 32.

11 Jest to jest pierwszy dokument strategiczny UE w zakresie cyberbezpieczeństwa. Została opublikowana 7 lutego 2013 roku przez Komisję Europejską.

12 C. Banasiński (red.), op.cit., s. 32.

13 C. Marcinkowski, Cyberprzestrzeń a istota wybranych zagrożeń społecznych dla bezpieczeństwa współczesnego człowieka [w:] D. Morańska (red.) *Patologie w cyberprzestrzeni : profilaktyka zagrożeń medialnych,* Dąbrowa Górnicza 2015, s 115.

14 C. Banasiński (red.), *op.cit.*, s. 33.

15 *Ibidem,* s. 36.

16 L. F. Korzeniowski, SECURITOLOGIA *Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków 2008, s. 48. Por. C. Banasiński [w:] C. Banasiński (red.), Cyberbezpieczeństwo. Zarys wykładu, Warszawa 2018, s. 37.

17 *Ibidem.*

Wbrew zatem co ogólnie przyjęło się społecznie wyobrażać, badania nad cyberbezpieczeństwem zaliczyć należy do nauk na wskroś społecznych, chociaż w swojej istocie determinowanych przemianami techniczno-technologicznymi, związanymi z fenomenem Internetu – i tego co on przynosi ze sobą – a więc dobrodziejstw cyberspołeczeństwa jak i cyberzagrożeń. Można się w tym miejscu pokusić o stwierdzenie, że współczesne nauki społeczne wręcz nie nadążają za zmianami, jakie przynosi ze sobą każdego dnia rewolucja cyfrowa, w każdym wymiarze życia – osobistym, społeczno-lokalnym czy państwowym.

Przejście w sferę życia cyfrowego musi zatem być wprost sprzężone z uwidocznieniem się zjawisk negatywnych. Tę rosnącą skalę cyberprzestępczości obserwować możemy także w Polsce, a obrazuje ją poniższa tabela przedstawiająca liczbę postępowań wszczętych i liczbę przestępstw stwierdzonych przez Policję w latach 2013–2020, które zostały popełnione w cyberprzestrzeni oraz z wykorzystaniem Internetu:[18]

Już na tej podstawie widzimy, że w okresie objętym badaniem liczba popełnianych przestępstw wzrosła ponad dwukrotnie, a liczba wszczętych postępowań aż trzykrotnie. Jak podaje dalej przywoływane uzasadnienie, „największa liczba cyberprzestępstw jest popełniana w następujących kategoriach:

1. przestępstwa przeciwko mieniu;
2. przestępstwa przeciwko prawom autorskim i prawom pokrewnym;
3. przestępstwa przeciwko wolności seksualnej i obyczajności;
4. przestępstwa przeciwko ochronie informacji;
5. przestępstwa przeciwko wiarygodności dokumentów;
6. przestępstwa przeciwko własności przemysłowej;
7. przestępstwa przeciwko wolności;
8. przestępstwa przeciwko czci i nietykalności cielesnej."[19]

Postępowania wszczęte							
2013 r.	2014 r.	2015 r.	2016 r.	2017 r.	2018 r.	2019 r.	2020 r.
18 226	**23 117**	**27 874**	**32 584**	**32 898**	**36 474**	**47 607**	**53 687**
Postępowania stwierdzone							
2013 r.	2014 r.	2015 r.	2016 r.	2017 r.	2018 r.	2019 r.	2020 r.
52 291	**59 768**	**63 723**	**65 707**	**80 355**	**79 825**	**105 739**	**107 518**

Źródło: Opracowanie własne na podstawie: M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu*, „BEZPIECZEŃSTWO NARODOWE" nr 22, II – 2012, s. 131.

18 *Uzasadnienie do rządowego projekt ustawy - o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości*, [na:] https://www.sejm.gov.pl/Sejm9.nsf/PrzebiegProc.xsp?nr=1742, dostęp: 31.08.2022.

19 *Uzasadnienie do rządowego projekt ustawy - o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości*, [na:] https://www.sejm.gov.pl/Sejm9.nsf/PrzebiegProc.xsp?nr=1742, dostęp: 31.08.2022.

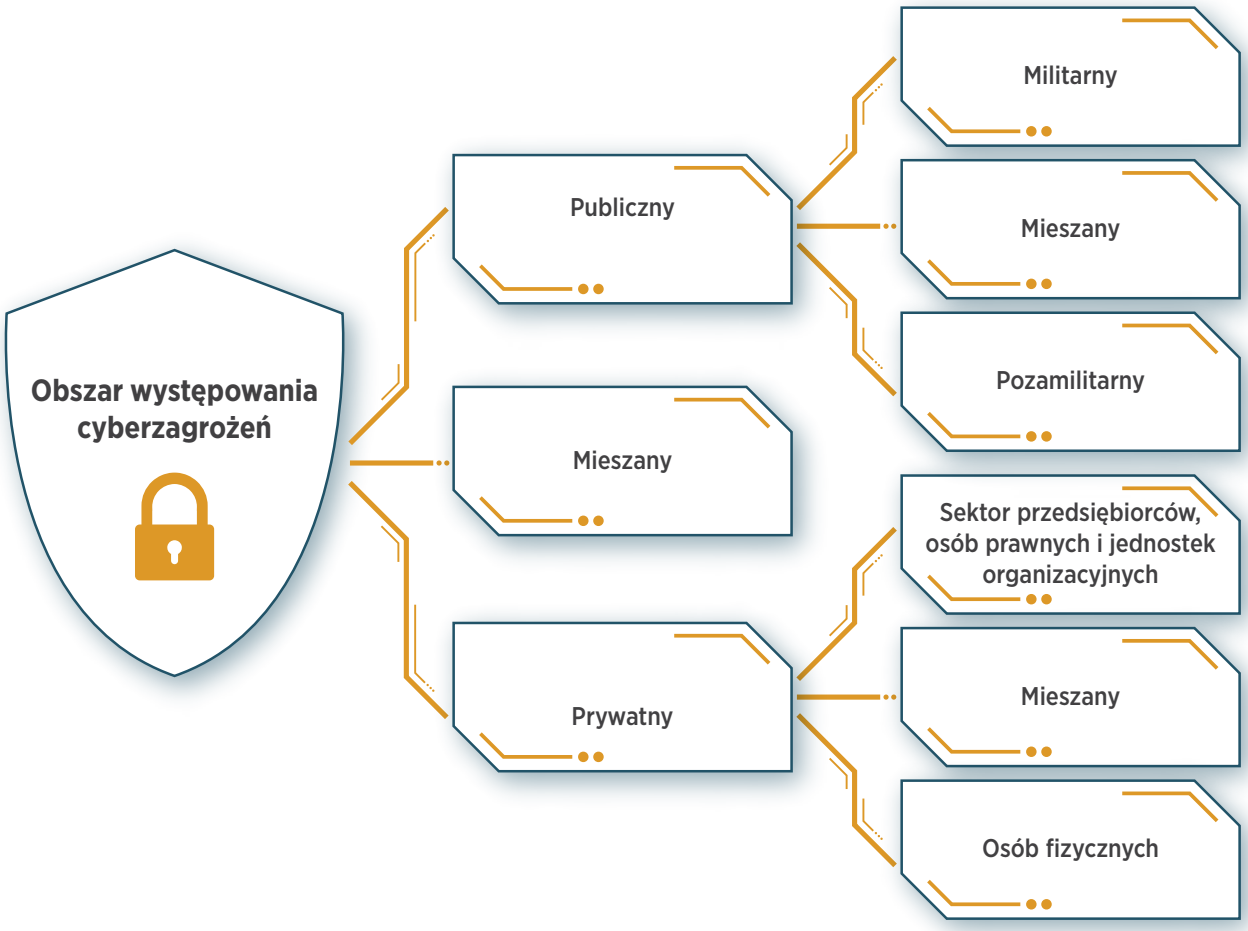
OBSZARY WYSTĘPOWANIA CYBERZAGROŻEŃ

Cyberzagrożeniem określamy „możliwość złośliwej próby uszkodzenia lub zakłócenia pracy sieci komputerowej lub systemu."[20] Będą to zatem wszelkie okoliczności lub zdarzenia mogące zaszkodzić danemu systemowi informatycznemu poprzez nieautoryzowany dostęp, zniszczenie, ujawnienie, modyfikację danych i/lub odmowę usługi.[21] Określając obszary, w których te zagrożenia mogą wystąpić, w sposób naturalny nasuwa się podział na sferę publiczną i prywatną.

Sfera publiczna – a więc obszar do którego zaliczymy m.in. instytucje i relacje międzypaństwowe, organy państwa: władzy wykonawczej, ustawodawczej i sądowniczej, instytucji państwowych, agencji rządowych, samorządu terytorialnego oraz inne emanacje o charakterze publicznym, a także aparat bezpieczeństwa państwa, w skład którego wchodzą służby, wojsko i policja. Z uwagi na jego specyfikę – możemy dokonać dalszego podziału na podobszar związany z bezpieczeństwem stricte „militarnym" – wojska i odpowiednich służb oraz podobszar pozamilitarny, związany z funkcjonowaniem „niemilitarnej" części aparatu państwowego. Oczywiście, trzeba mieć tu także na uwadze, że nie zawsze w sposób ostateczny i jednoznaczny daje się zakwalifikować dane zagrożenie, przez co może mieć ono charakter mieszany – nie tylko militarny i pozamilitarny, ale także publiczno-prywatny.[22]

Z kolei sfera prywatna – odnosić się będzie do obszaru funkcjonowania z jednej strony osób prawnych i jednostek organizacyjnych (tj. przedsiębiorców: IDG, spółek, stowarzyszeń, fundacji etc.) z drugiej zaś stricte osób fizycznych, przy czym oczywiście należy mieć tutaj na uwadze możliwość pojawienia się postaci mieszanej.

Rys. 1. Obszary występowania cyberzagrożeń (opracowanie własne)



20 *Czym są cyberzagrożenia? Rodzaje, przykłady i cyberataki,* [na:] https://businessinsider.com.pl/technologie/nowe-technologie/cyberzagrozenia-rodzaje-przyklady-definicja/8j4wwbz, dostęp: 31.08.2022.

21 *Ibidem*

22 W tym kontekście można wspomnieć o amerykańskim projekcie „Olympic Games", którego celem, zgodnie z doniesieniami medialnymi, było powstrzymanie irańskiego programu nuklearnego, m.in. za pomocą specjalnie opracowanego robaka Stuxnet. *3 Obama Order Sped Up Wave of Cyberattacks Against Iran,* „The New York Times", [na:] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all, dostęp: 31.08.2022

Chociaż katalog cyberzagrożeń w miarę upływu czasu coraz bardziej się poszerza, to w/w rys. 2 prezentuje katalog nadal bardzo popularnych zagrożeń cyberprzestrzeni. Nie wchodząc w pogłębioną analizę poszczególnych form, zwrócić należy uwagę w szczególności na grupę ataków APT (ang. advanced persistent threat), o których szczególnym zagrożeniu, świadczy już sam fakt, że stanowią one postać hybrydową łączącą narzędzia różnego typu (socjotechniczne, programistyczne itp.), i pomimo długiego czasu prowadzonych przygotowań pozostają one bardzo skuteczne.[23]

Jak wskazują dane CERT Polska najpopularniejszym typem incydentów w 2021 r. był phishing, który stanowił aż 76,57 % wszystkich obsłużonych incydentów.[24] Co istotne, rok do roku liczba phishingowych incydentów wzrosła o 196 proc. i osiągnęła rekordową liczbę 22575 incydentów.[25] Jak podają analitycy CERT Polska, najpopularniejszym phishingiem w 2021 r. było podszywanie się pod serwis społecznościowy Facebook – 4852 incydentów.[26] Drugim typem incydentów pod względem popularności jakie CERT Polska zarejestrował i obsłużył było szkodliwe oprogramowanie. Tego typu incydentów w 2021 r. zarejestrowano 2847, co stanowi 9,66 proc. wszystkich obsłużonych incydentów, a całkowita liczba w porównaniu do roku ubiegłego wzrosła o 281 proc.[27]

Oceniać należy, że notowane wzrosty są wynikiem koniunkcji głównego czynnika jakim jest pandemia COVID-19 – oraz towarzyszących jej lockdownów – w wyniku których jeszcze więcej czasu spędzamy w Internecie; skokowemu rozwojowi nowych – i niekoniecznie zrozumiałych przez przeciętnych użytkowników programów i aplikacji a także zjawisku niepewności prawnej i ekonomicznej, wynikającej pośrednio z konieczności przyjmowania przez ustawodawcę kolejnych inicjatyw legislacyjnych mających na celu poprawę sytuacji materialnej i zdrowotnej Polaków.

Rys. 2. Wybrane, najpopularniejsze zagrożenia cyberprzestrzeni



Źródło: Opracowanie własne na podstawie: M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „BEZPIECZEŃSTWO NARODOWE" nr 22, II – 2012, s. 131.

23 M. Grzelak, K. Liedel, *Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe" nr 22, II – 2012, s. 131.

24 *Statystyki obsługi incydentów*, [na:] https://cert.pl/posts/2022/04/statystyki-obslugi-incydentow-2021/, dostęp: 31.08.2022.

25 *Statystyki obsługi incydentów*, [na:] https://cert.pl/posts/2022/04/statystyki-obslugi-incydentow-2021/, dostęp: 31.08.2022.

26 *Ibidem.*

27 *Ibidem.*



KRAJOWE DOKUMENTY STRATEGICZNE

Aby prześledzić proces ewolucji i zmian w obszarze legislacji związanej z cyberbezpieczeństwem, warto się przyjrzeć bliżej wybranym, kluczowym dokumentom strategicznym – które w mniejszym lub większym stopniu do materii cyberbezpieczeństwa się odnosiły. Przegląd ten, w ujęciu chronologicznym, ukazuje z jednej strony rozwój samego cyberbezpieczeństwa, z drugiej zaś obrazuje pojawianie się coraz to nowych cyberzagrożeń i tym samym wzrastającej świadomości społecznej.

Warto zauważyć, iż pierwsza w historii Polski Strategia Bezpieczeństwa RP powstała w 2000 roku, a jej sektorowe rozwinięcie w kwestiach obrony narodowej stanowiła Strategia Obronności RP. Szybko jednak okazało się, że w kontekście nowych zagrożeń związanych z walką z terroryzmem, dalszą transformacją Paktu Północnoatlantyckiego - pozostaje ona niewystarczająca, przez co już 8 września 2003 r. przyjęto nowy dokument o tej nazwie.[28]

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007

Kolejny dokument pod nazwą „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007" (dalej: Strategia 2007) 13 listopada 2007 r. zatwierdził Prezydent RP Lech Kaczyński na wniosek na wniosek Prezesa Rady Ministrów Jarosława Kaczyńskiego. Dokument ten został wydany w oparciu o art. 4a ust.1 pkt.1 ustawy z dnia 21 listopada 1967 r. – o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. W Strategii 2007 zawarto jasną wizję polskich sił zbrojnych, określając zagrożenia i wskazując m.in. "że Polska jako kraj graniczny NATO i UE zajmuje ważne miejsce w europejskim systemie bezpieczeństwa."[29] Jednocześnie, jak podkreśla się w literaturze, Strategia 2007 realizuje postulat zintegrowanego podejścia do spraw bezpieczeństwa (w tym wzrost znaczenia problematyki bezpieczeństwa pozamilitarnego) jak również zwraca uwagę na nowe elementy w warunkach bezpieczeństwa (w tym cyberzagrożenia oraz trwające operacje w Afganistanie i Iraku).[30]

Ten 37 stronicowy dokument 2-krotnie zwraca uwagę na kwestie cybernetyczne. Po raz pierwszy ma to miejsce na stronie 10, gdzie w podrozdziale „2.2. Wyzwania i zagrożenia bezpieczeństwa" pkt. 36 – poświęconym przestępczości międzynarodowej, wymienia się także inne zagrożenie, którym „może być oddziaływanie w cyberprzestrzeni, skierowane w systemy i sieci teleinformatyczne infrastruktury krytycznej. Skutkiem takich działań mogą być zarówno straty materialne, jak i sparaliżowanie istotnych sfer życia publicznego".[31]

Drugi raz ma to miejsce w podrozdziale „3.6. Bezpieczeństwo ekonomicznie" pkt. 74., gdzie wskazano, iż „należy kontynuować rozwój nowoczesnej, zintegrowanej struktury łączności elektronicznej, która byłaby odporna na awarie i potencjalne ataki przestępczości cybernetycznej. Będzie to wymagać należytego współdziałania właściwych resortów i agend, a także podmiotów prywatnych".[32] Należy także na tym miejscu zaznaczyć, że Strategia Obronności Rzeczypospolitej Polskiej 2009 jako Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej z 2007 r., wymienia w podrozdziale „1.1. Środowisko bezpieczeństwa międzynarodowego - Bezpieczeństwo globalne": „cyberterroryzm" jako istotne zagrożenie dla bezpieczeństwa o charakterze asymetrycznym, w większości przypadków generowane przez państwa upadające i państwa upadłe.

28 S. Koziej, A. Brzozowski, *25 lat polskiej strategii bezpieczeństwa,* „Bezpieczeństwo Narodowe" nr 30, II – 2014, s. 12.

29 *Cztery lata prezydentury*, [na:] https://www.prezydent.pl/kancelaria/archiwum/archiwum-lecha-kaczynskiego/cztery-lata prezydentury/bezpieczenstwo, dostęp: 31.08.2022.

30 S. Koziej, A. Brzozowski, *op.cit*, s. 12.

31 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007*, Warszawa 2007, s. 10.

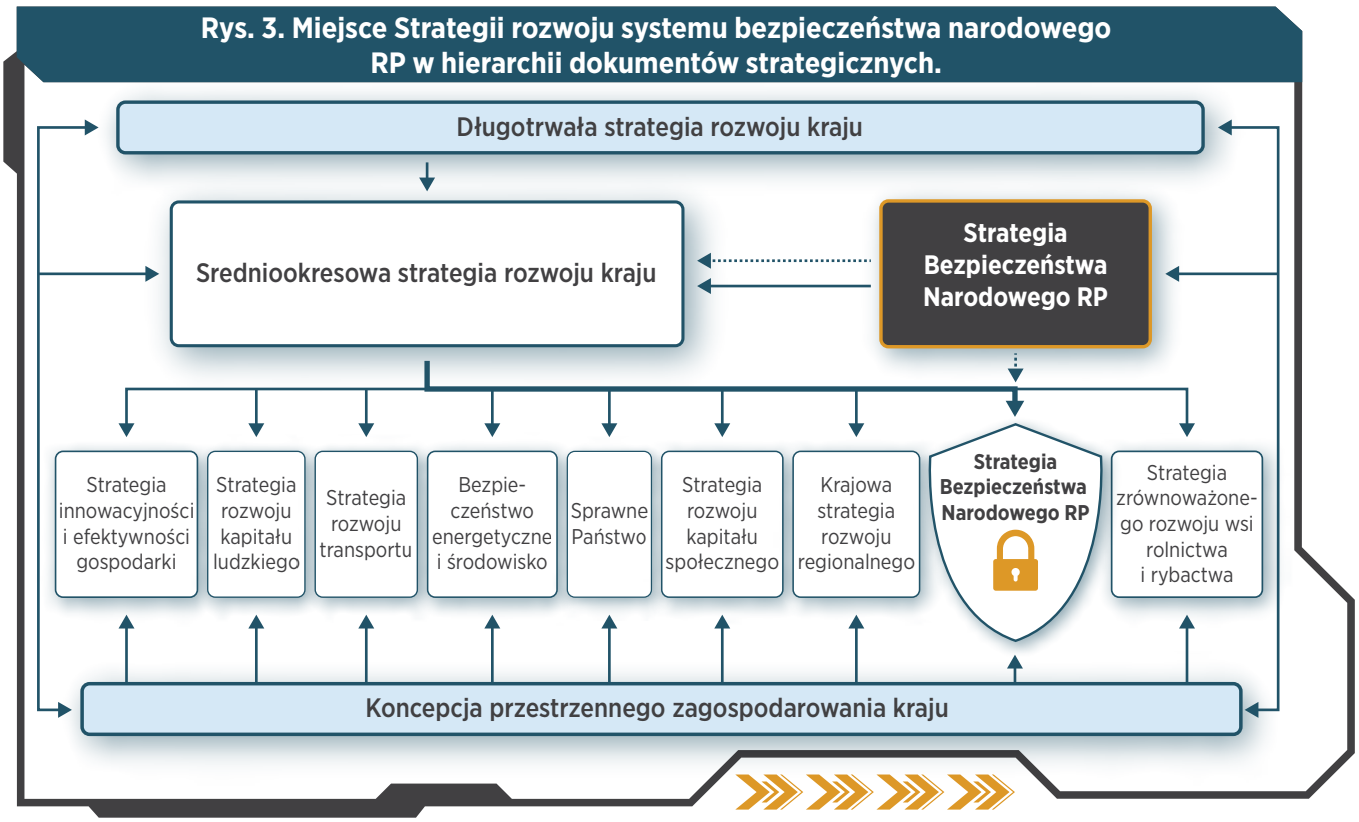
32 *Ibidem*, s. 19.

Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022 z 2013r.

Uchwałą Rady Ministrów z 9.04.2013 r. przyjęta została „Strategia Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022”[33] (dalej: Strategia Systemu 2013-2022). Podstawą prawną do jej przyjęcia był art. 14 ust. 3 ustawy z dnia 6 grudnia 2006 r. – o zasadach prowadzenia polityki rozwoju.[34] Horyzont tej ponad 100 stronicowej strategii określony został na lata 2013-2022. Przyjęcie tego dokumentu spowodowało utratę mocy przez „Strategię obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej”, przyjętą przez Radę Ministrów w dniu 23 grudnia 2009 r.[35] oraz „Strategię udziału Sił Zbrojnych Rzeczypospolitej Polskiej w operacjach międzynarodowych”[36], przyjętą przez Radę Ministrów w dniu 13 stycznia 2009 r.

Przedmiotowy dokument zawiera diagnozę systemu bezpieczeństwa narodowego, przedstawia wyzwania, trendy rozwojowe i wizję rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej a także prezentuje cele strategii i kierunki interwencji, system realizacji strategii oraz ramy finansowe strategii. Zawiera on także szereg odniesień do kwestii cybernetycznych, m.in. już we Wprowadzeniu, zwraca się uwagę, że wśród procesów zachodzących we współczesnym, globalnym środowisku bezpieczeństwa, które cechują się dużą dynamiką i złożonością zmian oraz występowaniem zagrożeń asymetrycznych, wśród najgroźniejszych wymienia się m.in. właśnie zagrożenia w cyberprzestrzeni.

Rys. 3. Miejsce Strategii rozwoju systemu bezpieczeństwa narodowego RP w hierarchii dokumentów strategicznych.



Źródło: Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022, Warszawa 2013, s. 6

33 *Uchwała nr 67 Rady Ministrów z dnia 9 kwietnia 2013 r. w sprawie przyjęcia „Strategii rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej”*, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WMP20130000377, dostęp: 31.08.2022.

34 *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 15 maja 2009 r. w sprawie ogłoszenia jednolitego tekstu ustawy o zasadach prowadzenia polityki rozwoju*, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20090840712, dostęp: 31.08.2022.

35 Należy zauważyć, że ten dokument 34 stronicowy dokument tylko raz odnosił się do kwestii cybernetycznych. W pkt. 15. poświęconym zagrożeniom dla środowiska bezpieczeństwa o charakterze asymetrycznym, wymieniony został cyberterroryzm jako jeden z rodzajów terroryzmu generowanego przez państwa upadające i państwa upadłe.

36 Ten dokument nie zawierał odniesień do kwestii cybernetycznych.

W szczególności w punkcie 1.1.5. Strategia Systemu 2013-2022 wskazuje się na konieczność pogłębiania współpracy na rzecz bezpieczeństwa cybernetycznego na forum NATO i UE. Zwraca się uwagę, że „Ataki cybernetyczne w coraz większym stopniu zagrażają bezpieczeństwu i stabilności obszaru euroatlantyckiego. Niektóre państwa dysponują dziś możliwościami przeprowadzania ataków cybernetycznych, których poziom byłby porównywalny do konwencjonalnych ataków zbrojnych. Stąd zarówno w NATO, jak i UE podniesiono rangę bezpieczeństwa cybernetycznego do poziomu rozpatrywanego przez najwyższe gremia polityczne. O bezpieczeństwie informatycznej infrastruktury krytycznej NATO i UE decyduje ich najsłabsze ogniwo. Stwarza to konieczność spełnienia standardów i wymagań obu organizacji przez infrastrukturę krajową”.[37] W tym zakresie proponuje się konkretne zadania do których należy:

„- wspieranie inicjatyw na rzecz wzmocnienia roli i zdolności NATO i UE w zakresie polityki bezpieczeństwa cybernetycznego oraz wyposażenie obu organizacji w instrumenty udzielania pomocy państwom członkowskim (w szczególności średnim i małym) narażonym na ataki cybernetyczne;

- wspieranie działań na rzecz uwzględnienia obrony cybernetycznej w bieżących pracach planistycznych NATO;

- wzmocnienie współpracy pomiędzy NATO i UE w obszarze bezpieczeństwa cybernetycznego, w tym w szczególności w zakresie ochrony infrastruktury krytycznej sektorów cywilnych (łączność, energetyka, transport, finanse);

- aktywny udział Polski w budowie i funkcjonowaniu unijnych i sojuszniczych elementów struktur obrony cybernetycznej;

- udoskonalenie zasad i mechanizmów współpracy wewnątrz- i międzyresortowej, w tym pomiędzy ABW i MON;

- uwzględnienie w Polityce bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej nowych elementów wynikających z prac NATO i UE nad polityką bezpieczeństwa cybernetycznego”.

Drugim wysoce ważnym elementem, na który w sposób szczególny zwrócono uwagę w ramach tzw. Celu 5 tj. „Tworzenie warunków do rozwoju zintegrowanego systemu bezpieczeństwa narodowego” w omawianym dokumencie, to zapewnienie bezpieczeństwa informacyjnego i telekomunikacyjnego w kontekście zintegrowanego systemu bezpieczeństwa narodowego.

Podnosi się, że „cyberterroryzm stanowi obecnie jedno z głównych zagrożeń dla bezpieczeństwa teleinformatycznego państw, w tym Polski. Spowodowane jest to między innymi rosnącą liczbą użytkowników sieci internetowej, niewielkimi kosztami związanymi z przeprowadzeniem ataku cyberterrorystycznego, a także możliwością zachowania praktycznie pełnej anonimowości przez odpowiedzialne za niego osoby bądź podmioty. W celu podwyższenia stopnia zabezpieczeń teleinformatycznych administracji państwowej przed zagrożeniami z Internetu, konieczne są kompleksowe i skoordynowane działania wszystkich podmiotów administracji publicznej, które poprzez prowadzenie analizy ryzyka będą wdrażały zabezpieczenia adekwatne do prawdopodobieństwa wystąpienia zagrożeń. Skoordynowane działania adekwatne do zagrożeń wszystkich podmiotów administracji pozwolą na radykalne podwyższenie stopnia zabezpieczeń z uwzględnieniem minimalizacji kosztów. Stosowne działania będą również podejmowane w ramach reagowania na zagrożenia związane z cyberwywiadem”.[38] W tym zakresie Strategia Systemu 2013-2022 zakładała główne działania:[39]

- przyjęcie Polityki ochrony cyberprzestrzeni Rzeczypospolitej Polskiej;[40]
- umocnienie mechanizmów koordynacji i współdziałania na poziomie państwa poprzez

37 *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, Warszawa 2013, s. 42-43.

38 *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, Warszawa 2013, s. 85-86.

39 *Ibidem*, s. 86.

40 Dokument przyjęty przez Komitet Rady Ministrów ds. Cyfryzacji w dniu 28.11.2012 r.

działania Komitetu Rady Ministrów ds. Cyfryzacji;

- zwiększenie zasięgu działania systemu ARAKIS. GOV[41] poprzez objęcie wszystkich urzędów i instytucji państwowych systemem;

- prowadzenie prac naukowych w obszarze reagowania na incydenty komputerowe w zakresie Systemu Zarządzania Bezpieczeństwem Informacji.

Również w ramach tzw. Celu 5 w pkt. 5.3.2. zwrócono uwagę na konieczność rozwijania Systemu Reagowania na Incydenty Komputerowe (SRnIK). Powołany został w tej sferze także działający – „analogicznie jak funkcjonujący dla administracji rządowej w sferze cywilnej CERT.GOV.PL – System Reagowania na Incydenty Komputerowe MON"[42], którego głównym zadaniem, zgodnie ze Strategią Systemu 2013-2022 miało być „zapewnienie realizacji i koordynacji procesów zapobiegania, wykrywania i reagowania na incydenty komputerowe w systemach i sieciach teleinformatycznych resortu obrony narodowej, a także współpraca w obszarze przeciwdziałania atakom cybernetycznym z Rządowym Zespołem Reagowania na Incydenty Komputerowe CERT.GOV.PL oraz CERT-POLSKA".[43]

W omawianym pkt. 5.3.2. zwrócono także uwagę że „wzrost zagrożeń w obszarze cyberprzestrzeni wymaga dostosowywania i ciągłego rozwijania istniejących struktur systemu reagowania".[44] Dlatego jednym z podstawowych zadań realizowanych w najbliższych latach miało być „kontynuowanie procesu rozbudowy powołanego w ramach SRnIK zespołu MIL-CERT i pozyskanie nowych kompetencji pozwalających na realizację zawansowanych technologicznie funkcji, w tym informatyki śledczej i aktywnej odpowiedzi na ataki cybernetyczne".[45] Miało się to odbywać w sposób powiązany „z rozwojem Rządowego Zespołu Reagowania na Incydenty Komputerowe oraz budową kompetencji strategicznej koordynacji w Ministerstwie Administracji i Cyfryzacji, właściwym dla działów łączność i informatyzacja".[46] W tym punkcie również zakładano główne działania polegające na:[47]

- dalszym rozszerzaniu współpracy z innymi zespołami narodowymi i organizacjami konsolidującymi międzynarodowe struktury CERT, w tym wówczas powstałym zespołem CERT UE;

- ustanowieniu Krajowego Systemu Reagowania na Incydenty Komputerowe pozwalającego na podjęcie szybkiej reakcji na zagrożenia z sieci Internet;

- posiadaniu przez Agencję Bezpieczeństwa Wewnętrznego oraz resort obrony narodowej silnych, wyposażonych w zaawansowane technologie zespołów reagowania (w tym zespołów szybkiego reagowania – Rapid Reaction Team) co usprawniło realizowanie współpracy międzynarodowej oraz miało pozwolić osiągnąć nowe zdolności operacyjne w zakresie zadań reagowania na incydenty bezpieczeństwa teleinformatycznego oraz dowodzenia i kierowania w cyberprzestrzeni.

Kolejnym ważnym elementem, do którego odnosi się pkt. 5.3.3. tzw. Celu 5 było „Rozwijanie Sieci Łączności Rządowej". Wskazywano tutaj, że „podmioty zaangażowane w proces kierowania bezpieczeństwem narodowym wymagają wzmocnionego zabezpieczenia systemów łączności i informatycznego wsparcia. Aby zapewnić im ochronę informacji przed nieuprawnionym ujawnieniem w trakcie rozmów telefonicznych i wideokonferencyjnych oraz podczas transmisji danych, w szczególności przed utratą poufności, dostępności i integralności, rozwijana będzie Sieć

41 ARAKIS (Agregacja, Analiza i Klasyfikacja Incydentów Sieciowych) – pasywny system wczesnego ostrzegania o zagrożeniach występujących w Internecie.

42 *Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej*, Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022, s. 86.

43 *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, Warszawa 2013, s.86.

44 *Ibidem.*

45 *Ibidem.*

46 *Ibidem.*

47 *Ibidem.*

Łączności Rządowej (SŁR)".[48] Ma ona zapewnić też łączność pomiędzy upoważnionymi osobami na wypadek sytuacji kryzysowych oraz spełniać istotną rolę w zapewnieniu łączności wydzielonej dla potrzeb Kancelarii Prezydenta, Kancelarii Sejmu, Kancelarii Senatu, administracji rządowej oraz innych podmiotów, zarówno w działalności bieżącej, jak i w sytuacjach kryzysowych.[49] SŁR[50] jest to sieć telekomunikacyjna, w ramach której świadczone są usługi telekomunikacyjne, w szczególności łączności głosowej, wideokonferencji, oparte o transmisję danych i inne usługi w ramach określanych potrzeb.[51] Od 2011 r. system mobilnej łączności niejawnej obejmował ponad 2000 abonentów (wyposażonych w telefony lub laptopy) i gwarantował całodobową wydzieloną, bezpieczną, szyfrowaną łączność pomiędzy najważniejszymi dla funkcjonowania i bezpieczeństwa państwa osobami - m.in. Prezydentem, Premierem, ministrami, szefami służb i ich jednostkami terenowymi.[52] Strategia Systemu 2013-2022 także w tym punkcie przewidywała główne działania do których zaliczono modernizację SŁR-N stacjonarnej poprzez zainstalowanie ok. 140 sztuk szyfrujących aparatów telefonicznych, zarówno w strefie centralnej sieci SŁR, jak i w strefie wojewódzkiej oraz migrację do nowoczesnej technologii wykorzystywanej w części mobilnej; oraz dalszą rozbudowę części mobilnej systemu niejawnego SŁR-N, m.in. dla dedykowanych zastosowań MON; a także docelową migrację SŁR do technologii IP (Protokołu Internetowego). [53]

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014

Na kolejną generację „Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej" przyszło nam czekać blisko 7 lat (dalej: Strategia 2014). Podobnie jak poprzedni dokument została ona przyjęta w oparciu o art. 4a ust.1 pkt.1 ustawy z dnia 21 listopada 1967 r. – o powszechnym obowiązku obrony Rzeczpospolitej Polskiej. Prezydent Rzeczypospolitej Polskiej Bronisław Komorowski 5 listopada 2014 r., na wniosek Prezesa Rady Ministrów, zatwierdził Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Strategia 2014 liczy 57 stron i do kwestii cybernetycznych odnosi się 38 razy.

W tej koncepcji rozwoju bezpieczeństwa narodowego, kwestie dotyczące cyberbezpieczeństwa stanowią istotny rys omawianego dokumentu. Po raz pierwszy, w sposób tak wyraźny pojawia się wprost postulat „zapewnienia bezpiecznego funkcjonowania Rzeczypospolitej Polskiej w cyberprzestrzeni"[54] jako cel strategiczny w dziedzinie bezpieczeństwa.

Po raz pierwszy także, w kontekście środowiska bezpieczeństwa Polski (Rozdział II), w wymiarze globalnym zwraca się uwagę w pkt. 31. na fakt, że „wraz z pojawieniem się nowych technologii teleinformatycznych oraz rozwojem sieci Internet pojawiły się nowe zagrożenia, takie jak cyberprzestępczość, cyberterroryzm, cyberszpiegostwo, cyberkonflikty z udziałem podmiotów niepaństwowych i cyberwojna, rozumiana jako konfrontacja w cyberprzestrzeni między państwami. Obecne trendy rozwoju zagrożeń w cyberprzestrzeni wyraźnie wskazują na rosnący wpływ poziomu bezpieczeństwa obszaru domeny cyfrowej na bezpieczeństwo ogólne kraju. Przy rosnącym uzależnieniu od technologii teleinformatycznych konflikty w cyberprzestrzeni mogą poważnie zakłócić funkcjonowanie społeczeństw i państw".[55] Natomiast w wymiarze regionalnym, zauważa się, że „znaczenie bezpieczeństwa w cyberprzestrzeni będzie rosło,

48 *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, Warszawa 2013, s.87.

49 *Ibidem*.

50 W październiku 2019 r. na wykaz prac legislacyjnych trafił Projekt ustawy - o Sieci Łączności Rządowej – numer z wykazu UD333, który został dotknięty zasadną dyskontynuacji prac parlamentu, [na:] https://legislacja.rcl.gov.pl/projekt/12321779,dostęp: 31.08.2022.

51 *Ibidem*.

52 *Ibidem*.

53 *Ibidem*.

54 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*, Warszawa 2014, s. 10.

55 *Ibidem*, s. 19.

podobnie jak odpowiedzialność państw za jej ochronę i obronę. Istotne znaczenie dla zwiększenia poziomu bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni ma polityka organizacji i struktur współpracy międzynarodowej, w pracach których Polska uczestniczy oraz współpraca dwustronna z wybranymi państwami, w szczególności z państwami NATO i UE".[56]

W Rozdziale III, w działaniach obronnych także wprost wskazuje się, że „cyberprzestrzeń stała się kolejnym środowiskiem walki zbrojnej. Siły zbrojne RP muszą dysponować zdolnościami defensywnymi i ofensywnymi w tej sferze, tak aby realizować funkcję odstraszania potencjalnego przeciwnika. W szczególności muszą być one gotowe, samodzielnie i we współpracy z sojusznikami, do prowadzenia operacji ochronnych i obronnych na większą skalę w razie cyberkonfliktu lub cyberwojny".[57]

W punkcie 84. powtórzono i wskazano także, że „zapewnienie bezpieczeństwa Polski w cyberprzestrzeni, w tym bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej, to jedno z podstawowych zadań w dziedzinie bezpieczeństwa państwa. Powinno być ono realizowane zarówno poprzez rozwój zdolności do działań defensywnych (obejmujących ochronę podmiotów działających w cyberprzestrzeni oraz samej cyberprzestrzeni), jak i ofensywnych. Szczególnie ważna jest: współpraca i koordynacja działań ochronnych z podmiotami sektora prywatnego – przede wszystkim finansowego, energetycznego, transportowego, telekomunikacyjnego i opieki zdrowotnej; prowadzenie działań o charakterze prewencyjnym i profilaktycznym w odniesieniu do zagrożeń w cyberprzestrzeni; wypracowanie i stosowanie właściwych procedur komunikacji społecznej w tym zakresie; rozpoznawanie przestępstw dokonywanych w cyberprzestrzeni i zapobieganie im oraz ściganie ich sprawców; prowadzenie walki informacyjnej w cyberprzestrzeni; współpraca sojusznicza, także na poziomie działalności operacyjnej służącej do aktywnego zwalczania cyberprzestępstw, w tym wymiany doświadczeń i dobrych praktyk w celu podnoszenia skuteczności i efektywności działań krajowych".[58]

Strategia 2014 w pkt. 128 odnosi się także wprost do sprecyzowania instytucji właściwych do spraw cyberbezpieczeństwa wskazując, że „do najważniejszych zadań przygotowawczych w obszarze cyberbezpieczeństwa należy wdrożenie i rozwijanie systemowego podejścia do sfery cyberbezpieczeństwa w wymiarze prawnym, organizacyjnym i technicznym. Konieczne jest określenie zasad prowadzenia aktywnej obrony oraz budowa narodowego systemu obrony cybernetycznej, w tym rozwijanie krajowego Systemu reagowania na incydenty komputerowe w cyberprzestrzeni Rzeczypospolitej Polskiej, kompatybilnego z systemami państw sojuszniczych. Istotne jest stworzenie narodowego ośrodka koordynacji, wspierającego organizację współpracy pomiędzy poszczególnymi podmiotami realizującymi zadania w zakresie cyberbezpieczeństwa i wymianę informacji oraz promującego dobre praktyki w dziedzinie cyberbezpieczeństwa. Ważne jest nabycie pełnych kompetencji do rozpoznawania, zapobiegania i zwalczania cyberzagrożeń oraz zdolności do wytwarzania polskich rozwiązań technologicznych przeznaczonych do zapewnienia odpowiedniego poziomu bezpieczeństwa w cyberprzestrzeni. Zapewnione zostaną odpowiednie warunki tworzenia i działania partnerstwa publiczno-prywatnego w dziedzinie cyberbezpieczeństwa".[59]

Na koniec, podkreśla się, w pkt. 130., że „istotne jest też zwiększanie świadomości użytkowników o zagrożeniach w cyberprzestrzeni poprzez intensyfikację działań edukacyjnych na wszystkich poziomach nauczania, a także w formie szkoleń i kampanii społecznych. Wskazane jest uruchomienie specjalnych kierunków studiów związanych z bezpieczeństwem funkcjonowania w cyberprzestrzeni oraz rozwijanie programów badawczych w tym obszarze".[60]

56 *Ibidem*, s. 23.

57 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*, s. 32.

58 *Ibidem*, s. 34-35.

59 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*, Warszawa 2014, s. 49.

60 *Ibidem*.

Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)

Wśród ważnych dokumentów o charakterze strategicznym, nie sposób pominąć przyjętej uchwałą Rady Ministrów z 14.02.2017 r. niezwykle obszernej (416 stron) „Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)" (SOR).[61] Pozostaje ona kluczowym dokumentem państwa polskiego w obszarze średnio- i długofalowej polityki gospodarczej, realizowanym zgodnie z paradygmatem prorozwojowym.

Dokument ten wskazuje, że m.in. „Kształt globalnych procesów w sferze ekonomicznej, społecznej i militarnej, a także działania światowej społeczności w odniesieniu do środowiska naturalnego będą konsekwencją rozwoju technologii. Moce obliczeniowe i zdolność przechowywania danych stają się dostępne niemal za darmo. Sieci i chmura obliczeniowa zapewnią globalny dostęp do odpowiednich rozwiązań. Media społecznościowe i rozwiązania w sferze bezpieczeństwa cyberprzestrzeni stają się ważnymi obszarami rynku".[62] W rezultacie zwraca się następnie uwagę, że po przeprowadzonej analizie, wśród szeregu sektorów strategicznych, które mają szanse stać się przyszłymi motorami polskiej gospodarki znajduje się właśnie sektor specjalistycznych technologii teleinformatycznych zawierający obok np. fintechu, automatyki maszyn i budynków, gier komputerowych, bioinformatyki także cyberbezpieczeństwo.[63]

W ramach rozwoju kompetencji polskich firm i jednostek naukowo-badawczych w dziedzinie cyberbezpieczeństwa i analizy danych planuje się powołanie do życia ośrodka Cyberpark Enigma, dysponującego potencjałem pozwalającym konkurować na europejskim rynku specjalistycznych usług IT.[64] Szansa rozwojowa tkwi także w biocybernetyce (wszczepialnych implantach, sztucznych narządach przeznaczonych do zastąpienia lub wsparcia upośledzonych funkcji narządów oraz systemach je wspomagających).[65]

Ważnym punktem SOR jest „Wzmocnienie cyfrowego rozwoju kraju". W dokumencie zwraca się uwagę, na okoliczność, że „Wraz z popularyzacją usług internetowych i przenoszeniem ich do coraz to nowych sfer gospodarki, pojawiają się nowe zagrożenia nazywane ogólnie cyberprzestępczością. Użytkownik korzystający z usługi musi czuć się bezpiecznie, umieć samodzielnie zastosować podstawowe środki ochrony, oraz mieć zagwarantowany wysoki poziom pewności, że nikt niepowołany nie dostanie się do jego danych osobowych, zasobów finansowych czy innych danych wrażliwych. Wymaga to wykorzystania specjalnych mechanizmów identyfikowania i uwierzytelniania oraz stosowania konkretnych norm bezpiecznego przesyłu danych".[66] Właśnie w tym obszarze SOR zaproponowała Zintegrowany System Zarządzania Bieżącego Bezpieczeństwem Cyberprzestrzeni RP[67], jako projekt strategiczny, którego celem „jest objęcie monitoringiem i korelacją zdarzeń kluczowych usług informatycznych zapewniających bezpieczeństwo funkcjonowania państwa, obywateli i podmiotów gospodarczych. Projekt ma na celu dostarczenie rozwiązań, które umożliwią dostęp do bieżącej informacji o stanie bezpieczeństwa teleinformatycznego niezbędnego do oceny sytuacji i stanu bezpieczeństwa w cyberprzestrzeni w Polsce oraz koordynacji reagowania na incydenty komputerowe na poziomie krajowym".[68] Wszystkie podejmowane działania mają zmierzać do

61 Uchwała Nr 8 Rady Ministrów z 14.02.2017 r. w sprawie przyjęcia Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.) (M.P. z 2017 r. poz. 260).

62 *Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*, Warszawa 2017, s. 20.

63 *Ibidem*, s. 68.

64 *Ibidem*, s. 78.

65 *Ibidem*, s. 282.

66 *Ibidem*, s. 297.

67 Za realizację projektu Zintegrowanego Systemu Zarządzania Bieżącego Bezpieczeństwem Cyberprzestrzeni RP, zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa, odpowiedzialny jest minister właściwy do spraw informatyzacji, a jego „rdzeń" stanowi projekt Narodowej Platformy Cyberbezpieczeństwa (NPC) realizowany w konsorcjum, którego liderem jest NASK PIB.

68 *Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*, Warszawa 2017, s. 299.

zapewnienia cyberbezpieczeństwa – tj. „ochrony poufności informacji, ciągłości działania systemów informatycznych, ciągłości działania systemów wspieranych rozwiązaniami cyfrowymi, a także ochrony prywatności obywateli zarówno w publicznej przestrzeni, jak również w zakresie danych gromadzonych przez administrację publiczną”.[69]

SOR zwraca także uwagę, na fakt, że „(...) dużym wyzwaniem jest zapewnienie odporności sieci przesyłowych i dystrybucyjnych tak paliw gazowych, płynnych, jak i energii elektrycznej na zjawiska pogodowe, siłową ingerencję człowieka, a także cyberzagrożenia. Elementem komplikacji jest tu nie tylko możliwość zdalnego ataku na urządzenia sieciowe, ale także wywołanie zakłóceń w funkcjonowaniu odbiorców, tak by skumulowany efekt doprowadził do awarii sieci. Ochrony wymaga też informacja związana z indywidualnym użytkowaniem energii, gdyż może ona zostać wykorzystana do wywoływania takich zachowań wśród użytkowników, które mogą stanowić zagrożenie”.[70]

SOR także w ramach diagnozy odnosi się do elementów bezpieczeństwa narodowego sensu stricte, stwierdzając w swojej treści, że m.in. „Zmienia się międzynarodowe środowisko bezpieczeństwa Polski. Konflikty w bezpośrednim lub bliskim sąsiedztwie Polski, niestabilność na południowej flance Sojuszu Północnoatlantyckiego i Unii Europejskiej oraz próby zmierzające do zmiany układu sił i odbudowy strefy wpływów, również przy wykorzystaniu środków militarnych oraz ekonomicznych, to obecnie najważniejsze czynniki wpływające na bezpieczeństwo Polski i całego regionu. Dużymi wyzwaniami dla Unii Europejskiej i jej państw członkowskich są zagrożenie terroryzmem oraz fala migracji. Rośnie znaczenie zagrożeń hybrydowych oraz dla cyberbezpieczeństwa, które mogą utrudnić sprawne funkcjonowanie państwa. Równocześnie aktualność zachowują wyzwania o charakterze gospodarczym, społecznym, demograficznym, technologicznym, ekologicznym, związane z globalizacją, przepływem informacji, zorganizowaną przestępczością, handlem bronią, pandemiami itp”.[71]

Ponadto w tej części diagnozy SOR zwraca się uwagę na korelację, wedle której „wraz z rozwojem i upowszechnieniem dostępu do internetu, wzrosło znaczenie cyberbezpieczeństwa, które dla przedsiębiorców (a szerzej – gospodarki) oznacza zapewnienie ciągłości funkcji biznesowych w tym ochronę poufnych danych i bezpieczeństwo zgromadzonych informacji. Natomiast w skali państwa oznacza ochronę obywateli oraz państwowej infrastruktury przed atakiem czy naruszeniem integralności”.[72]

W ramach proponowanych w tym obszarze działań SOR wskazuje na m.in.

- konieczność zapewnienia „systemu łączności dla potrzeb kierowania bezpieczeństwem narodowym, szybkiej i niezawodnej wymiany informacji niejawnych oraz jego sprawności i odporności na zagrożenia w cyberprzestrzeni”;[73]
- jak również wskazuje na niezbędność podjęcia działań na rzecz zapewnienia zdolności państwa do obrony oraz przeciwstawienia się agresji, w tym zdolności odstraszania, również przeciw zagrożeniom hybrydowym i w cyberprzestrzeni;[74]
- zwiększenie odporności infrastruktury krytycznej, w tym na cyberzagrożenia;[75]
- kształtowanie kapitału społecznego na rzecz bezpieczeństwa, m.in. poprzez podtrzymywanie i upowszechnianie wartości patriotycznych, rozwój świadomości narodowej, obywatelskiej i kulturowej oraz pogłębianie umiejętności rozpoznawania zagrożeń w życiu codziennym, w tym w cyberprzestrzeni.[76]

69 *Ibidem*

70 *Ibidem*, s. 321.

71 *Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*, Warszawa 2017, s. 353.

72 *Ibidem*, s. 355.

73 *Ibidem*, s. 357.

74 *Ibidem*, s. 358.

75 *Ibidem*, s. 359.

76 *Ibidem*.

Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020

Aktualne obowiązuje „Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej" w wersji z 2020 roku (dalej: Strategia 2020). Podobnie jak wcześniejsze strategie bezpieczeństwa narodowego, dokument został przyjęty w oparciu o art. 4a ust.1 pkt 1 ustawy z dnia 21 listopada 1967 r. – o powszechnym obowiązku obrony Rzeczypospolitej Polskiej. Zwrócić jednak należy uwagę, że od kilku miesięcy nową podstawę dla tworzenia strategii bezpieczeństwa narodowego stanowi art. 24 ust. 1 pkt 2 ustawy z dnia 11 marca 2022 r. – o obronie Ojczyzny.[77] Prezydent Rzeczypospolitej Polskiej Andrzej Duda w dniu 12 maja 2020 r., na wniosek Prezesa Rady Ministrów Mateusza Morawieckiego, zatwierdził Strategię Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej. Strategia 2020 liczy 37 stron, a kwestiom cyberbezpieczeństwa poświęca cały podrozdział w ramach Filaru I „Bezpieczeństwo Państwa I Obywateli".

Wcześniej jednak, jeszcze na etapie definiowania aktualnego „środowiska bezpieczeństwa" zauważono, że „Federacja Rosyjska prowadzi również działania poniżej progu wojny (o charakterze hybrydowym), niosące ryzyko wybuchu konfliktu (w tym niezamierzonego, wynikającego z gwałtownej eskalacji w rezultacie incydentu, szczególnie militarnego), a także podejmuje wszechstronne i kompleksowe działania za pomocą środków pozamilitarnych (w tym: cyberataki, dezinformacja) celem destabilizacji struktur państw i społeczeństw zachodnich oraz wywoływania podziałów wśród państw sojuszniczych. Należy przyjąć, że Federacja Rosyjska będzie kontynuowała politykę podważania obecnego ładu międzynarodowego, opartego na prawie międzynarodowym, w celu odbudowy pozycji mocarstwowej i stref wpływów".[78]

Jak pokazał czas, już w niecałe dwa lata później, Federacja Rosyjska dokonała konwencjonalnej inwazji[79] (w ramach tzw. „operacji specjalnej") na terytorium Ukrainy.[80] Ten pełnowymiarowy konflikt, obejmuje działania na lądzie, morzu i w powietrzu, ale też w przestrzeni cybernetycznej. Dokonywanie są ataki za pośrednictwem sieci mające wywołać poczucie strachu, destabilizacji, a także służyć dezinformacji i propagandzie.[81]

Strategia 2020 zauważa także, że „(...) działania poniżej progu wojny, w tym działania o charakterze hybrydowym, w dalszym ciągu będą pozostawać istotnym środkiem polityki, służącym zarówno podmiotom państwowym, jak i pozapaństwowym do osiągania ich celów. Można spodziewać się dalszego rozwoju zdolności do prowadzenia działań w wielu wymiarach, w tym w cyberprzestrzeni[82] i w przestrzeni kosmicznej".[83]

Strategia 2020 postuluje także, by w kontekście rewolucji cyfrowej „uwzględnić szczególną rolę cyberprzestrzeni oraz przestrzeni informacyjnej. Stwarza to również pole do dezinformacji i manipulacji

77 *Ustawa z dnia 11 marca 2022 o obronie Ojczyzny*, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000655, dostęp: 31.08.2022.

78 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020, s. 6.

79 Należy zauważyć, że w przeddzień zbrojnej inwazji doszło do kolejnego incydentu cybernetycznego, będącego – podobnie jak w przypadku problemów z 15 lutego 2022 r. – atakiem DDoS. Jak podaje blog omegasoft.pl „Atak DDoS (ang. *distributed denial of service*, czyli rozproszona odmowa usługi) to atak na system komputerowy lub usługę sieciową mający na celu uniemożliwienie działania poprzez zajęcie wszystkich wolnych zasobów. Przeprowadza się go równocześnie z wielu komputerów. Na dany sygnał atakujące urządzenia zaczynają jednocześnie atakować system ofiary, zasypując go fałszywymi próbami skorzystania z jego usług. Prowadzi to do wyczerpania dostępnych zasobów, a w efekcie do przerwy w działaniu systemu lub jego zawieszenia na dłuższy czas.", [na:] https://www.omegasoft.pl/blog/wojna-cybernetyczna-atak-na-ukraine-to-nie-tylko-dzialania-militarne/, dostęp: 31.08.2022.

80 Już po zajęciu Krymu przez Rosję i wojnie w Donbasie Ukraina była celem wielu ataków cyberwojennych. Za najgłośniejsze, skierowane przeciw niej uchodzą: wiper NotPetya (zwany bardziej jako Petya; wiper - złośliwe oprogramowanie, którego celem jest wyczyszczenie nośnika danych podłączonego do komputera, który infekuje, np. dysk twardy) oraz atak zespołu hakerskiego Sandworm Team (rzekomo jednostką cybermilitarną GRU, zwaną również Unit 74455), który jako jedyny w historii, zdołał wywołać rzeczywiste przerwy w dostawie prądu, po ataku na ukraińskie zakłady elektryczne w 2015 i 2016 roku, [na:] https://mlodytechnik.pl/news/30858-cyberatak-na-ukraine, dostęp: 31.08.2022.

81 *Wojna cybernetyczna – atak na Ukrainę to nie tylko działania militarne*, [na:] https://www.omegasoft.pl/blog/wojna-cybernetyczna-atak-na-ukraine-to-nie-tylko-dzialania-militarne/, dostęp: 31.08.2022.

82 Jak zauważa M. Duszczyk, „W ciągu ostatnich miesięcy wojsko stało się głównym celem hakerów szukających ofiar nad Wisłą. To novum, bo wcześniej najczęściej uderzali w sektor edukacji, badań i nauki(...)Co ciekawe, za uderzeniami w armię stoją grupy powiązane z Moskwą, Mińskiem i Pekinem. Eksperci wymieniają choćby takie hakerskie zespoły, jak UNC1151 (znana też jako Ghostwriter), wiązana z białoruskim reżimem, wspierane przez Kreml Fancy Bear (nazywana też APT28) i Killnet, czy Mustang Panda (kojarzona z Chinami).", M. Duszczyk, *Zmasowane cyberataki Rosji, Białorusi i Chin na polską armię*, „Rzeczpospolita" z 2.08.2022, https://www.rp.pl/gospodarka/art36801221-zmasowane-cyberataki-rosji-bialorusi-i-chin-na-polska-armie, dostęp: 31.08.2022.

83 Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020, Warszawa 2020, s. 7.

informacją, co wymaga prowadzenia skutecznych działań z zakresu komunikacji strategicznej." Należy podkreślić tutaj słuszność tego postulatu przywołując chociażby informację ze strony Krajowego Instytutu Cyberbezpieczeństwa, wskazującej, że ostatni czas to masowa dezinformacja i wzrost incydentów nawet o 20 000%![84]

W części poświęconej „Zarządzaniu bezpieczeństwem narodowym" postuluje się pkt 1.1. Zintegrowanie zarządzania bezpieczeństwem narodowym, w tym kierowanie obroną państwa oraz budowanie zdolności adaptacyjnych. W ramach tej części wskazuje się m.in. na potrzebę zintegrowania systemu „zarządzania bezpieczeństwem narodowym, w tym kierowania obroną państwa, umożliwiając połączenie procesów, procedur i praktyk działania, poprzez scalenie dotychczas funkcjonujących systemów, w szczególności kierowania bezpieczeństwem narodowym, zarządzania kryzysowego oraz cyberbezpieczeństwa"[85] co w rezultacie ma zapewnić zdolność do szybkiej adaptacji wobec pojawiających się nowych wyzwań i zagrożeń oraz identyfikacji szans.

Z kolei w części „Odporność państwa i obrona powszechna" w pkt. 2.10 zwraca się uwagę na konieczność rozwoju „zdolności państwa w zakresie zapobiegania i reagowania na zagrożenia o charakterze terrorystycznym oraz zwalczania przestępczości zorganizowanej, z uwzględnieniem działalności przestępczej w cyberprzestrzeni".[86]

W kolejnej części Strategia 2020 w pkt. 3.10 za cel wskazuje uzyskanie zdolności operacyjnych do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni, a także wyznacza niezwykle istotny z perspektywy państwa polskiego cel rozwoju wojska obrony cyberprzestrzeni oraz budowy zdolności do prowadzenia działań w przestrzeni kosmicznej, także w kontekście do działań informacyjnych.[87]

Podrozdział 4 Strategii 2020 zatytułowany jest „Cyberbezpieczeństwo". W jego treści zwraca się uwagę na konieczność podniesienia poziomu odporności na cyberzagrożenia oraz zwiększenia poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji.[88] Realizacji tej dyrektywy, służą cele szczegółowe:[89]

- Zwiększanie poziomu odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnięcie zdolności do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia (pkt 4.1);
- Wzmocnienie defensywnego potencjału państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa (pkt 4.2.);
- Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni (pkt 4.3.);
- Rozwinięcie krajowej zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa (pkt 4.4);
- Rozwinięcie kompetencji, wiedzy oraz świadomości zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa (pkt 4.5);
- Wzmocnienie i rozbudowanie potencjału państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także

84 KICB, *Masowa Dezinformacja W Mediach Społecznościowych,* Sierpień 2022, [na:] https://kicb.pl/masowa-dezinformacja-w-mediach-spolecznosciowych/, dostęp: 31.08.2022. Por. *RCB ostrzega przed fałszywymi narracjami o wojnie w Ukrainie. W sieci masowa dezinformacja, KPRM wydaje alert,* [na:] https://www.wirtualnemedia.pl/artykul/falszywa-narracja-wojna-ukraina-na-co-uwazac-rzadowe-centrum-bezpieczenstwa, dostęp: 31.08.2022.

85 *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020, s. 13.

86 *Ibidem*, s. 16.

87 *Ibidem* , s. 19.

88 *Ibidem*, s. 20.

89 *Ibidem*.

współpracę z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami – zarówno z sektora publicznego, jak i prywatnego (pkt 4.6.).

Ww. cele Strategii 2020 w dużej mierze znajdują swoje doprecyzowanie w obowiązującej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, a przejawami ich wdrażania jest m.in. realizacja i rozwój krajowego systemu cyberbezpieczeństwa i powołanie nowej instytucji – Centralnego Biura Zwalczania Cyberprzestępczości oraz Wojsk Obrony Cyberprzestrzeni o czym będzie mowa w dalszej części raportu.



Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2013

Dokumentem rangowo niższym, ale stanowiącym istotny krok na drodze tworzenia aktualnej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 było przyjęcie Polityki Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej (Dalej: Polityka Cyberprzestrzeni RP). Podkreśla się, że był to pierwszy dokument strategiczny w zakresie cyberbezpieczeństwa w Polsce,[90] pomimo, że został on przyjęty uchwałą Rady Ministrów 25 czerwca 2013 roku i obejmował swoim zakresem tylko administrację rządową.[91]

Dokument ten został opracowany w Ministerstwie Administracji i Cyfryzacji, we współpracy z Agencją Bezpieczeństwa Wewnętrznego, w oparciu o: omówiony 9 marca 2009 r. przez Komitet Stały Rady Ministrów dokument „Rządowy program ochrony cyberprzestrzeni RP na lata 2009-2011 – założenia", okresowe raporty o stanie bezpieczeństwa obszaru gov.pl, publikowane przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT. GOV.PL, decyzję Przewodniczącego Komitetu Rady Ministrów do spraw Cyfryzacji nr 1/2012 z dnia 24 stycznia 2012r. w przedmiocie powołania Zespołu zadaniowego do spraw ochrony portali rządowych.[92]

Polityka Cyberprzestrzeni RP to dokument 24 stronicowy, podzielony na 6 części:

1. GŁÓWNE PRZESŁANKI I ZAŁOŻENIA POLITYKI OCHRONY CYBERPRZESTRZENI RP
2. UWARUNKOWANIA I PROBLEMY OBSZARU CYBERPRZESTRZENI
3. GŁÓWNE KIERUNKI DZIAŁAŃ
4. WDROŻENIE I MECHANIZMY REALIZACJI ZAPISÓW DOKUMENTU
5. FINANSOWANIE
6. OCENA SKUTECZNOŚCI POLITYKI

Celem strategicznym omawianego dokumentu było osiągnięcie akceptowalnego poziomu bezpieczeństwa cyberprzestrzeni państwa. Dokument ten wyznaczał także istotne cele szczegółowe, a mianowicie:

- Zwiększenie poziomu bezpieczeństwa infrastruktury teleinformatycznej państwa;
- Zwiększenie zdolności do zapobiegania cyberzagrożeniom oraz ich zwalczania;
- Zmniejszenie skutków incydentów godzących w bezpieczeństwo teleinformatyczne;
- Określenie kompetencji podmiotów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni;
- Stworzenie spójnego dla wszystkich podmiotów administracji rządowej systemu zarządzania bezpieczeństwem cyberprzestrzeni oraz ustanowienie wytycznych w tym zakresie dla podmiotów niepublicznych;
- Stworzenie trwałego systemu koordynacji i wymiany informacji pomiędzy podmiotami odpowiedzialnymi za bezpieczeństwo cyberprzestrzeni oraz jej użytkownikami;
- Zwiększenie świadomości użytkowników w zakresie metod i środków bezpieczeństwa w cyberprzestrzeni."[93]

Ważnym elementem Polityki Ochrony Cyberprzestrzeni RP było wdrożenie mechanizmu szacowania ryzyka przez każdą jednostkę administracji rządowej, która miała co roku przekazywać sprawozdanie ministrowi właściwemu ds. informatyzacji. Dodatkowo każda jednostka organizacyjna administracji rządowej zobligowania została do ustanowienia systemu zarządzania bezpieczeństwem informacji oraz wyznaczenia pełnomocnika ds. bezpieczeństwa cyberprzestrzeni.[94]

90 *Polityka ochrony cyberprzestrzeni RP*, [na:] https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/, dostęp: 31.08.2022.

91 *Ibidem*.

92 *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 3.

93 *Ibidem*, s. 6.

94 Polityka ochrony cyberprzestrzeni RP, [na:] https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/, dostęp: 31.08.2022.

Zgodnie z Polityką Cyberprzestrzeni RP do zadań tego pełnomocnika należało przede wszystkim:[95]

- realizacja obowiązków wynikających z przepisów aktów prawnych właściwych dla zapewnienia bezpieczeństwa cyberprzestrzeni;
- opracowanie i wdrożenie procedur reagowania na incydenty komputerowe, które będą obowiązywały w organizacji;
- identyfikacja i prowadzenie cyklicznych analiz ryzyka;
- przygotowanie planów awaryjnych oraz ich testowanie;
- opracowanie procedur zapewniających informowanie właściwych zespołów CERT o:
    a) wystąpieniu incydentów komputerowych,
    b) zmianie lokalizacji jednostki organizacyjnej, danych kontaktowych, itp.;

Drugim niezwykle ważnym elementem wdrożonym przez Politykę Cyberprzestrzeni RP był trzypoziomowy Krajowy System Reagowania na Incydenty Komputerowe. W Poziomie I minister właściwy ds. informatyzacji odpowiadał za koordynację. Poziom II to reagowanie na incydenty komputerowe, które przypisane zostało do kompetencji Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL – realizującego jednocześnie zadania głównego narodowego zespołu odpowiadającego za koordynację obsługi incydentów komputerowych w obszarze cyberprzestrzeni RP oraz Resortowego Centrum Zarządzania Bezpieczeństwem Sieci i Usług Teleinformatycznych realizującego zadania w sferze militarnej. Poziom III – w ramach tego elementu, administratorzy odpowiadają za poszczególne systemy teleinformatyczne w cyberprzestrzeni.[96]

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022

Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej 2013 została zastąpiona przez dokument o nazwie „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022" (dalej: Krajowe Ramy 2017), opracowany przez grupę składającą się z przedstawicieli resortów: cyfryzacji, obrony narodowej, spraw wewnętrznych i administracji oraz przedstawicieli Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego. 9 maja 2017 r. Prezes Rady Ministrów Beata Szydło podpisała uchwałę nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. w sprawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022.[97] Zakres Krajowych Ram Polityki Cyberbezpieczeństwa obejmował, w szczególności:[98]

- cele w zakresie bezpieczeństwa teleinformatycznego,
- główne podmioty zaangażowane we wdrażanie krajowych ram polityki w zakresie bezpieczeństwa teleinformatycznego,
- ramy zarządzania służące realizacji celów krajowych ram polityki w zakresie bezpieczeństwa teleinformatycznego, na potrzebę zapobiegania i reagowania w odniesieniu do incydentów oraz przywracania stanu normalnego zakłóconego incydentem, w tym zasady współpracy pomiędzy sektorami publicznym i prywatnym,
- podejście do oceny ryzyka,

95 *Ibidem*, s. 13.

96 *Ibidem*, s. 19.

97 *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, [na:]* https://www.gov.pl/web/cyfryzacja/krajowe-ramy-polityki-cyberbezpieczenstwa, dostęp: 31.08.2022.

98 *Ibidem*.

- kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa,
- działania odnoszące się do planów badawczo-rozwojowych w zakresie bezpieczeństwa teleinformatycznego,
- podejście do współpracy międzynarodowej w zakresie cyberbezpieczeństwa.

Celami Krajowych Ram 2017 było:[99]

- oddziaływanie w sposób bezpośredni na podmioty administracji rządowej, a w sposób pośredni, po przyjęciu z inicjatywy Rady Ministrów przepisów prawa powszechnego, na pozostałe podmioty władzy publicznej, przedsiębiorców oraz obywateli, aby zapewnić im wysoki poziom bezpieczeństwa w zakresie świadczenia lub korzystania z usług kluczowych oraz usług cyfrowych;
- osiągnięcie zdolności do skoordynowanych działań w skali kraju,
- wzmocnienie zdolności do przeciwdziałania zagrożeniom dla cyberbezpieczeństwa,
- zwiększanie potencjału narodowego oraz kompetencji w zakresie bezpieczeństwa w cyberprzestrzeni,
- zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa.

Ten 29-stronicowy dokument został przyjęty z perspektywą 5-letnią, a Koordynatorem odpowiedzialnym za wdrożenie dokumentu mianowany został Minister Cyfryzacji. Już na wstępie założono, że po dwóch latach od przyjęcia dokumentu będzie on podlegał przeglądowi i ocenie jego oddziaływania. Wyniki przeglądu zostały przedstawione Radzie Ministrów. Zgodnie z postanowieniami Krajowych Ram 2017 Koordynator po 6 miesiącach od przyjęcia dokumentu, we współpracy z członkami Rady Ministrów, kierownikami urzędów centralnych, Dyrektorem Rządowego Centrum Bezpieczeństwa opracował Plan działań na rzecz jego wdrożenia. Organy wymienione powyżej uwzględniły w swoich działaniach problematykę cyberbezpieczeństwa w zakresie zgodnym z ustawowymi kompetencjami.[100] Plan działań obejmował w szczególności:[101]

- nazwę celu szczegółowego,
- nazwę zadania,
- typ działania – działanie: legislacyjne, organizacyjne, technologiczne, edukacyjne, informacyjne, promocyjne, inne,
- podejmowane przedsięwzięcia lub narzędzia realizacji,
- harmonogram – termin rozpoczęcia i termin zakończenia podejmowanej inicjatywy,
- organ lub organy – organ wiodący i organy współpracujące przy realizacji zadania,
- oczekiwane efekty wynikające z realizacji zadania,
- szacunkowy koszt realizacji zadania.

Koordynator został zobowiązany także do corocznego przygotowania sprawozdania o postępach wdrażania Krajowych Ram 2017 za rok poprzedni na podstawie informacji otrzymywanych od podmiotów zaangażowanych w ich realizację, a przygotowane sprawozdania miały być przedkładane Radzie Ministrów.[102]

99 *Ibidem.*

100 *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022, [na:]* https://www.gov.pl/web/cyfryzacja/krajowe-ramy-polityki-cyberbezpieczenstwa, dostęp: 31.08.2022.

101 *Ibidem.*

102 *Ibidem.*

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024

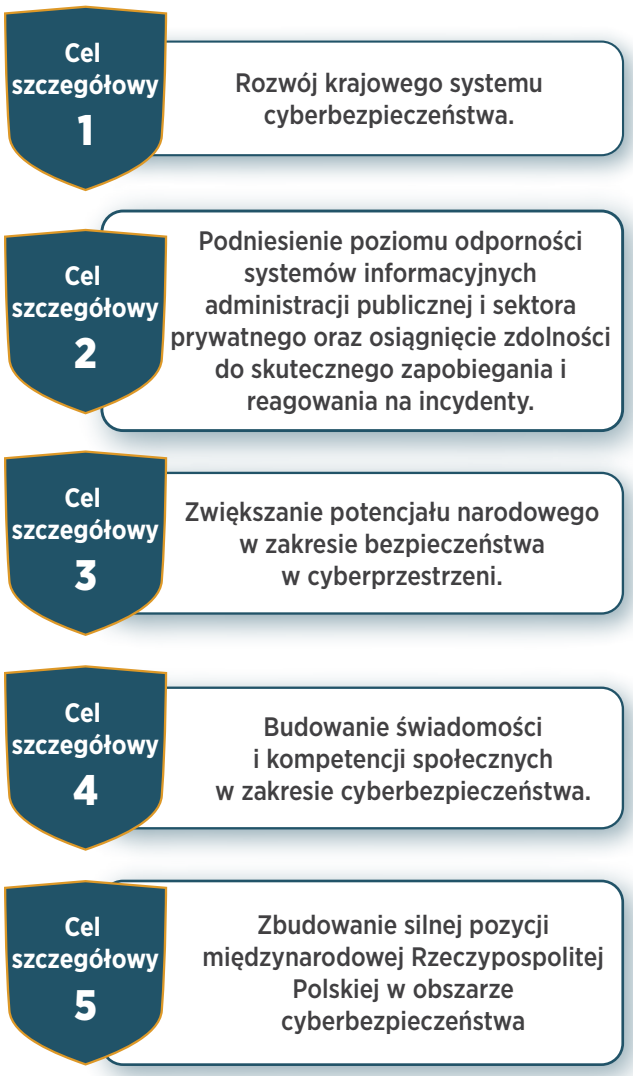
Przyjęcie w 2018 r. ustawy o krajowym systemie cyberbezpieczeństwa stworzyło podstawy prawne i organizacyjne dla opracowania Strategii Cyberbezpieczeństwa RP na lata 2019-2024 zastępującej Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Strategia rozszerza działania podjęte przez administrację rządową celem podniesienia poziomu cyberbezpieczeństwa w Rzeczypospolitej Polskiej i zgodnie z ustawą o Krajowym Systemie Cyberbezpieczeństwa uwzględnia w szczególności:

- cele i priorytety w zakresie cyberbezpieczeństwa;
- podmioty zaangażowane we wdrażanie i realizację Strategii;
- środki służące realizacji celów Strategii;
- określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym;
- podejście do oceny ryzyka;
- działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa;
- działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa.

Zamierzeniem omawianej strategii jest określenie celów strategicznych oraz odpowiednich środków politycznych i regulacyjnych, mających na celu uzyskanie wysokiego poziomu cyberbezpieczeństwa, a także zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń. Zgodnie ze strategią realizacja celów strategicznych ma wpływać na podniesienie bezpieczeństwa narodowego, zwiększenie skuteczności organów ścigania i wymiaru sprawiedliwości w wykrywaniu i zwalczaniu cyberprzestępstw oraz działań o charakterze hybrydowym (w tym działań o charakterze terrorystycznym) i szpiegowskim w cyberprzestrzeni.[103]

Celem głównym strategii jest podniesienie poziomu odporności na cyberzagrożenia, a także zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Poniższa tabela określa główne cele szczegółowe omawianego dokumentu.

Rys. 4. Cele szczegółowe zawarte w Strategii Cyberbezpieczeństwa RP na lata 2019-2024



103 *Strategia Cyberbezpieczeństwa RP na lata 2019-2024, str. 8*

Poniżej znajduje się zakres celów szczegółowych uwzględnionych w omawianej strategii.

Cel szczegółowy 1 - Rozwój krajowego systemu cyberbezpieczeństwa:

- Wdrożenie i ocena funkcjonowania przepisów o krajowym systemie cyberbezpieczeństwa;
- Podniesienie efektywności funkcjonowania krajowego systemu cyberbezpieczeństwa;
- Rozbudowa systemu wymiany informacji na potrzeby kierowania bezpieczeństwem narodowym;
- Zwiększenie cyberbezpieczeństwa usług kluczowych i cyfrowych oraz infrastruktury krytycznej;
- Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym;
- Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym;
- Opracowanie i wdrożenie Narodowych Standardów Cyberbezpieczeństwa oraz promowanie dobrych praktyk i zaleceń.

Cel szczegółowy 2 - Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty:

- Bezpieczeństwo łańcucha dostaw;
- Testy i audyty cyberbezpieczeństwa.

Cel szczegółowy 3 - Zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni:

- Rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa;
- Nastawienie na rozwój współpracy między sektorem publicznym i prywatnym;
- Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa;
- Uzyskanie zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni.

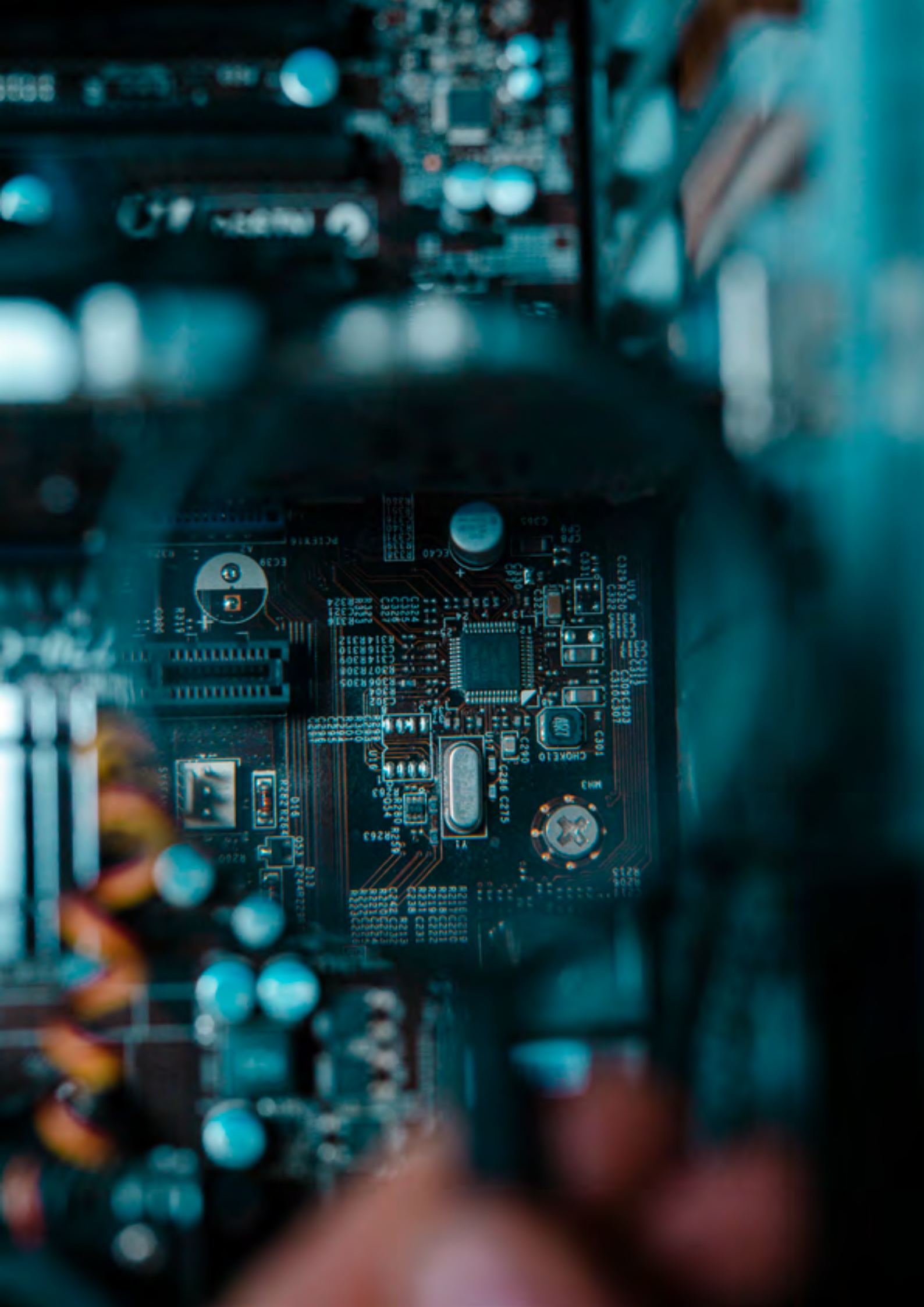
Cel szczegółowy 4 - Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa:

- Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej;
- Stworzenie warunków do bezpiecznego korzystania z cyberprzestrzeni przez obywateli.

Cel szczegółowy 5 - Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa:

- Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym;
- Aktywna współpraca międzynarodowa na poziomie operacyjnym i technicznym.

Należy dodać, że Strategia ustalana jest na okres pięcioletni z możliwością wprowadzenia zmian w okresie jej obowiązywania. Ponadto minister właściwy do spraw informatyzacji we współpracy z Pełnomocnikiem, innymi ministrami i właściwymi kierownikami urzędów centralnych dokonuje przeglądu Strategii co 2 lata. Obowiązkiem ministra jest również przekazanie Strategii Komisji Europejskiej w terminie 3 miesięcy od dnia jej przyjęcia przez Radę Ministrów.



KRAJOWY SYSTEM CYBERBEZPIECZEŃSTWA

W Polsce jednym z podstawowych aktów prawnych regulujących kwestie związane z cyberbezpieczeństwem jest ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zwana dalej jako „u.k.s.c", która implementuje do polskiego porządku prawnego Dyrektywę NIS[104].

Zgodnie z art. 1 u.k.s.c. określa organizację krajowego systemu cyberbezpieczeństwa oraz zadania i obowiązki podmiotów wchodzących w skład tego systemu, sposób sprawowania nadzoru i kontroli w zakresie stosowania przepisów ustawy oraz zakres Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej.

Jej celem 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.

Rys. 5. Definicja obsługi incydentów
(zgodnie z definicją zawartą w art. 2 u.k.s.c.)



Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560, dostęp: 31.08.2022.



104 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, [na:] https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=celex:32016L1148, dostęp: 31.08.2022.

Ustawa wprowadza trzypoziomowy podział incydentów – pierwszy oznacza wszystkie zdarzenia o niekorzystnym wpływie na cyberbezpieczeństwo, drugi to incydenty poważne (występujące u operatorów usług kluczowych), istotne (występujące u dostawców usług cyfrowych) oraz w podmiocie publicznym (występujące w podmiotach publicznych) natomiast trzeci definiuje je jako incydenty krytyczne (niosące za sobą większe zagrożenie, niż pozostałe).

Rys. 6. Poziomy incydentów

Poziom I

INCYDENT ZWYKŁY
Zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo – ten incydent nie podlega zgłoszeniu, ale też należy go obsługiwać.

Poziom II

INCYDENT POWAŻNY
Powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości działania świadczonej usługi kluczowej - progi incydentu poważnego zostaną określone w rozporządzeniu.

INCYDENT ISTOTNY
Ma istotny wpływ na świadczenie usługi cyfrowej

INCYDENT W PODMIOCIE PUBLICZNYM
powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny.

Poziom III

INCYDENT KRYTYCZNY
Incydent, skutkujący znaczną szkodą dla bezpieczeństwa lub porządku publicznego, interesów międzynarodowych, interesów gospodarczych, działania instytucji publicznych, praw i wolności obywatelskich lub życia i zdrowia ludzi.

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560, dostęp: 31.08.2022.

Art. 4 u.k.s.c. określa podmioty objęte krajowym systemem cyberbezpieczeństwa tj. operatorów usług kluczowych, dostawców usług, CSIRT MON, CSIRT NASK, CSIRT GOV[105], sektorowe zespoły cyberbezpieczeństwa, jednostki sektora finansów publicznych, instytuty badawcze, Narodowy Bank Polski, Bank Gospodarstwa Krajowego, Urząd Dozoru Technicznego, Polską Agencję Żeglugi Powietrznej, Polskie Centrum Akredytacji, Narodowy Fundusz Ochrony Środowiska i Gospodarki Wodnej oraz wojewódzkie fundusze ochrony środowiska i gospodarki wodnej, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa, Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Kolegium do Spraw Cyberbezpieczeństwa.

W rozdziale II u.k.s.c. określony został tryb identyfikacji operatorów usług kluczowych. Jak wynika z art. 5 operatorem usługi kluczowej jest podmiot posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory i podsektory oraz rodzaj podmiotów są określone w odrębnym dokumencie (załącznik nr.1 do u.k.s.c.).

„Identyfikacja operatorów usług kluczowych ma przy tym jednocześnie służyć skutecznemu reagowaniu na wyzwania związane z zapewnieniem cyberbezpieczeństwa poprzez przyjęcie całościowego podejścia na poziomie Unii, „obejmującego wymogi dotyczące budowania i planowania wspólnych minimalnych zdolności, wymianę informacji, współpracę oraz wspólne wymogi w zakresie bezpieczeństwa dla operatorów usług kluczowych i dostawców usług cyfrowych" (por. pkt 6 preambuły dyrektywy NIS)".[106]

105 Zgodnie z art. 2 u.k.s.c. użyte w ustawie określenia oznaczają:

1) CSIRT GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;

2) CSIRT MON – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;

3) CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

106 M. Wilbrandt-Gotowicz, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, Rozdział 2.

Rys. 7. Zadania Pojedynczego Punktu Kontaktowego.



- tworzenie ram prawnych funkcjonowania obszaru cyberbezpieczeństwa RP, w tym czuwanie nad ich spójnością
- pełnienie funkcji łącznika w celu zapewnienia współpracy pomiędzy podmiotami odpowiedzialnymi za cyberbezpieczeństwo
- gromadzenie i przetwarzanie informacji otrzymanych od m.in. operatorów usług kluczowych
- kontrolowanie spełniania przez podmioty świadczące usługi z zakresu cyberbezpieczeństwa wymagań organizacyjnych i technicznych
- przekazywanie na wniosek właściwego CSIRT, zgłoszenia incydentu poważnego lub incydentu istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej do pojedynczych punktów kontaktowych innych państw członkowskich UE
- zapewnienie reprezentacji RP w Grupie Współpracy
- zapewnienie współpracy z Komisją Europejską w dziedzinie cyberbezpieczeństwa
- koordynację współpracy między organami właściwymi ds. cyberbezpieczeństwa RP z odpowiednimi organami w państwach członkowskich UE

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa stron internetowych Rządu RP.

Art. 5 ust. 1 u.k.s.c. definiuje operatora usługi kluczowej jako podmiot spełniający łącznie trzy rodzaje przesłanek – ustrojowe (podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej), materialne (realizacja kryteriów wymienionych w art. 5 ust. 2 u.k.s.c) oraz przesłankę formalną (względem którego wydano decyzję administracyjną o uznaniu za operatora usługi kluczowej).

W rozdziale III u.k.s.c. zostały omówione regulacje, które swoim zakresem obejmują wdrożenie rozwiązań służących zapewnieniu cyberbezpieczeństwa w systemie informacyjnym państwa, obowiązki operatora usług kluczowych (uwzględniające zasady tworzenia i postępowania z dokumentacją dot. cyberbezpieczeństwa), a także zgłoszenia i obsługi incydentów, szczególnie tych kwalifikowanych jako incydenty poważne.

Ustawa (art. 8) wyjaśnia, iż operator usługi kluczowej wdraża system zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej, zapewniający:

- prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
- wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, w tym:
  - utrzymanie i bezpieczną eksploatację systemu informacyjnego,
  - bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu,
  - bezpieczeństwo i ciągłość dostaw usług, od których zależy świadczenie usługi kluczowej,
  - wdrażanie, dokumentowanie i utrzymywanie planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji,
  - objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym;

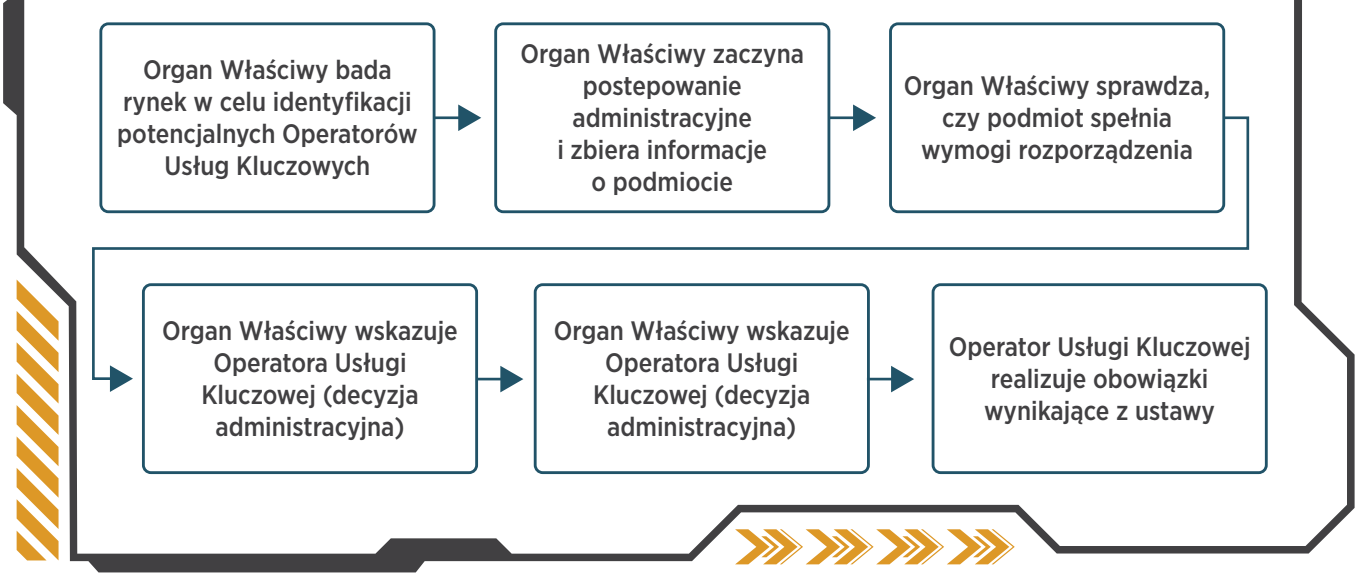
- zbieranie informacji o zagrożeniach cyberbezpieczeństwa i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej;
- zarządzanie incydentami;
- stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w tym:
  - stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
  - dbałość o aktualizację oprogramowania,
  - ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
  - niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub zagrożeń cyberbezpieczeństwa;
- stosowanie środków łączności umożliwiających prawidłową i bezpieczną komunikację w ramach krajowego systemu cyberbezpieczeństwa.

Natomiast art. 9 wskazuje na obowiązek wyznaczenia osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, a także obowiązek zapewnienia użytkownikowi usługi kluczowej dostępu do wiedzy w zakresie zagrożeń cyberbezpieczeństwa.

„Operator usługi kluczowej powinien wyznaczyć osobę, której zakres obowiązków będzie obejmował bieżące kontakty z podmiotami należącymi do krajowego systemu cyberbezpieczeństwa. Rozwiązanie to charakteryzuje się podobieństwami do przewidzianej treścią RODO instytucji Inspektora Ochrony Danych. Na podstawie art. 9 ust. 2 dane osoby wykonującej omawiane obowiązki powinny być przekazane w terminie 14 dni od dnia jej wyznaczenia do organu właściwego do spraw cyberbezpieczeństwa, właściwego CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowego zespołu cyberbezpieczeństwa. Obowiązek taki materializuje się również w przypadku zmiany takich danych."[107]

Należy również dodać, że operator usługi kluczowej ma obowiązek informacyjny w stosunku do osoby będącej użytkownikiem takiej usługi (może się to odbyć za pośrednictwem strony internetowej operatora). Te regulacje nie wymagają konieczności przesłania spersonalizowanych wiadomości przy wykorzystaniu poczty elektronicznej bądź innych środków komunikacji elektronicznej.

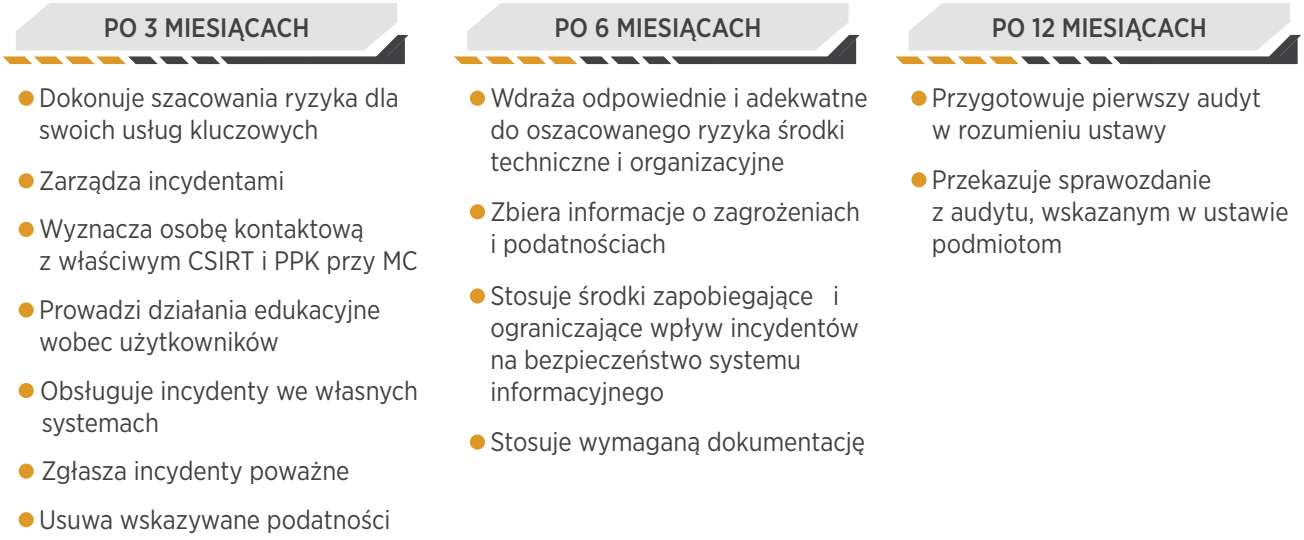
Rys. 8. Wyznaczanie operatorów usług kluczowych



Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz strony internetowe Rządu RP.

107 K. Świtała, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, art. 9.

Rys. 9. Obowiązki operatora usług kluczowych



Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz strony internetowe Rządu RP.

Na postawie art. 9 ust.1 u.k.s.c. operator usługi kluczowej informuje organ właściwy do spraw cyberbezpieczeństwa o tym, w których państwach członkowskich UE podmiot został uznany za operatora usługi kluczowej, jak również o dacie zakończenia świadczenia usługi kluczowej w terminie 3 miesięcy od zmiany tych danych.

Zgodnie z Art. 10 u.k.s.c. operator usługi kluczowej opracowuje, stosuje i aktualizuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej. Ponadto operator usługi kluczowej jest obowiązany do ustanowienia nadzoru nad dokumentacją dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, zapewniającego:

- dostępność dokumentów wyłącznie dla osób upoważnionych zgodnie z realizowanymi przez nie zadaniami;
- ochronę dokumentów przed niewłaściwym użyciem lub utratą integralności;
- oznaczanie kolejnych wersji dokumentów umożliwiające określenie zmian dokonanych w tych dokumentach.

Operator usługi kluczowej przechowuje dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej przez co najmniej 2 lata od dnia jej wycofania z użytkowania lub zakończenia świadczenia usługi kluczowej, z uwzględnieniem przepisów ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach (Dz. U. z 2018 r. poz. 217, 357, 398 i 650).

Operator usługi kluczowej będący jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej, wymienionych w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2018 r. poz. 1401), który posiada zatwierdzony plan ochrony infrastruktury krytycznej uwzględniający dokumentację dotyczącą cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, nie ma obowiązku opracowania dokumentacji, o której mowa wyżej.

Rada Ministrów określa, w drodze rozporządzenia, rodzaje dokumentacji, o której mowa wyżej, uwzględniając polskie normy oraz potrzebę zapewnienia cyberbezpieczeństwa podczas świadczenia usług kluczowych i ciągłości świadczenia tych usług.

Art. 11 u.k.s.c. dotyczy obsługi incydentów, zgłaszania incydentów poważnych i współdziałania przy obsłudze incydentu poważnego, a także incydentu krytycznego.

Rys. 10. Zadania Sektorowego Zespołu Cyberbezpieczeństwa



- przyjmowanie zgłoszeń o incydentach poważnych oraz wsparcie w ich obsłudze
- wspieranie operatorów usług kluczowych w wykonywaniu obowiązków
- analizowanie incydentów poważnych, wyszukiwanie powiązań pomiędzy incydentami oraz opracowywanie wniosków z ich obsługi
- współpraca z właściwym CSIRT NASK, CSIRT GOV, CSIRT MON w zakresie koordynowania obsługi incydentów poważnych
- SZC może przekazywać do innych państw i przyjmować od nich informacje o incydentach poważnych, w tym dot. dwóch lub większej liczby państw członkowskich UE
- SZC może otrzymywać zgłoszenia incydentu poważnego z innego państwa członkowskiego UE, dot. dwóch lub większej liczby państw. Takie zgłoszenia przekazuje do właściwego CSIRT NASK, CSIRT GOV, CSIRT MON oraz PPK

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560, dostęp: 31.08.2022.

Incydent, który został uznany za poważny powinien być zgłoszony niezwłocznie, nie dłużej niż w ciągu 24 godzin. Wymóg ten nie zwalnia operatora z obowiązku skutecznego przekazania zgłoszenia w sytuacji braku komunikacji elektronicznej (musi korzystać z innych dostępnych środków komunikacji). Ponadto, w razie powołania sektorowego zespołu cyberbezpieczeństwa w związku z wykryciem incydentu, to również z nim należy podjąć współpracę.

Operator usługi kluczowej jest zobowiązany do współdziałania i informowania o okolicznościach wystąpienia incydentu oraz do usunięcia podatności, które na skutek wystąpienia zagrożenia doprowadziły do powstania incydentu.

W art. 12 u.k.s.c. został określony zakres informacji przekazywanych uprawnionym podmiotom w związku ze zgłoszeniem incydentu poważnego. Pozwala to na odpowiednie rozpoznanie okoliczności zdarzenia i wdrożenia odpowiedniej reakcji. Takie zgłoszenie powinno zawierać dane podmiotu zgłaszającego, personalia osoby dokonującej zgłoszenia i uprawnionej do składania wyjaśnień, opis wpływu incydentu poważnego na świadczenie usługi kluczowej oraz podjęte działania zapobiegawcze i naprawcze.

Art. 13 u.k.s.c. dot. przekazywania przez operatora usługi kluczowej informacji (w postaci elektronicznej) dot. innych incydentów i zagrożeń dla cyberbezpieczeństwa do właściwego CSIRT.

Natomiast art. 14 u.k.s.c. wymaga od operatorów usługi kluczowej powołania wewnętrznych struktur odpowiedzialnych za cyberbezpieczeństwo lub zawarcia umowy z podmiotem świadczącym usługi z zakresu cyberbezpieczeństwa. Po zawarciu takiej umowy ma on obowiązek poinformować w ciągu 14 dni organ właściwy do spraw cyberbezpieczeństwa i właściwy CSIRT MON, CSIRT NASK, CSIRT GOV oraz w razie powołania sektorowy zespół cyberbezpieczeństwa o podmiocie, z którym została zawarta umowa, danych kontaktowych tego podmiotu, a także zakresie świadczonej usługi. Art. 15 u.k.s.c. zobowiązuje operatora usług kluczowych do przeprowadzenia audytu bezpieczeństwa systemu informacyjnego wykorzystanego do świadczenia usługi kluczowej. Taki audyt ma obowiązek być przeprowadzony raz na dwa lata (pierwszy audyt powinien zostać przeprowadzony w ciągu roku od dnia doręczenia decyzji o uznaniu za operatora usługi kluczowej). Na podstawie zebranych dokumentów i dowodów audytor sporządza pisemne sprawozdanie z odpowiednimi wnioskami, a następnie przekazuje je operatorowi usługi kluczowej wraz z dokumentacją audytu.

Zgodnie z treścią art. 15 ust. 7 u.k.s.c. operator usługi kluczowej przekazuje kopię sprawozdania z przeprowadzonego audytu na uzasadniony wniosek organu właściwego do spraw cyberbezpieczeństwa, dyrektora Rządowego Centrum Bezpieczeństwa (w przypadku gdy operator usługi kluczowej

jest jednocześnie właścicielem, posiadaczem samoistnym albo posiadaczem zależnym obiektów, instalacji, urządzeń lub usług wchodzących w skład infrastruktury krytycznej) oraz Szefa Agencji Bezpieczeństwa Wewnętrznego. Art. 16 u.k.s.c. określa terminy realizacji obowiązków przez operatora usługi kluczowej.

IV rozdział u.k.s.c. omawia status i obowiązki dostawcy usługi cyfrowej, obowiązki w zakresie wykrywania, rejestrowania, analizowania oraz klasyfikowania incydentów. Opisano w nim również zgłoszenie incydentu istotnego, a także omówiono zakres informacji przekazywanych przez dostawców usług cyfrowych. Do usług cyfrowych Digital Service Providers (DSP) zaliczane są: internetowe platformy handlowe, usługi przetwarzania w chmurze oraz wyszukiwarki internetowe. Z zakresu ustawy zostały wyjęte małe i mikroprzedsiębiorstwa.[108]

Rys. 11. Definicja usług cyfrowych zgodnie z załącznikiem nr 2 do u.k.s.c.

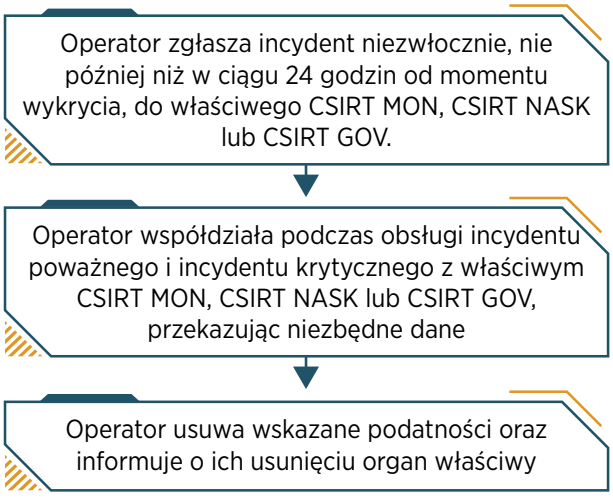


Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560, dostęp: 31.08.2022.

DSP zostały objęte lżejszą regulacją, niż operatorzy usług kluczowych ze względu na transgraniczny charakter usług cyfrowych i międzynarodową specyfikę podmiotów świadczących tego rodzaju usługi. Do ich obowiązków należy prowadzenie czynności umożliwiających wykrywanie, rejestrowanie, analizowanie oraz klasyfikowanie incydentów. Ponadto mają obowiązek zarządzać ryzkiem systemów informacyjnych, wykorzystywanych do świadczenia usługi cyfrowej. W przypadku wystąpienia istotnego incydentu, dostawca usługi cyfrowej musi przekazać informację do właściwego CSIRT nie później niż w ciągu 24 godzin od momentu wykrycia. DSP podlegają nadzorowi orangów właściwych, które są uprawnione do ich kontrolowania oraz nakładania kar finansowych.

Rozdział V u.k.s.c. zawiera opis obowiązków takich jak wyznaczenie osoby odpowiedzialnej za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zgłaszania i obsługi incydentu w podmiocie publicznym, informacje przekazywane do właściwego CSIRT oraz przepisy stosowane do podmiotu publicznego uznanego za operatora usługi kluczowej.

Rys. 12. Przekazywanie informacji o incydencie przez operatora usługi kluczowej zgodnie z u.k.s.c.



Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa oraz strony internetowe Rządu RP.

108 Art. 104 Ustawy o swobodzie gospodarczej z dnia 2 lipca 2004 r. definiuje mikroprzedsiębiorcę jako przedsiębiorcę, który w co najmniej jednym z dwóch ostatnich lat obrotowych zatrudniał średniorocznie mniej niż 10 pracowników oraz osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych, nieprzekraczający równowartości w złotych 2 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 2 milionów euro. Art. 105 tej ustawy określa małego przedsiębiorcę jako przedsiębiorcę, który zatrudniał średniorocznie mniej niż 250 pracowników oraz osiągnął roczny obrót netto ze sprzedaży towarów, wyrobów i usług oraz operacji finansowych nieprzekraczający równowartości w złotych 50 milionów euro, lub sumy aktywów jego bilansu sporządzonego na koniec jednego z tych lat nie przekroczyły równowartości w złotych 43 milionów euro.

Dyrektywa NIS daje dowolność w kwestii liczby powołanych CSIRT jeśli operatorzy usług kluczowych i dostawcy usług cyfrowych mają wyznaczony CSIRT, do którego będą raportować. Rozdział VI u.k.s.c. omawia trzy wyznaczone przez ustawodawcę CSIRT poziomu krajowego:

a. CSIRT NASK w strukturach Państwowego Instytutu Badawczego NASK;

b. CSIRT GOV w strukturach Agencji Bezpieczeństwa Wewnętrznego;

c. CSIRT MON w strukturach Ministerstwa Obrony Narodowej.

Zespoły funkcjonują od dłuższego czasu w obszarze cyberbezpieczeństwa kraju i mają jasno określony zakres podmiotów, które zobowiązane są do składania raportów i którym świadczą wsparcie.

Do zadań CSIRT MON, CSIRT NASK i CSIRT GOV należy:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
- przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydenty;
- klasyfikowanie incydentów, w tym incydentów poważnych oraz incydentów istotnych, jako incydenty krytyczne oraz koordynowanie obsługi incydentów krytycznych;
- zmiana klasyfikacji incydentów poważnych i incydentów istotnych;
- przekazywanie do właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV informacji technicznych dotyczących incydentu, którego koordynacja obsługi wymaga współpracy CSIRT;
- przeprowadzanie w uzasadnionych przypadkach badania urządzenia informatycznego lub oprogramowania w celu identyfikacji podatności, której wykorzystanie może zagrozić w szczególności integralności, poufności, rozliczalności, autentyczności lub dostępności przetwarzanych danych, które może mieć wpływ na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa;
- składanie wniosków w sprawie rekomendacji dla podmiotów krajowego systemu cyberbezpieczeństwa dotyczących stosowania urządzeń informatycznych lub oprogramowania, w szczególności w zakresie wpływu na bezpieczeństwo publiczne lub istotny interes bezpieczeństwa państwa;
- współpraca z sektorowymi zespołami cyberbezpieczeństwa w zakresie koordynowania obsługi incydentów poważnych, w tym dotyczących dwóch lub większej liczby państw członkowskich Unii Europejskiej i incydentów krytycznych oraz w zakresie wymiany informacji pozwalających przeciwdziałać zagrożeniom cyberbezpieczeństwa;

Rys. 13. Podział zakresu podmiotów pomiędzy trzy CSIRT poziomu krajowego

CSIRT ABW	CSIRT MON	CSIRT NASK
Administracja rządowa Narodowy Bank Polski Bank Gospodarstwa Krajowego	Podmioty podległe Ministrowi Obrony Narodowej Przedsiębiorstwa o szczególnym znaczeniu gospodarczo-obronnym	Pozostałe podmioty

Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560, dostęp: 31.08.2022.

- przekazywanie do innych państw, w tym państw członkowskich Unii Europejskiej i przyjmowanie z tych państw informacji o incydentach poważnych i incydentach istotnych dotyczących dwóch lub większej liczby państw członkowskich, a także przekazywanie do Pojedynczego Punktu Kontaktowego zgłoszenia incydentu poważnego i istotnego dotyczącego dwóch lub większej liczby państw członkowskich Unii Europejskiej;

- przekazywanie do Pojedynczego Punktu Kontaktowego (ministra właściwego ds. informatyzacji) zestawienia incydentów poważnych i istotnych zgłoszonych w poprzednim roku kalendarzowym;

- wspólne opracowywanie i przekazywanie ministrowi właściwemu do spraw informatyzacji części Raportu o zagrożeniach bezpieczeństwa narodowego, o którym mowa w art. 5a ust. 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym, dotyczącej cyberbezpieczeństwa;

CSIRT poziomu krajowego odpowiada również za zapewnienie zaplecza analitycznego oraz badawczo-rozwojowego poprzez:

- prowadzenie zaawansowanej analizy złośliwego oprogramowania oraz analizy podatności,

- monitorowanie wskaźników zagrożeń cyberbezpieczeństwa,

- rozwijania narzędzia i metod do wykrywania oraz zwalczania zagrożeń cyberbezpieczeństwa,

- prowadzenie analizy i opracowań standardów, rekomendacji i dobrej praktyki w zakresie cyberbezpieczeństwa,

- wspierania podmiotów krajowego systemu cyberbezpieczeństwa w budowaniu potencjału i zdolności w obszarze cyberbezpieczeństwa,

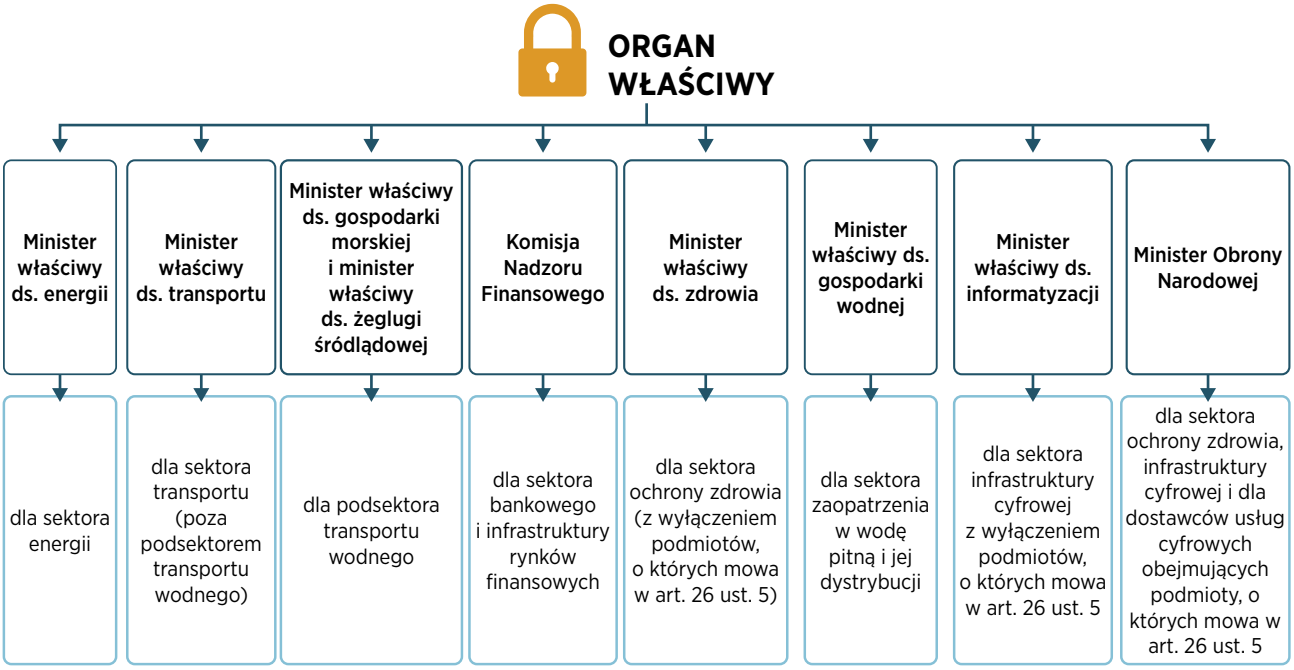
- prowadzenie działania z zakresu budowania świadomości w obszarze cyberbezpieczeństwa,

- współpracę w zakresie rozwiązań edukacyjnych w obszarze cyberbezpieczeństwa.

W rozdziale VII u.k.s.c. zostały omówione zasady udostępniania informacji i przetwarzania danych osobowych. Zgodnie z art. 37 u.k.s.c. do udostępniania informacji o podatnościach, incydentach i zagrożeniach cyberbezpieczeństwa oraz o ryzyku wystąpienia incydentów nie stosuje się ustawy z dnia 6 września 2001 r. o dostępie do informacji publicznej. Natomiast art. 38 u.k.s.c. informuje, iż nie udostępnia się informacji przetwarzanych na podstawie ustawy, jeżeli ich ujawnienie naruszyłoby ochronę interesu publicznego w odniesieniu do bezpieczeństwa lub porządku publicznego, a także negatywnie wpłynęłoby na prowadzenie postępowań przygotowawczych w sprawie przestępstw, ich wykrywania i ścigania. W art. 39 u.k.s.c. określono podstawy prawne, cele i zakres przetwarzania danych osobowych przez CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa, a także inne wskazane w tym przepisie podmioty. Jednocześnie w art. 40 u.k.s.c. ustawodawca określił podstawę prawną do przetwarzania informacji stanowiących tajemnice prawnie chronione oraz do ich udostępniania organom ścigania w związku z incydentem wyczerpującym znamiona przestępstwa. W art. 40 ust. 3 u.k.s.c. bez względu na obowiązki związane z przetwarzaniem informacji stanowiących tajemnice prawnie chronione ustawodawca wprowadził też samoistną tajemnicę CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowych zespołów cyberbezpieczeństwa.

W rozdziale VIII u.k.s.c. omówiono katalog organów właściwych do spraw cyberbezpieczeństwa, zadania organów właściwych do spraw cyberbezpieczeństwa, sposób przekazywania informacji na żądanie organów właściwych do spraw cyberbezpieczeństwa oraz możliwość powołania sektorowego zespołu cyberbezpieczeństwa.

Rys. 14. Organy właściwe do spraw cyberbezpieczeństwa



Źródło: Opracowanie własne na podstawie: Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560, dostęp: 31.08.2022.

Zgodnie z art. 41 u.k.s.c. organy właściwe do spraw cyberbezpieczeństwa przedstawia powyższy schemat.

Zgodnie z art. 42. u.k.s.c. organ właściwy do spraw cyberbezpieczeństwa:

- prowadzi bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej;
- wydaje decyzje o uznaniu podmiotu za operatora usługi kluczowej albo decyzje stwierdzające wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej;
- niezwłocznie po wydaniu decyzji o uznaniu za operatora usługi kluczowej albo decyzji stwierdzającej wygaśnięcie decyzji o uznaniu za operatora usługi kluczowej przekazuje wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu;
- składa wnioski o zmianę danych w wykazie operatorów usług kluczowych, nie później niż w terminie 6 miesięcy od zmiany tych danych;
- przygotowuje we współpracy z CSIRT NASK, CSIRT GOV, CSIRT MON i sektorowymi zespołami cyberbezpieczeństwa rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa, w tym wytyczne sektorowe dotyczące zgłaszania incydentów;
- monitoruje stosowanie przepisów ustawy przez operatorów usług kluczowych i dostawców usług cyfrowych;
- wzywa na wniosek CSIRT NASK, CSIRT GOV lub CSIRT MON operatorów usług kluczowych lub dostawców usług cyfrowych do usunięcia w wyznaczonym terminie podatności, które doprowadziły lub mogły doprowadzić do incydentu poważnego, istotnego lub krytycznego;
- prowadzi kontrole operatorów usług kluczowych i dostawców usług cyfrowych;
- może prowadzić współpracę z właściwymi organami państw członkowskich Unii Europejskiej za pośrednictwem Pojedynczego Punktu Kontaktowego;
- przetwarza informacje, w tym dane osobowe, dotyczące świadczonych usług kluczowych i usług cyfrowych oraz operatorów usług kluczowych

lub dostawców usług cyfrowych w zakresie niezbędnym do realizacji zadań wynikających z ustawy;

- uczestniczy w ćwiczeniach w zakresie cyberbezpieczeństwa organizowanych w Rzeczypospolitej Polskiej lub w Unii Europejskiej (np. defensywne ćwiczenia bezpieczeństwa teleinformatycznego Locked Shields).[109]

Ponadto ust. 3 art. 42 u.k.s.c. stanowi, iż organ właściwy do spraw cyberbezpieczeństwa może powierzyć realizację, w jego imieniu, niektórych zadań, o których mowa w ust. 1, jednostkom podległym lub nadzorowanym przez ten organ. Ust. 4. art. 42 u.k.s.c. stanowi, iż powierzenie następuje na podstawie porozumienia organu właściwego do spraw cyberbezpieczeństwa z podmiotami, o których mowa w ust. 3. Natomiast w porozumieniu, o którym mowa w ust. 4, określa się zasady sprawowania przez organ właściwy do spraw cyberbezpieczeństwa kontroli nad prawidłowym wykonywaniem powierzonych zadań. Organy właściwe do spraw cyberbezpieczeństwa i Pojedynczy Punkt Kontaktowy w uzasadnionych przypadkach współpracują z organami ścigania i organem właściwym do spraw ochrony danych osobowych.

Art. 43 opisuje proces przekazywania informacji na żądanie organów właściwych do spraw cyberbezpieczeństwa natomiast art. 44 zawiera ważną regulację dotyczącą sektorowych zespołów cyberbezpieczeństwa, które mogą być powoływane przez właściwe organy.

Rozdział IX precyzuje zadania ministra właściwego do spraw informatyzacji, który odpowiada za cywilne aspekty cyberbezpieczeństwa RP. Do tych zadań możemy zaliczyć m.in. realizację czynności technicznych i organizacyjnych w ramach krajowego systemu cyberbezpieczeństwa. Związane są one z gromadzeniem i udostępnianiem informacji, monitorowaniem wdrażania Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, zapewnieniem rozwoju i utrzymania systemu teleinformatycznego[110], a także z prowadzeniem Pojedynczego Punktu Kontaktowego, który odpowiada za współpracę z Komisją Europejską i przekazywaniem corocznych raportów (współpracuje z innymi państwami członkowskimi w zakresie cyberbezpieczeństwa oraz koordynuje współpracę pomiędzy organami właściwymi w kraju). Do jego zadań należy również prowadzenie działań informacyjnych na temat dobrych praktyk, programów edukacyjnych oraz szkoleń z poszerzania wiedzy i budowania świadomości w zakresie cyberbezpieczeństwa.

Rozdział X definiuje zdania Ministra Obrony Narodowej oraz proces nadzoru nad cyberobroną polskiego państwa. Do głównych zadań ministra możemy zaliczyć:

- współpracę Sił Zbrojnych Rzeczypospolitej Polskiej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej i organizacji międzynarodowych w obszarze obrony narodowej, w zakresie cyberbezpieczeństwa;
- zapewnienie zdolności Siłom Zbrojnym Rzeczypospolitej Polskiej w układzie sojuszniczym i koalicyjnym do prowadzenia działań militarnych w przypadku zagrożenia cyberbezpieczeństwa powodującego konieczność działań obronnych;
- rozwijanie umiejętności Sił Zbrojnych Rzeczypospolitej Polskiej w zakresie zapewnienia cyberbezpieczeństwa przez organizację specjalistycznych przedsięwzięć szkoleniowych;
- pozyskiwanie i rozwój narzędzi służących budowaniu zdolności zapewnienia cyberbezpieczeństwa w Siłach Zbrojnych Rzeczypospolitej Polskiej;
- kierowanie działaniami związanymi z obsługą incydentów w czasie stanu wojennego;
- ocenę wpływu incydentów na system obrony państwa;
- ocenę zagrożeń cyberbezpieczeństwa w czasie

109 NATO Locked Shields to największe międzynarodowe techniczne ćwiczenia obrony teleinformatycznej na świecie. Są organizowane od 2010 roku przez Sojusznicze Centrum Doskonalenia Obrony Cybernetycznej w Estonii (NATO Cooperative Cyber Defence Centre of Excellence).

110 Jest on wykorzystywany do wymiany informacji między podmiotami tworzącymi krajowy system cyberbezpieczeństwa.

stanu wojennego oraz przedstawianie właściwym organom propozycji dotyczących działań obronnych;

- koordynację, we współpracy z ministrem właściwym do spraw wewnętrznych i ministrem właściwym do spraw informatyzacji, realizacji zadań organów administracji rządowej i jednostek samorządu terytorialnego w czasie stanu wojennego dotyczących działań obronnych w przypadku zagrożenia cyberbezpieczeństwa.

- Ponadto Minister Obrony Narodowej prowadzi Narodowy Punkt Kontaktowy do współpracy z Organizacją Traktatu Północnoatlantyckiego, do którego zadań należy:

- zapewnienie współpracy w obszarze obrony narodowej z właściwymi organami Organizacji Traktatu Północnoatlantyckiego w zakresie cyberbezpieczeństwa;

- koordynacja działań w zakresie wzmacniania zdolności obronnych w przypadku zagrożenia cyberbezpieczeństwa;

- zapewnienie współpracy między narodowymi i sojuszniczymi siłami zbrojnymi w zakresie zapewnienia cyberbezpieczeństwa;

- rozwijanie systemów wymiany informacji o zagrożeniach cyberbezpieczeństwa w obszarze obrony narodowej;

- udział w realizacji celów Organizacji Traktatu Północnoatlantyckiego w obszarze cyberbezpieczeństwa i kryptologii.

Rozdział XI reguluje kwestie związane z nadzorem i kontrolą usług kluczowych, dostawców usług cyfrowych i podmiotów świadczących usługi w zakresie cyberbezpieczeństwa. Art. od 53 do 59 zawierają informacje o podmiotach sprawujących nadzór i działania podejmowane w ramach nadzoru, kontroli i stosowanych przepisów innych ustaw, uprawnieniach osób prowadzących czynności kontrolne wobec przedsiębiorców, obowiązkach kontrolowanych przedsiębiorców, postępowaniu dowodowym w ramach kontroli przedsiębiorców, protokołach kontroli oraz zaleceniach pokontrolnych.

Rozdział XII zawiera informacje nt. realizacji polityki rządu w zakresie zapewnienia cyberbezpieczeństwa przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz ogólny zakres działania Kolegium.[111] Zgodnie z Art. 61 u.k.s.c. Pełnomocnika powołuje i odwołuje Prezes Rady Ministrów. Występuje on w randze ministra, sekretarza stanu albo podsekretarza stanu. Podlega Radzie Ministrów, a obsługę merytoryczną, organizacyjno-prawną, techniczną i kancelaryjno-biurową Pełnomocnika zapewnia ministerstwo albo inny urząd administracji rządowej, w którym go powołano. Do zadań pełnomocnika zgodnie z art. 62 u.k.s.c. w ramach koordynowania działań i realizowania polityki rządu w zakresie zapewnienia cyberbezpieczeństwa należy:

- analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych z udziałem organów administracji publicznej, organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV;

- nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych z udziałem organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV;

- opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;

- upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;

- inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa;

- wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.

111 Organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa.

Do zadań Pełnomocnika wykonywanych w porozumieniu z właściwymi ministrami należy również:

- współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;
- podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa;
- podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu.

Art. 63 u.k.s.c. określa sposób przedstawienia przez Pełnomocnika Rządu ds. Cyberbezpieczeństwa Radzie Ministrów rocznego sprawozdania wraz wnioskami i rekomendacjami, a także wszelkich analiz, ocen i wniosków związanych z zakresem jego działania oraz wszelkich zagrożeń w realizacji powierzonych mu zadań jeśli takowe występują. Natomiast art. 64 i 65 u.k.s.c. zawierają informacje nt. działania Kolegium, a także powierzonych mu zadań. Art. 66 u.k.s.c. określa skład Kolegium, Role Przewodniczącego i Sekretarza Kolegium, a także szczegółowy zakres działania i tryb pracy Kolegium.



W skład Kolegium wchodzą:

- przewodniczący Kolegium – Prezes Rady Ministrów;[112]
- Pełnomocnik;
- sekretarz Kolegium;[113]
- członkowie Kolegium:
  - minister właściwy do spraw wewnętrznych,
  - minister właściwy do spraw informatyzacji,
  - Minister Obrony Narodowej,
  - minister właściwy do spraw zagranicznych,
  - Szef Kancelarii Prezesa Rady Ministrów,
  - Szef Biura Bezpieczeństwa Narodowego, jeżeli został wyznaczony przez Prezydenta Rzeczypospolitej Polskiej,
- minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych lub osoba przez niego upoważniona w randze sekretarza stanu albo podsekretarza stanu, a jeżeli minister – członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych nie został wyznaczony – Szef Agencji Bezpieczeństwa Wewnętrznego.

Ponadto w posiedzeniach Kolegium uczestniczą również:

- Dyrektor Rządowego Centrum Bezpieczeństwa;
- Szef Agencji Bezpieczeństwa Wewnętrznego albo jego zastępca;
- Szef Służby Kontrwywiadu Wojskowego albo jego zastępca;
- Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego.

Zgodnie z Art. 67. u.k.s.c. Prezes Rady Ministrów w celu koordynacji działań administracji rządowej w zakresie cyberbezpieczeństwa może, na podstawie rekomendacji Kolegium, wydawać wiążące wytyczne

112 Do pełnienia funkcji przewodniczącego Kolegium Prezes Rady Ministrów może upoważnić Pełnomocnika. Przewodniczący Kolegium zwołuje posiedzenia Kolegium i może zapraszać do udziału w posiedzeniach: przewodniczących właściwych komisji sejmowych, przedstawicieli organów państwowych, przedstawicieli organów właściwych do spraw cyberbezpieczeństwa oraz inne osoby, których uczestnictwo jest niezbędne ze względu na tematykę obrad.

113 Jest powoływany i odwoływany przez Prezesa Rady Ministrów. Powołana może być wyłącznie osoba spełniająca wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji niejawnych o klauzuli „tajne". Sekretarz Kolegium organizuje pracę Kolegium oraz wykonywanie zadań wynikających z wyrażonych przez Kolegium rekomendacji i opinii oraz decyzji przewodniczącego Kolegium.

dotyczące zapewnienia cyberbezpieczeństwa na poziomie krajowym oraz funkcjonowania krajowego systemu cyberbezpieczeństwa, a także żądać informacji i opinii w tym zakresie od:

- ministra właściwego do spraw wewnętrznych – w odniesieniu do działalności Policji, Straży Granicznej i Służby Ochrony Państwa;
- Ministra Obrony Narodowej – w odniesieniu do działalności CSIRT MON;
- Szefa Agencji Bezpieczeństwa Wewnętrznego – w odniesieniu do działalności CSIRT GOV;
- Dyrektora Rządowego Centrum Bezpieczeństwa – w odniesieniu do zadań realizowanych zgodnie z ustawą;
- Dyrektora Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego – w odniesieniu do działalności CSIRT NASK;
- ministra właściwego do spraw informatyzacji – w odniesieniu do zadań realizowanych zgodnie z ustawą.

Należy dodać, że Prezes Rady Ministrów wydaje wiążące wytyczne dla CSIRT MON, CSIRT GOV i CSIRT NASK w zakresie obsługi incydentów krytycznych, w tym wskazuje CSIRT odpowiedzialny za obsługę incydentu krytycznego.

Rozdział XIII poświęcony jest strategii, celom strategicznym oraz wszelkim innym zagadnieniom z nią związanym. Zgodnie z art. 68 i 69 u.k.s.c. Rada Ministrów przyjmuje Strategię w drodze uchwały. Określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Strategia obejmuje sektory, usługi cyfrowe oraz podmioty publiczne.

Jej cele strategiczne i szczegółowe zostały omówione w podrozdziale 4.8 Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024.

Rozdział XIV określa przepisy o karach pieniężnych, wyjaśnia wszelkie zaniechania podlegające karze pieniężnej oraz jej wysokość. Określa proces nakładania kary pieniężnej oraz wpływów z kar pieniężnych jako dochodu do budżetu państwa. Omawia wymierzenie, niezależnie od kary nałożonej na operatora usługi kluczowej, a także kary pieniężnej kierownikowi operatora usługi kluczowej. Wprowadzone w ustawie sankcje na operatorów usług kluczowych i dostawców usług cyfrowych za nieprzestrzeganie przepisów mogą wynieść od 1000 do 1 000 000 zł. Kary są nakładane w drodze decyzji administracyjnej przez organ właściwy do spraw cyberbezpieczeństwa, a wpływy pochodzące z kar stanowią dochód budżetu państwa.

Zgodnie z art. 74 u.k.s.c. karę pieniężną nakłada w drodze decyzji organ właściwy do spraw cyberbezpieczeństwa. Wpływy z tytułu kar pieniężnych, o których mowa w art. 73, stanowią przychód Funduszu Cyberbezpieczeństwa, o którym mowa w art. 2 ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, w zakresie maksymalnej kwoty prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego, o którym mowa w art. 5 omawianej ustawy. W art. 75 u.k.s.c. organ właściwy do spraw cyberbezpieczeństwa może nałożyć karę pieniężną na kierownika operatora usługi kluczowej w przypadku, gdy nie dochował należytej staranności celem spełnienia obowiązków, o których mowa w art. 8 pkt 1, art. 9 ust. 1 pkt 1 oraz art. 15 ust. 1, z tym że kara ta może być wymierzona w kwocie nie większej niż 200% jego miesięcznego wynagrodzenia. Natomiast art. 76 u.k.s.c. mówi, że kara, o której mowa w art. 73, może zostać nałożona również w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli organ właściwy do spraw cyberbezpieczeństwa uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia.

„Przewidziane w ustawie kary oprócz funkcji represyjnej – egzekwowanie obowiązków w sytuacji gdy nie zostały one dobrowolnie zrealizowanie – mają przede wszystkim charakter prewencyjny i dyscyplinujący, tak aby skutecznie przeciwdziałać zaniedbywaniu realizacji przez operatorów usług kluczowych i dostawców usług cyfrowych obowiązków określonych w ustawie o KSC."[114]

114 K. Prusak-Górniak, *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, K. Czaplicki, A. Gryszczyńska, G. Szpor (red.), Warszawa 2019, Rozdział 14.

Rozdział XV nazwany przez ustawodawcę „zmiany w przepisach, przepisy przejściowe, dostosowujące i końcowe" możemy podzielić na trzy części. W pierwszej obejmującej art. 77-82 u.k.s.c. zostały ujęte regulacje modyfikujące poszczególne unormowania wcześniejszych aktów prawnych, w części drugiej obejmującej art. 83-92 u.k.s.c. zawarto regulacje przejściowe związane z wdrożeniem u.k.s.c i dostosowaniem jej do dyrektywy NIS (głównie w zakresie harmonogramu implementacji jej postanowień do prawa krajowego), a w części trzeciej znalazły się przepisy dotyczące maksymalnego limitu wydatków z budżetu państwa (art. 93 u.k.s.c.), a także o wejściu w życie ustawy w terminie 14 dni od jej ogłoszenia przypadającym na dzień 28.08.2018 r. (94 u.k.s.c.).

Wprowadzenie ustawy o krajowym systemie cyberbezpieczeństwa było nie tylko wyzwaniem dla administracji ale również dla sektora prywatnego. Organizacja poszczególnych sektorów związana ze zmianami w prawie sektorowym czy też ustanowieniem sektorowych zespołów cyberbezpieczeństwa angażowała sporo czasu i wysiłku. Sam obowiązek raportowania incydentów stanowi znaczącą zmianę dla sektora prywatnego, a opracowanie konkretnych narzędzi – systemu teleinformatycznego, którego zadaniem jest wspierać krajowy system cyberbezpieczeństwa wymagało wiele pracy.



WOJSKA OBRONY CYBERPRZESTRZENI



Materializacja aktualnych strategii *Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020* oraz *Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* przyjmuje obecnie bardzo konkretne kształty – które uzupełniają, a zarazem zabezpieczają funkcjonowanie Krajowego Systemu Cyberberbezpieczeństwa.

Najistotniejszym aktualnie aktem prawa w sferze cybermilitarnej - będącym swoistą „konstytucją bezpieczeństwa dla RP" jest przyjęta w marcu 2022 r. ustawa z dnia 11 marca 2022 r. - *o obronie Ojczyzny*[115] (dalej: ustawa o obronie Ojczyzny.), przygotowana pod auspicjami Wiceprezesa Rady Ministrów Jarosława Kaczyńskiego. Jej art. 15 ust. 4 pkt 2 wyodrębnia w ramach Sił Zbrojnych RP **Wojska Obrony Cyberprzestrzeni** jako specjalistyczny komponent Sił Zbrojnych, właściwy do realizacji pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych.[116]

Ustawa ta, określając „cyberprzestrzeń" odsyła do definicji, o której mowa w art. 2 ust. 1b ustawy z dnia 29 sierpnia 2002 r. - *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej* (Dz. U. z 2017 r. poz. 1932).

Nowo ukonstytuowany **Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni**, zgodnie z art. 23 ustawy o obronie Ojczyzny jest właściwy w zakresie dowodzenia jednostkami wojskowymi i związkami organizacyjnymi Wojsk Obrony Cyberprzestrzeni i podlega:

1. Ministrowi Obrony Narodowej do czasu mianowania Naczelnego Dowódcy Sił Zbrojnych;
2. Naczelnemu Dowódcy Sił Zbrojnych z chwilą jego mianowania i przejęcia przez niego dowodzenia Siłami Zbrojnymi.

Do zakresu działania Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni (art. 23 ust. 2. ustawy o obronie Ojczyzny) należy w szczególności:

1. realizacja programu rozwoju Sił Zbrojnych;
2. programowanie, planowanie, organizowanie, prowadzenie oraz nadzorowanie prowadzenia szkoleń będących we właściwości Dowódcy Komponentu Wojsk Obrony Cyberprzestrzeni na rzecz podległych jednostek wojskowych i związków organizacyjnych, komórek organizacyjnych i jednostek organizacyjnych, a także instytucji, organów i podmiotów, na podstawie zawartych porozumień;
3. planowanie oraz organizowanie mobilizacyjnego i operacyjnego rozwinięcia oraz użycia Wojsk Obrony Cyberprzestrzeni;
4. budowa, utrzymanie oraz ochrona infrastruktury, a także ochrona informacji w cyberprzestrzeni;
5. prowadzenie działań i operacji w cyberprzestrzeni;
6. zapewnienie wsparcia operacji militarnych prowadzonych przez Siły Zbrojne oraz operacji w układzie sojuszniczym i koalicyjnym;
7. współpraca z innymi organami i podmiotami w sprawach związanych z obronnością państwa;
8. zarządzanie i przeprowadzanie kontroli

115 *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny*, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000655, dostęp: 4.09.2022. .

116 O operacyjnych działaniach cyberobronnych w strukturach Obrony Terytorialnej pisze m.in.: R. Jakubczyk, *Powszechna Obrona Terytorialna w bezpieczeństwie narodowym RP*, Warszawa 2020, s. 188 – 191.

podległych jednostek wojskowych i związków organizacyjnych na zasadach i w trybie określonych w ustawie z dnia 15 lipca 2011 r. o kontroli w administracji rządowej.”.[117]

Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni wykonuje swoje zadania przy pomocy Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni. Co istotne, Minister Obrony Narodowej określa w drodze **zarządzenia niepodlegającego ogłoszeniu,** szczegółowy zakres działania, siedzibę i strukturę organizacyjną Dowództwa Komponentu Wojsk Obrony Cyberprzestrzeni oraz jednostek bezpośrednio podporządkowanych. Dowództwo jest ściśle zintegrowane z utworzonym w 2019 r. Narodowym Centrum Bezpieczeństwa Cyberprzestrzeni, które stanowi zaplecze naukowe i w istotny sposób wpływa na odporność Wojska Polskiego przed zagrożeniami z cyberprzestrzeni.[118]

Nadto, zgodnie z art. 448 ust. 1 ustawy o obronie Ojczyzny żołnierzowi zawodowemu realizującemu zadania, o których mowa w art. 5 ustawy z dnia 2 grudnia 2021 r. - *o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa*[119], przysługuje świadczenie teleinformatyczne, o którym mowa w art. 5 tej ustawy, na czas wykonywania tych zadań w wysokości ustalonej zgodnie z przepisami wydanymi na podstawie art. 8 ust. 1 tej ustawy. Szczegóły dot. realizacji świadczenia określa sama ustawa o obronie Ojczyzny, ustawa z dnia 2 grudnia 2021 r. - *o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa* oraz rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. – *w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa.*[120]

Wojska Obrony Cyberprzestrzeni – jako specjalistyczny komponent polskich Sił Zbrojnych utworzony został 8 lutego 2022 r. (de facto, 23 kwietnia 2022 de iure) przez Ministra Obrony Narodowej Mariusza Błaszczaka, a na ich czele stanął gen. bryg. Karol Molenda,[121] który już od lutego 2019 r. pełnił też funkcję Pełnomocnika Ministra Obrony Narodowej ds. utworzenia Wojsk Obrony Cyberprzestrzeni, które pełną zdolność bojową mają osiągnąć do końca 2024 roku.[122] Dowództwu Komponentu Wojsk Obrony Cyberprzestrzeni (DKWOC) podporządkowane są jednostki poziomu taktycznego, których prawidłowe funkcjonowanie zapewnia Jednostka Wsparcia Działań.[123] DKWOC odpowiada również w resorcie obrony narodowej za kluczowe obszary związane z kryptologią, cyberbezpieczeństwem oraz budową i eksploatacją systemów IT.[124] W praktyce, kluczowymi zadaniami tej jednostki jest:[125]

- zapewnianie bezpieczeństwa teleinformatycznego całego resortu,
- budowa, wdrażanie, użytkowanie oraz ochrona narodowych technologii kryptologicznych;
- wytwarzanie nowych produktów dla państwa przez zespolenie potencjału naukowego i przemysłowego w obszarze zaawansowanych technologii informatycznych i kryptograficznych;
- działalność naukowo-edukacyjna, wdrożeniowa, badawczo-rozwojowa i opiniodawcza;
- zapewnianie prawidłowego funkcjonowania zespołu CSIRT MON (Zespołu Reagowania na

117 *Ustawa z dnia 11 marca 2022 r. o obronie Ojczyzny*, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000655, dostęp: 4.09.2022. .

118 Wojska Obrony cyberprzestrzeni rozpoczęły działalność, [na:] https://www.wojsko-polskie.pl/wat/articles/aktualnosci-w/wojska-obrony-cyberprzestrzeni-rozpoczely-dzialalnosc/, dostęp: 4.09.2022.

119 Ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wyngradzania osób realizujących zadania z zakresu cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210002333, dostęp: 4.09.2022.

120 Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20220000131, dostęp: 4.09.2022.

121 *Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni*, [na:] https://www.wojsko-polskie.pl/woc/dyrektor-dowodca/, dostęp: 4.09.2022.

122 *Ibidem.*

123 *Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni*, [na:] https://www.cyber.mil.pl/articles/o-nas-f/2018-10-268-dowodztwo-komponentu-wojsk-obrony-cyberprzestrzeni/, dostęp: 4.09.2022.

124 *Dowództwo Komponentu Wojsk Obrony Cyberprzestrzeni*, [na:] https://www.cyber.mil.pl/articles/o-nas-f/2018-10-268-dowodztwo-komponentu-wojsk-obrony-cyberprzestrzeni/, dostęp: 4.09.2022.

125 *Ibidem.*

Incydenty Bezpieczeństwa Komputerowego). CSIRT MON monitorując sieci resortu obrony narodowej w trybie 24/7 realizuje obronę pasywną polskiej cyberprzestrzeni;

Eksperci DKWOC opracowują nowoczesne metody wykrywania incydentów w cyberprzestrzeni, projektują rozwiązania do ochrony i zabezpieczenia informacji, rozwijają też własne metody i urządzenia kryptograficzne.[126]

Należy też wspomnieć, że Ministerstwo Obrony Narodowej długofalowo realizuje Program CYBER.MIL. PL którego celem jest zwiększenie bezpieczeństwa państwa i obywateli w cyberprzestrzeni,[127] współtworzony także przez DKWOC.

126 *Ibidem.*

127 https://www.cyber.mil.pl/o-nas/, dostęp: 4.09.2022.



CENTRALNE BIURO ZWALCZANIA CYBERPRZESTĘPCZOŚCI

W sferze pozamilitarnej, realizacją aktualnych strategii *Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020* oraz *Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024* jest m.in. ustawa z dnia 17 grudnia 2021 r. - *o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości* (dalej: ustawa o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości).[128]

Rdzeniem tej ustawy jest powołanie Centralnego Biura Zwalczania Cyberprzestępczości - CBZC (art. 5d ustawy z dnia 6 kwietnia 1990 r. - *o Policji*[129]) nowej specjalistycznej jednostki organizacyjnej Policji - służby zwalczania cyberprzestępczości, będącej odpowiedzialną za realizację na obszarze całego kraju zadań w zakresie:

- rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw;

- wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw, o których mowa wyżej, a także wykrywaniu i ściganiu sprawców tych przestępstw.

Na czele CBZC stoi Komendant, który jest organem Policji podległym Komendantowi Głównemu Policji, a jego głównymi obowiązkami jest kierowanie CBZC oraz bycie przełożonym policjantów CBZC. Komendanta CBZC powołuje, spośród oficerów Policji, i odwołuje minister właściwy do spraw wewnętrznych na wniosek Komendanta Głównego Policji, z kolei Zastępców Komendanta CBZC powołuje, spośród oficerów Policji, i odwołuje Komendant Główny Policji na wniosek Komendanta CBZC. Siedzibą Komendanta CBZC jest miasto stołeczne Warszawa.

Oficjalnie CBZC ruszyło 12 stycznia 2022 r. a Komendantem Centralnego Biura Zwalczania Cyberprzestępczości został nadinspektorAdam Cieślak. Docelowo jednostka ma liczyć 1800 funkcjonariuszy. W pierwszej turze rekrutowano policjantów. „Dokumenty złożyło prawie 900 osób. Po ich analizie do rozmów przystąpiło prawie 650 osób, z czego z obecnego pionu cyber – z wydziałów Komend Wojewódzkich, Komendy Stołecznej i biura cyber Komendy Głównej Policji – ponad 320, które przystąpiły do postępowania kwalifikacyjnego. Z tego zakwalifikowało się blisko 70 proc. policjantów."[130]

128 *Ustawa z dnia 17 grudnia 2021 o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości*, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210002447, dostęp: 4.09.2022.

129 Ustawa z dnia 6 kwietnia 1990 o Policji, [na:] https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20210001882, dostęp: 4.09.2022.

130 N. Bochyńska, *Komendant Centralnego Biura Zwalczania Cyberprzestępczości, insp. Adam Cieślak: „Szukamy ludzi, którzy mają poczucie misji", [na:]* https://cyberdefence24.pl/polityka-i-prawo/komendant-centralnego-biura-zwalczania-cyberprzestepczosci-insp-adam-cieslak-szukamy-ludzi-ktorzy-maja-poczucie-misji, dostęp: 4.09.2022.

PODSUMOWANIE

Bez wątpliwości należy uznać, że jesteśmy świadkami rewolucji w sferze cyberbezpieczeństwa w Polsce. Zarówno determinowany przez czynniki unijne Krajowy System Cyberbezpieczeństwa jak i poszczególne działania krajowe – składają się na olbrzymi proces transformacji, która zapewnić ma nam realne bezpieczeństwo w cyberprzestrzeni – zarówno w kontekście militarnym jak i pozamilitarnym.

Doświadczenia postpandemicze oraz trwający obecnie wielowymiarowy konflikt rosyjsko-ukraiński, dodatkowo wpływają z jednej strony na zwiększenie aktywności cyberprzestępców - z drugiej zaś – wymuszają proaktywną postawę organów państwa.

Należy przewidywać, że sektor cyberbezpieczeństwa w perspektywie przynajmniej do 2030 roku będzie aktywnie się rozwijać,[131] co z jednej strony wymagać będzie jeszcze większych nakładów finansowych, z drugiej zaś wymuszać będzie dostosowanie się społeczeństwa do nowych standardów cyberbezpieczeństwa. Ten drugi element wymagać będzie redefiniowania i dostosowania m.in. wielu programów nauczania, edukacji w szkołach podstawowych i ponadpodstawowych czy kształcenia na studiach wyższych – co ważne – zarówno technicznych jak i społeczno-humanistycznych.

Zauważyć trzeba, że teoretyczne wyznaczanie ambitnych celów we wcześniej prezentowanych dokumentach strategicznych nie zawsze wiązało się i ich realną implementacją. Począwszy jednak od 2016[132] roku zauważyć możemy bardzo poważną intensyfikację w obszarze legislacji jak i działań organizacyjnych, która w sposób namacalny pokazuje nam konkretne rezultaty przeprowadzonych reform – jak cały Krajowy System Cyberbezpieczeństwa, Wojska Obrony Cyberprzestrzeni czy Centralne Biuro Zwalczania Cyberprzestępczości.

Skokowa profesjonalizacja służb mundurowych niewątpliwe przyniesie już niebawem pożądane rezultaty, o ile kierunek reform będzie w dalszej mierze konsekwentnie realizowany, przy wykorzystaniu zwiększonych zasobów finansowych. Trzeba rzetelnie zwrócić uwagę na ten element – cyberprzestępstwa i ciemna strona internetu uszczuplają dochody Skarbu Państwa. Właściwa alokacja środków na cele cyberobrony i przeciwdziałania cyberprzestępczości, jest więc w rezultacie dalekowzroczną działalnością inwestycyjną. Inwestycją w bezpieczeństwo Polski i Polaków – nie tylko w wymiarze stricte militarnym – ale co istotniejsze obecnie – także ekonomicznym,[133] szacuje się bowiem że roczny globalny koszt cyberprzestępczości wyniesie 10.5 biliona dolarów do 2025 r.[134]

131 „Warto przytoczyć konkretne liczby. Dokładnie 23 309 przypadków faktycznego naruszenia bezpieczeństwa teleinformatycznego w instytucjach państwowych odnotował w 2020 r. CSIRT GOV,(...). Zgłoszeń o potencjalnym wystąpieniu incydentów komputerowych odnotowano 246 107, podczas gdy rok wcześniej było ich 226 914, a w 2018 r. „zaledwie" 31 865. Zaznaczmy, że ten skokowy wzrost liczby zgłoszeń w ciągu dwóch ostatnich lat wynika przede wszystkim z wejścia w życie u.k.s.c., a konkretnie obowiązku zgłaszania incydentów na gruncie tej ustawy. Tym samym w latach 2019–2020 nastąpił zauważalny wzrost zgłoszeń przesyłanych do CSIRT GOV w porównaniu z wcześniejszymi okresami sprawozdawczymi. W swoim raporcie ABW ostrzega przed rosnącą liczbą incydentów wykrywanych w ramach infrastruktury państwowej oraz infrastruktury krytycznej znajdującej się w kompetencji zespołu CSIRT GOV(...) za: *E. Chilmon, Stan bezpieczeństwa cyberprzestrzeni RP, [na:]* https://itwadministracji.pl/2021/10/07/stan-bezpieczenstwa-cyberprzestrzeni-rp/, dostęp: 10.09.2022). Por. https://www.gov.pl/web/sluzby-specjalne/bezpieczenstwo-rp-w-sieci, dostęp: 10.09.2022). W 2021 CERT Polska odnotował wzrost obsłużonych incydentów na poziomie 182 proc. w porównaniu do roku ubiegłego. Przypomnijmy, że w 2020 r. CERT Polska obsłużył 10 420 unikalnych incydentów cyberbezpieczeństwa. Za: https://cert.pl/posts/2022/04/statystyki-obslugi-incydentow-2021/, dostęp: 10.09.2022.

132 Warto zauważyć, że Najwyższa Izba Kontroli jeszcze w 2015 roku wyraźnie zwracała uwagę na tą kwestię. Wskazując, że „Bezpieczeństwo w cyberprzestrzeni nie jest w Polsce właściwie chronione. Nie podjęto dotąd spójnych i systemowych działań w zakresie monitorowania i przeciwdziałania zagrożeniom występującym w cyberprzestrzeni. Aktywność państwa paraliżował przede wszystkim brak jednego ośrodka decyzyjnego, koordynującego działania innych instytucji publicznych oraz bierne oczekiwanie na rozwiązania, które w tym obszarze ma zaproponować Unia Europejska. NIK stwierdziła, że działania podmiotów państwowych związane z ochroną cyberprzestrzeni były prowadzone w sposób rozproszony i bez spójnej wizji systemowej. Sprowadzały się one do doraźnego, ograniczonego reagowania na bieżące wydarzeni a oraz biernego oczekiwania na regulacje unijne" Za: https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html, dostęp: 10.09.2022.

133 *Coraz więcej problemów z nieautoryzowanymi transakcjami*, [na:] https://rf.gov.pl/2021/03/01/coraz-wiecej-problemow-z-nieautoryzowanym-transakcjami/, dostęp: 10.09.2022) oraz *Nieautoryzowane transakcje płatnicze – analiza aktualnej sytuacji rynkowej i główne problemy*, [na:] https://rf.gov.pl/nieautoryzowane-transakcje-platnicze-analiza-2020/, dostęp: 10.09.2022). Por. M. Musiał, *Coraz więcej oszustów. Rośnie problem nieautoryzowanych transakcji bankowych*, [na:] https://forsal.pl/lifestyle/technologie/artykuly/8108361,coraz-wiecej-oszustow-rosnie-problem-nieautoryzowanych-transakcji-bankowych.html, dostęp: 10.09.2022). W/w autor podaje: „2020 r. do Rzecznika Finansowego (RF) trafiło niemal 1200 wniosków o interwencję w sporze ws. nieautoryzowanej transakcji bankowej, skala tego problemu w czasie pandemii dynamicznie rośnie."

134 *Ponad 40 statystyk i faktów dotyczących cyberbezpieczeństwa za 2022 r.*, [na:] https://www.websiterating.com/pl/research/cybersecurity-statistics-facts/#references, dostęp: 10.09.2022).

BIBLIOGRAFIA

Artykuły, rozdziały i pozycje monograficzne:

- Banasiński C. (red.), *Cyberbezpieczeństwo. Zarys wykładu*, Warszawa 2018.
- Chałubińska-Jentkiewicz K.*, Cyberbezpieczeństwo – zagadnienia definicyjne*, „Cybersecurity and Law" 2019, Nr 2(2).
- Chmielewski Z., *Polityka publiczna w zakresie ochrony cyberprzestrzeni w UE i państwach członkowskich*, „Studia z Polityki Publicznej" 2016, nr 2(10).
- Czaplicki K., Gryszczyńska A., Szpor G. (red.*), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, Warszawa 2019.
- Grzelak M., Liedel K.*, Bezpieczeństwo w cyberprzestrzeni. Zagrożenia i wyzwania dla Polski – zarys problemu,* „Bezpieczeństwo Narodowe", II – 2012, nr 22.
- Hydzik W., Cyberbezpieczeństwo i ochrona danych osobowych w świetle regulacji europejskich i krajowych, „PUG" 2019, nr 3, s. 84-87.
- Jakubczyk R., *Powszechna Obrona Terytorialna w bezpieczeństwie narodowym RP*, Warszawa 2020;
- Korzeniowski L. F., *Securitologia. Nauka o bezpieczeństwie człowieka i organizacji społecznych*, Kraków 2008;
- Koziej S., Brzozowski A., *25 lat polskiej strategii bezpieczeństwa, „*BEZPIECZEŃSTWO NARODOWE" II – 2014, nr 30.
- Krawczyk-Jezierska A., Koszty instytucji finansowych w świetle zagrożeń cybernetycznych, „PUG" 2019, nr 8, s. 23-31.
- Krzyżanowski T., Nowa przesłanka wykluczenia z postępowania, „Zam.Pub.Dor." 2020, nr 10, s. 45-50.
- Lisiak-Felicka D., Szmit M., *Cyberbezpieczeństwo administracji publicznej w Polsce. Wybrane zagadnienia*, Kraków 2016.
- Marcinkowski C., *Cyberprzestrzeń a istota wybranych zagrożeń społecznych dla bezpieczeństwa współczesnego człowieka,* w: *Patologie w cyberprzestrzeni: profilaktyka zagrożeń medialnych,* D. Morańska (red.*)* , Dąbrowa Górnicza 2015.
- Piątek S., Obowiązki przedsiębiorców telekomunikacyjnych w zakresie cyberbezpieczeństwa, „IKAR" 2020, nr 2. s. 28-41.
- Proć T., Odpowiedzialność dostawcy usług cyfrowych w Krajowym Systemie Cyberbezpieczeństwa, „IKAR" 2020, nr 2, s. 42-53.
- Siwicki M.*, Kilka uwag na temat ochrony infrastruktury krytycznej w internecie na tle dyrektywy NIS i jej transpozycji do polskiego porządku prawnego*, „EPS" 2019, nr 9, s. 13-20.
- Szkurłat A.*, Kompetencje Prezesa UODO w zakresie cyberbezpieczeństwa w świetle polskich i unijnych regulacji prawnych*, „IKAR" 2020 nr 2, s. 54-60.

- Wajda P., *Cyberbezpieczeństwo - sektorowe aspekty regulacyjne*, „IKAR" 2020, nr 2, s. 9-27.
- Wilbrandt-Gotowicz M., *Perspektywy ochrony interesu publicznego na podstawie regulacji ustawy z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, „Admin." 2018, nr 3, s. 88-102;
- Vishik C., Matsubara M., Plonk A.*, Key Concepts in Cyber Security: Towards a Common Policy and Technology Context for Cyber Security Norms*, w: International Cyber Norms: Legal, Policy & Industry Perspectives, A.-M. Maria Osula, H. Rõigas (Eds.), NATO CCD COE Publications, Tallinn 2016, s. 221-222;

Akty prawne i dokumenty strategiczne, oraz projekty z uzasadnieniami:

- Ustawa z dnia 14 lipca 1983 r. - *o narodowym zasobie archiwalnym i archiwach* (Tekst jedn. Dz.U. z 2020 r. poz. 164).
- Ustawa z dnia 6 kwietnia 1990 r. - *o Policji* (Tekst jedn. Dz.U. z 2021 r. poz. 1882).
- Ustawa z dnia 29 sierpnia 2002 r. - *o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej* Polskiej (Tekst jedn. Dz. U. z 2017 r. poz. 1932);
- Ustawa z dnia 6 grudnia 2006 r. - *o zasadach prowadzenia polityki rozwoju* (Tekst jedn. Dz.U. z 2021 r. poz. 1057).
- Ustawa z dnia 26 kwietnia 2007 r. - *o zarządzaniu kryzysowym* (Tekst jedn. Dz.U. 2022 poz. 261).
- Ustawa z dnia 5 lipca 2018 r. - *o krajowym systemie cyberbezpieczeństwa* (Tekst. Jedn. Dz.U. z 2022 r. poz. 1863).
- Ustawa z dnia 2 grudnia 2021 r. - *o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa* (Dz.U. z 2021 r. poz. 2333).
- Ustawa z dnia 17 grudnia 2021 r. - *o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości* (Dz.U. z 2021 r. poz. 2447).
- Ustawa z dnia 11 marca 2022 r. - *o obronie Ojczyzny* (Dz.U. z 2022 r. poz. 655).
- 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 z 2016 r. L 194/1 z 19.7.2016).
- Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. - w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz.U. z 2022 r. poz. 131).
- Uchwała Rady Ministrów z 9.04.2013 r. przyjmująca „Strategię rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022" (M.P. z 2013 r. poz. 377).
- Uchwała Nr 8 Rady Ministrów z 14.02.2017 r. w sprawie przyjęcia „Strategii na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)" (M.P. z 2017 r. poz. 260).
- Zarządzenie Nr 63 Prezesa Rady Ministrów z dnia 4 września 2013 r. - *w sprawie Międzyresortowego Zespołu*

do spraw Opracowania Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej (M. P. z 2013 r., poz. 719).

- Decyzja Nr 357/MON Ministra Obrony Narodowej z dnia 29 lipca 2008 r. - *w sprawie organizacji i funkcjonowania systemu reagowania na incydenty komputerowe w resorcie obrony narodowej* (Dz. Urz. MON z 2008 r. nr.16 poz. 205).
- *Strategia bezpieczeństwa cybernetycznego Unii Europejskiej „Otwarta, bezpieczna i chroniona cyberprzestrzeń*, Bruksela 2013.
- *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2007*, Warszawa 2007.
- *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2014*, Warszawa 2014.
- *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2020*, Warszawa 2020.
- *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*, Warszawa 2019.
- *Strategia na rzecz Odpowiedzialnego Rozwoju do roku 2020 (z perspektywą do 2030 r.)*, Warszawa 2017.
- *Strategia rozwoju systemu bezpieczeństwa narodowego Rzeczypospolitej Polskiej 2022*, Warszawa 2013.
- *Strategia Obronności Rzeczypospolitej Polskiej. Strategia sektorowa do Strategii Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2009.
- *Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022*, Warszawa 2017.
- *Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej*, Warszawa 2013, s. 13.
- Projekt ustawy - *o Sieci Łączności Rządowej* – numer z wykazu UD333, który został dotknięty zasadną dyskontynuacji prac parlamentu.
- Uzasadnienie do rządowego projekt ustawy - *o zmianie ustawy o Policji oraz niektórych innych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości*.

NETOGRAFIA:

- *Bezpieczeństwo,* [na:] https://www.prezydent.pl/kancelaria/archiwum/archiwum-lecha-kaczynskiego/cztery-lata-prezydentury/bezpieczenstwo.
- Breczko B., *Wojna Rosja - Ukraina. Gigantyczny wzrost liczby ataków w internecie*, [na:] https://biznes.wprost.pl/technologie/cyberbezpieczenstwo/10640638/wojna-rosja-ukraina-gigantyczny-wzrost-liczby-atakow-w-internecie.html.
- Bochyńska N., *Komendant Centralnego Biura Zwalczania Cyberprzestępczości, insp. Adam Cieślak: „Szukamy ludzi, którzy mają poczucie misji",* [na:] https://cyberdefence24.pl/polityka-i-prawo/komendant-centralnego-biura-zwalczania-cyberprzestepczosci-insp-adam-cieslak-szukamy-ludzi-ktorzy-maja-poczucie-misji.
- *Czym są cyberzagrożenia? Rodzaje, przykłady i cyberataki* z 20 maja 2022 r., [na:] https://businessinsider.com.pl/technologie/nowe-technologie/cyberzagrozenia-rodzaje-przyklady-definicja/8j4wwbz.
- *Chilmon E., Stan bezpieczeństwa cyberprzestrzeni RP,* [na:] https://itwadministracji.pl/2021/10/07/stan-bezpieczenstwa-cyberprzestrzeni-rp/.
- *Coraz więcej problemów z nieautoryzowanymi transakcjami*, [na:] https://rf.gov.pl/2021/03/01/coraz-wiecej-problemow-z-nieautoryzowanym-transakcjami/.
- *Cyberatak na Ukrainę*, [na:] https://mlodytechnik.pl/news/30858-cyberatak-na-ukraine.
- *Cyberbezpieczeństwo*, [na:] https://www.nask.pl/pl/dzialalnosc/cyberbezpieczenstwo/3284,Cyberbezpieczenstwo.html (dostęp: 31.08.2022).
- *Cyberbezpieczeństwo RP: coraz więcej incydentów*, [na:] https://www.gov.pl/web/sluzby-specjalne/bezpieczenstwo-rp-w-sieci.
- Dowódca Komponentu Wojsk Obrony Cyberprzestrzeni, [na:] https://www.wojsko-polskie.pl/woc/dyrektor-dowodca/.
- *Dowództwo Komponentu Wojsk Cyberprzestrzeni*, [na:] https://www.cyber.mil.pl/articles/o-nas-f/2018-10-268-dowodztwo-komponentu-wojsk-obrony-cyberprzestrzeni/.
- Duszczyk M., *Zmasowane cyberataki Rosji, Białorusi i Chin na polską armię*, [na:] https://www.rp.pl/gospodarka/art36801221-zmasowane-cyberataki-rosji-bialorusi-i-chin-na-polska-armie.
- *Krajowe Ramy Polityki Cyberbezpieczeństwa na lata 2017-2022*, [na:] https://www.gov.pl/web/cyfryzacja/krajowe-ramy-polityki-cyberbezpieczenstwa.
- *Masowa Dezinformacja W Mediach Społecznościowych,* [na:] https://kicb.pl/masowa-dezinformacja-w-mediach-spolecznosciowych/.
- Musiał M., *Coraz więcej oszustów. Rośnie problem nieautoryzowanych transakcji bankowych*, [na:] https://forsal.pl/lifestyle/technologie/artykuly/8108361,coraz-wiecej-oszustow-rosnie-problem-nieautoryzowanych-transakcji-bankowych.html.
- *NIK o bezpieczeństwie w cyberprzestrzeni*, [na:] https://www.nik.gov.pl/aktualnosci/nik-o-bezpieczenstwie-w-cyberprzestrzeni.html.

- *Nieautoryzowane transakcje płatnicze – analiza aktualnej sytuacji rynkowej i główne problemy*, https://rf.gov.pl/nieautoryzowane-transakcje-platnicze-analiza-2020/.
- *Polityka ochrony cyberprzestrzeni RP*, [na:] https://cyberpolicy.nask.pl/polityka-ochrony-cyberprzestrzeni-rp/.
- *Ponad 40 statystyk i faktów dotyczących cyberbezpieczeństwa za 2022 r.,* [na:] https://www.websiterating.com/pl/research/cybersecurity-statistics-facts/#references.
- *RCB ostrzega przed fałszywymi narracjami o wojnie w Ukrainie. W sieci masowa dezinformacja, KPRM wydaje alert,* [na:] https://www.wirtualnemedia.pl/artykul/falszywa-narracja-wojna-ukraina-na-co-uwazac-rzadowe-centrum-bezpieczenstwa.
- Sanger D. E.*, Obama Order Sped Up Wave of Cyberattacks Against Iran,* [na:] http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?pagewanted=all.
- *Wojna cybernetyczna – atak na Ukrainę to nie tylko działania militarne*, [na:] https://www.omegasoft.pl/blog/wojna-cybernetyczna-atak-na-ukraine-to-nie-tylko-dzialania-militarne/.
- *Wojska Obrony Cyberprzestrzeni rozpoczęły działalność*, [na:] https://www.wojsko-polskie.pl/wat/articles/aktualnosci-w/wojska-obrony-cyberprzestrzeni-rozpoczely-dzialalnosc/.
- http://www.bbn.gov.pl/pl/bezpieczenstwo-narodowe/minislownik-bbn-propozy/6035,MINISLOWNIK-BBN-Propozycje-nowych-terminow-z-dziedziny-bezpieczenstwa.html.



Instytut im. Kazimierza Promyka
ul. Obozowa 82A/19
01-434 Warszawa
www.instytutpromyka.pl
e-mail: kontakt@instytutpromyka.pl