NCBR
Narodowe Centrum Badań i Rozwoju

Openfield

Opole, 2023

Raport końcowy z ewaluacji on-going programu CyberSecIdent „Cyberbezpieczeństwo i e-Tożsamość”

SPIS TREŚCI

Spis skrótów

Skrót	Wyjaśnienie
AI	ang. Artificial Intelligence, sztuczna inteligencja
B+R	działalność badawczo-rozwojowa
CERT	ang. Computer Emergency Response Team, w niniejszym dokumencie: Zespół CERT Polska w strukturach NASK - PIB
CSI, Program	program CyberSecIdent „Cyberbezpieczeństwo i eTożsamość”
CSIRT	ang. Computer Security Incident Response Team, Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego
DDoS	ang. Distributed Denial of Service, atak rozproszonej odmowy usługi
DOB	Dział Zarządzania Programami i Projektami na rzecz Bezpieczeństwa i Obronności Państwa w NCBR
FENG	program Fundusze Europejskie dla Nowoczesnej Gospodarki 2021-2027
FERC	program Fundusze Europejskie na Rozwój Cyfrowy 2021-2027
ICT	ang. Information and communication technologies, technologie informacyjno-telekomunikacyjne
IDI	ang. Individual in-Depth Interview, indywidualny wywiad pogłębiony
IoT	ang. Internet of Things, Internet Rzeczy
IoV	ang. Internet of Vehicles, Internet Pojazdów
IP	Instytucja Pośrednicząca
KIS	Krajowa Inteligentna Specjalizacja
KS	Komitet Sterujący NCBR
KSC	Krajowy System Cyberbezpieczeństwa
LLM	Ang. Large Language Model, duży język modelowy
NASK	Naukowa i Akademicka Sieć Komputerowa
NCBR	Narodowe Centrum Badań i Rozwoju
OP	Oś Priorytetowa
PIB	Państwowy Instytut Badawczy
POIR	Program Operacyjny Inteligentny Rozwój 2014-2020
POPC	Program Operacyjny Polska Cyfrowa 2014-2020
PWCyber	Program Współpracy w Cyberbezpieczeństwie
RP	Rzeczpospolita Polska
UE	Unia Europejska

Streszczenie wykonawcze

Wstęp

Celem niniejszego badania była ocena przebiegu i dotychczasowych efektów programu krajowego CyberSecIdent pod kątem weryfikacji potrzeby kontynuacji wsparcia. Program wspiera realizację projektów, które wypracowują rozwiązania z zakresu cyberbezpieczeństwa. W związku z tym przeprowadzono analizy dokumentacji dotyczącej Programu oraz innych dostępnych opracowań z zakresu cyberbezpieczeństwa. Zrealizowano też wywiady pogłębione z przedstawicielami różnych grup:

- podmiotów, które skorzystały ze wsparcia Programu i realizowały projekty w jego ramach,
- podmiotów, które starały się o wsparcie Programu, ale go nie otrzymały,
- jednostek organizacyjnych Narodowego Centrum Badań i Rozwoju, które zajmują się Programem.

W ramach badań przeprowadzono również panel ekspercki z udziałem specjalistów z obszaru cyberbezpieczeństwa oraz przeprowadzono studia przypadków, czyli analizy opisujące projekty bardziej szczegółowo pod kątem skuteczności ich realizacji.

Główny wniosek z badania

Należy pozytywnie ocenić przebieg i dotychczasowe efekty Programu CyberSecIdent. Wnioski z badania wskazują, że powinno się kontynuować podobną inicjatywę wspierającą obszar cyberbezpieczeństwa.

Ocena dotychczasowych efektów Programu

CyberSecIdent odpowiada na potrzeby państwa w obszarze cyberbezpieczeństwa.

Przeprowadzone analizy wykazały przede wszystkim, że zakres podejmowanych działań w Programie odpowiada jego celom. Co najważniejsze, pozwala na osiągnięcie celu głównego, jakim jest podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie

dostępności narzędzi sprzętowo-programistycznych, do roku 2023. (rozdział 1.1. Założenia Programu są trafne, Rysunek 1)

Założenia i tematyka Programu są trafne, wynikają z odpowiednio zdiagnozowanych wyzwań. Badanie wykazało, że uwzględniają szeroki zakres projektów, co pozwala na większą swobodę i kreatywność projektodawców. Ułatwia też dostosowanie sposobu realizacji projektów do zmian w obszarze nowych technologii i szczegółowych wyzwań z zakresu cyberbezpieczeństwa. (rozdział 1.1. Założenia Programu są trafne, Schemat 2)

Dotychczas zakończono realizację 8 z 23 projektów. Rezultaty trzech z nich są już wykorzystywane w praktyce. Mimo tego, na podstawie danych na temat realizacji wszystkich projektów, ogółem można wysoko ocenić ich potencjał i możliwości wypracowania rozwiązań zgodnie z założonymi celami. (rozdział 1.2. CyberSecIdent skutecznie wspiera rozwiązania na rzecz cyberbezpieczeństwa).

Badanie potwierdza, że opracowane rozwiązania w ramach projektów wpływają na podniesienie bezpieczeństwa cyberprzestrzeni. Ich rezultaty wspierają wdrażanie nowych regulacji unijnych i krajowych związanych z cyberbezpieczeństwem. (rozdział 1.3.

Realizacja Programu przynosi korzystne efekty w wielu wymiarach).

Należy podkreślić też, że Program daje możliwości tworzenia rodzimych rozwiązań z obszaru cyberbezpieczeństwa, co wpływa na budowanie polskiej niezależności w tym zakresie. Pozytywnym efektem Programu jest też rozwój wiedzy i kompetencji przez jednostki realizujące projekty. (rozdział 1.3.

Realizacja Programu przynosi korzystne efekty w wielu wymiarach).

Skutecznej realizacji projektów sprzyjała współpraca jednostek naukowo-badawczych z podmiotami sektora prywatnego. Jej przebieg oceniany jest pozytywnie – podejmowanie wspólnych działań z zachowaniem dobrej organizacji i podziału zadań wpływa na wysoką efektywność. Dobrymi opiniami cieszy się też prowadzona komunikacja między realizatorami projektów a Narodowym Centrum Badań i Rozwoju. (rozdział 1.5. Współpraca kluczem do sukcesu).

Do barier wpływających na realizację projektów należy zaliczyć przede wszystkim dynamicznie przebiegające zmiany w branży informatycznej. Podkreśla się także negatywny wpływ pandemii COVID-19 oraz trudności w dotarciu do specjalistów z obszaru cyberbezpieczeństwa. Dodatkowo, problemem związanym z realizacją Programu są niejasne zasady dotyczące praw autorskich do wypracowanych rozwiązań i problemy z ich komercjalizacją. (rozdział 1.4.

Największe trudności wynikają z dynamicznych zmian technologicznych).

Ocena komplementarności CyberSecIdent z innymi programami

Poza Programem CyberSecIdent, identyfikuje się inne inicjatywy o zasięgu ogólnopolskim, które w różnym stopniu dotyczą obszaru cyberbezpieczeństwa. Żaden z nich nie ma jednak takiego istotnego statusu, jaki ma CyberSecIdent, w ramach kluczowego dokumentu strategicznego dotyczącego cyberbezpieczeństwa państwa, jakim jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024. (rozdział 2.1. NCBR realizuje inne inicjatywy wspierające obszar cyberbezpieczeństwa).

Badanie wykazało komplementarność Programu względem innych inicjatyw w tym zakresie. Uzupełniają się pod kątem przedmiotu wsparcia i osiągnięcie efektów poszczególnych programów nie jest uzależnione od realizacji pozostałych. (rozdział 2.3. CyberSecIdent uzupełnia się z pozostałymi inicjatywami).

Projekty realizowane dzięki CyberSecIdent w największym stopniu mogłyby być skutecznie realizowane w ramach inicjatywy „Szybka ścieżka – innowacje cyfrowe”. Nie oznacza to, że nie

byłoby to możliwe w ramach innych programów (w szczególności międzynarodowych, w ramach inicjatywy „Eureka"). Wymagałoby to jednak znacznego przemodelowania sposobu realizacji projektu (m.in. w zakresie posiadania zagranicznego partnera) (rozdział 2.3. CyberSecIdent uzupełnia się z pozostałymi inicjatywami).

Rekomendacje zmian założeń podobnego programu w przyszłości

Wnioski z badania wskazują, że zasadna jest kontynuacja wsparcia obszaru cyberbezpieczeństwa w postaci realizacji podobnego programu do CyberSecIdent, z zachowaniem pewnych warunków jego realizacji. W wyniku przeprowadzonego badania zaproponowano rekomendacje dotyczące kształtowania jego założeń (Załącznik nr 2 **Błąd! Nie można odnaleźć źródła odwołania.**).

1) Program powinien być kontynuowany pod warunkiem włączenia w etap definiowana zakresu tematycznego kolejnych konkursów instytucji zaangażowanych we wdrażanie zadań strategii cyberbezpieczeństwa i cyfryzacji Polski – takich jak: Minister ds. cyfryzacji, Minister ds. administracji, Minister ds. spraw wewnętrznych. Zakres programu powinien być definiowany na podstawie rekomendacji wyżej wymienionych instytucji i być spójny z aktualnymi wyzwaniami identyfikowanymi we wskazanych obszarach. Zakres programu powinien być też komplementarny względem wsparcia oferowanego w ramach innych programów publicznych, w tym głównie FERC.
2) W przyszłych zapisach Programu należy uwzględnić wprowadzane zmiany w regulacjach odnoszących się do kształtowania unijnej polityki cyberbezpieczeństwa – w szczególności w zakresie dyrektywy NIS2 (dyrektywa na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa, nakładająca szereg obowiązków na podmioty kluczowe i ważne), Cybersecurity Act (dot. wzmacniania odporności UE i krajów członkowskich na zagrożenia teleinformatyczne poprzez budowę silnego systemu cyberbezpieczeństwa) i Digital Resilience Act (DORA – dot. operacyjnej odporności cyfrowej sektora finansowego). Cele szczegółowe programu o tematyce cyberbezpieczeństwa powinny być formułowane w sposób szeroki, ale jednocześnie wskazujący pożądane kierunki rozwiązań, podyktowane strategicznymi dokumentami kształtującymi politykę europejską i krajową w tym obszarze.

3) W przypadku kontynuacji programu należy wzmocnić działania informacyjne dotyczące możliwości planowania w projekcie mechanizmów aktualizacji jego założeń. Wnioskodawcy na etapie przygotowywania projektów definiują zadania kończące się kamieniami milowymi, na podstawie których podejmowana jest decyzja np. o modyfikacji projektu. W umowie o dofinansowanie określone są warunki dotyczące wprowadzania zmian w projekcie m.in. zmiany terminów realizacji zadań projektowych, przesuwania kosztów i wprowadzania zmian merytorycznych. Należy jednak podkreślić, że wprowadzenie zmian nie może negatywnie wpłynąć na osiągnięcie zamierzonych celów projektu.
4) Dopracowania wymagają zapisy dotyczące zasad przejmowania praw majątkowych przez Ministra Cyfryzacji do rezultatów wypracowanych w projektach.
5) Uwzględnienie wymiaru edukacyjnego w założeniach dostępnego wsparcia powiązanego z obszarem cyberbezpieczeństwa. W przypadku kontynuacji Programu CSI, nie powinien on jednak koncentrować się na wyżej wskazanych kwestiach. Elementy dot. aspektu edukacji, wzmacniania kompetencji i świadomości w zakresie dziedzin powiązanych z cyberbezpieczeństwem powinny być realizowane w ramach innych komplementarnych działań (taka możliwość identyfikowana jest przede wszystkim w ramach FERC; ponadto w ramach FERS zaplanowano działania uświadamiające i popularyzujące skierowane szczególnie do osób zagrożonych wykluczeniem cyfrowym, zakładające upowszechnianie podstawowych informacji z zakresu umiejętności cyfrowych, w tym dotyczących bezpieczeństwa w sieci). W Programie kontynuującym CSI rekomenduje się rozważenie pośrednich działań wspierających rozwój kadry specjalistów, takich jak mechanizmy zwiększające udział młodej kadry w pracach projektowych.
6) W przyszłych działaniach wspierających cyberbezpieczeństwo, należy w większym stopniu adresować cyberzagrożenia dotykające obywateli i przedsiębiorców. Należy wspierać rozwój rozwiązań systemowych lub proceduralnych m.in. w zakresie zgłoszeń przypadków dezinformacji. Wsparcie dla wypracowania takich systemowych rozwiązań powinno się znaleźć w programach komplementarnych względem CSI w obszarze cyberbezpieczeństwa (w szczególności FERC, do rozważenia Infostrateg, w zależności od planowanych założeń kontynuacji tego programu lub w ramach programu Gospostrateg w trybie projektów zamawianych).

Executive summary

Introduction

The purpose of this study was to assess the progress and impact to date of the CyberSecIdent national programme in order to verify the need for continued support. The Programme supports the implementation of projects that develop solutions in the field of cyber security. Accordingly, analyses of the Programme documentation and other available studies in the field of cyber security were carried out. In-depth interviews were also conducted with representatives of various groups:

- organisations that benefited from the support of the Programme and implemented projects under it,
- organisations that applied for support from the Programme, but did not receive it,
- units of the National Centre for Research and Development, which deal with the Programme.

The research also included an expert panel with the participation of specialists in the field of cyber security and case studies, i.e. analyses describing projects in more detail in terms of their effectiveness.

Main conclusion of the study

The process and the results of the CyberSecIdent Programme so far should be evaluated positively. The conclusions of the study indicate that a similar initiative to support the area of cyber security should be continued.

Evaluation of the Programme's impact so far

CyberSecIdent responds to the state's needs in the area of cyber security. The analyses carried out have shown, first of all, that the scope of activities undertaken in the Programme corresponds to its objectives. Most importantly, it allows for the achievement of the main objective, which is to increase the level of security of the Polish cyberspace by increasing the availability of hardware and software tools, by 2023.

The assumptions and themes of the Programme are accurate, stemming from appropriately diagnosed challenges. The study showed that they take into account a wide range of projects, which allows more freedom and creativity for project applicants. It also makes it easier to adapt the way projects are implemented to changes in the area of new technologies and specific cyber security challenges.

Up to now, eight of the 23 projects have been completed. The results of three of them are already being used in practice. Despite this, based on the implementation data of all projects, overall, their potential and ability to develop solutions in line with their objectives can be highly assessed.

The research confirms that the solutions developed in the projects contribute to the improvement of cybersecurity. Their results support the implementation of new EU and national regulations related to cyber security.

It should also be emphasised that the Programme provides opportunities for the development of national solutions in the area of cyber security, which contributes to building Poland's independence in this area. Another positive effect of the Programme is the development of knowledge and competence by the units implementing the projects.

Effective implementation of projects was supported by cooperation of scientific and research units with private sector entities. Such cooperation is assessed positively - taking joint actions while maintaining good organisation and division of tasks results in high effectiveness. Communication between project implementers and the National Centre for Research and Development is also evaluated positively.

Barriers affecting project implementation include, above all, the dynamic changes in the IT industry. The negative impact of the COVID-19 pandemic and the difficulty in reaching cyber security specialists are also highlighted. Additionally, unclear rules regarding copyrights to the developed solutions and problems with their commercialisation are a problem related to the implementation of the Programme.

Assessment of the complementarity of CyberSecIdent with other programmes

In addition to the CyberSecIdent Programme, other nationwide initiatives are identified that address the area of cyber security to varying degrees. None of them, however, have the significant status that CyberSecIdent has, within the key strategic document on the country's cyber security, the Cybersecurity Strategy of the Republic of Poland 2019-2024.

The study showed the Programme's complementarity with other initiatives in this area. They are complementary in terms of the object of support and the achievement of the effects of each programme is not dependent on the implementation of the others.

The projects implemented through CyberSecIdent could be most effectively implemented under the 'Fast Track - Digital Innovation' initiative. This does not mean that it would not be possible under other programmes (in particular international programmes, under the Eureka initiative). However, it would require a significant re-modelling of the way the project is implemented (including having a foreign partner).

Recommendations for future changes to a similar programme

The conclusions of the study indicate that it is reasonable to continue to support the area of cyber security through the implementation of a similar programme to CyberSecIdent, with certain conditions for its implementation. As a result of the study, recommendations for shaping its assumptions were proposed:

1) The programme should be continued on the condition that institutions involved in the implementation of the tasks connected with Poland's cyber security and digitalisation strategy –0 such as minister of digitalisation, minister of administration, minister of internal affairs – are involved in the stage of defining the thematic scope of subsequent competitions. The scope of the programme should be defined on the basis of the recommendations of the above-mentioned institutions and be consistent with the current challenges identified in the indicated areas. The scope of the programme should also be complementary to the support offered under other public programmes, mainly FERC.

2) Future provisions of the Programme should take into account changes in regulations relating to the development of the EU cyber security policy - in particular the NIS2 Directive (a directive for a high common level of cyber security, imposing a number of obligations on key and important entities), the Cybersecurity Act (on strengthening the resilience of the EU and member states to ICT threats by building a strong cyber security system) and the Digital Resilience Act (DORA - on operational digital resilience of the financial sector). The specific objectives of the programme on cyber security should be formulated in a broad manner, but at the same time indicating the desired directions of solutions, dictated by the strategic documents shaping European and national policy in this area.
3) In the case of continuation of the programme, information activities concerning the possibility of planning in the project of mechanisms for updating its assumptions should be strengthened. At the stage of project preparation, the applicants define tasks ending with milestones, on the basis of which a decision is made, e.g. to modify the project. The grant agreement defines the conditions for introducing changes to the project, e.g. changes of deadlines for the implementation of project tasks, moving costs and introducing content-related changes. It should be emphasised, however, that the introduction of changes cannot adversely affect the achievement of the intended objectives of the project.
4) The rules concerning the assumption of property rights by the Minister of Digitalisation to the results developed in the projects need to be refined.
5) Inclusion of an educational dimension in the assumptions of the available support linked to the area of cyber security. If the CSI Programme is continued, however, it should not focus on the above-mentioned issues. Elements concerning the aspect of education, strengthening of competences and awareness in areas related to cyber security should be implemented within the framework of other complementary activities (such a possibility is identified first of all within FERC; moreover, within FERS, awareness-raising and popularisation measures are planned, directed especially to those threatened by digital exclusion, assuming the propagation of basic information on digital skills, including online security). The CSI follow-up programme recommends considering indirect measures to support the development of a workforce of

professionals, such as mechanisms to increase the participation of young staff in project work.

6) In future measures to support cyber security, cyber threats affecting citizens and businesses should be addressed to a greater extent. The development of systems or procedural solutions for, among other things, disinformation reporting should be supported. Support for the development of such systems-based solutions should be found in programmes complementary to the CSI in the area of cyber security (in particular FERC, for consideration Infostrateg, depending on the planned continuation of this programme, or under the Gospostrateg programme in the form of contracted projects).

EWALUACJA ON-GOING PROGRAMU CYBERSECIDENT

GŁÓWNE WNIOSKI

- Pozytywna ocena przebiegu i dotychczasowych efektów Programu.
- Potrzebna kontynuacja podobnej inicjatywy wspierającej obszar cyberbezpieczeństwa.

OCENA DOTYCHCZASOWYCH EFEKTÓW PROGRAMU

Podniesienie bezpieczeństwa cyberprzestrzeni

Wspieranie wdrażania nowych regulacji unijnych i krajowych

Tworzenie rodzimych rozwiązań, a przez to wpływ na wzrost polskiej niezależności w zakresie cyberbezpieczeństwa

Rozwój wiedzy w obszarze cyberbezpieczeństwa

Rozwój współpracy między jednostkami badawczymi i sektorem prywatnym

Opracowanie i wdrażanie sprawdzonych rozwiązań wspierających bezpieczeństwo cyberprzestrzeni

PRZYKŁADOWE REZULTATY NAJBARDZIEJ ZAAWANSOWANYCH PROJEKTÓW

Narodowa Platforma Cyberbezpieczeństwa	**Regionalne Centrum Bezpieczeństwa Cybernetycznego**
System ochrony przed atakami DDoS - TAMA	**Polski schemat oceny i certyfikacji - KSO3C**

KOMPLEMENTARNOŚĆ Z INNYMI PROGRAMAMI

Badanie wykazało, że CyberSecIdent uzupełnia się z innymi inicjatywami wspierającymi działania na rzecz cyberbezpieczeństwa. Żaden inny program nie ma jednak tak istotnego statusu strategicznego w kontekście cyberbezpieczeństwa.

INNE INICJATYWY WSPIERAJĄCE CYBERBEZPIECZEŃSTWO

Infostrateg	Program Polska Cyfrowa 2014-2020
Szafir	Fundusze Europejskie na Rozwój Cyfrowy 2021-2027
Młodzi naukowcy	Program Współpracy w Cyberbezpieczeństwie (PWCyber)
Inicjatywa Eureka (konkursy polsko-tajwańskie oraz konkurs GlobalStars)	Fundusz Cyberbezpieczeństwa

REKOMENDACJE

1. Kontynuowanie Programu w przyszłości, pod warunkiem, że jego planowanie i realizacja będzie przebiegać z zaangażowaniem państwowych instytucji, których działalność wiąże się z obszarem cyberbezpieczeństwa.
2. Uwzględnianie w kolejnym Programie zmian wprowadzanych w regulacjach odnoszących się do kształtowania unijnej polityki cyberbezpieczeństwa. Cele szczegółowe programu powinny szerokie, ale jednocześnie wskazujące pożądane kierunki rozwiązań.
3. Wdrożenie działań komunikacyjnych i edukacyjnych skierowanych do potencjalnych beneficjentów na temat możliwości planowania w projekcie mechanizmów aktualizacji jego założeń – pod warunkiem, że zmiany te nadal będą prowadzić do osiągnięcia zakładanego celu całego przedsięwzięcia.
4. Dopracowanie zapisów dotyczących zasad przejmowania praw majątkowych przez Ministra Cyfryzacji do rezultatów wypracowanych w projektach.
5. Uwzględnienie wymiaru edukacyjnego w założeniach dostępnego wsparcia powiązanego z obszarem cyberbezpieczeństwa. Elementy dot. aspektu edukacji, wzmacniania kompetencji i świadomości w zakresie dziedzin powiązanych z cyberbezpieczeństwem powinny być realizowane w ramach innych komplementarnych działań, a nie w CSI.
6. Zwiększenie stopnia adresowania cyberzagrożeń dotykających obywateli i przedsiębiorców. Wspieranie rozwoju rozwiązań systemowych lub proceduralnych m.in. w zakresie zagłoszeń przypadków dezinformacji. Wsparcie dla tych kwestii powinno się znaleźć poza CSI.

Wstęp

Opis badania

Głównym celem badania była **ocena przebiegu i dotychczasowych efektów programu krajowego CyberSecIdent pod kątem weryfikacji potrzeby kontynuacji wsparcia**. Dodatkowo wyznaczono też trzy cele szczegółowe o następującym brzmieniu:

- ocena dotychczasowych efektów projektów w nawiązaniu do celu głównego Programu jakim jest podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP poprzez zwiększenie dostępności narzędzi sprzętowo programistycznych oraz ich użyteczności dla beneficjentów i potencjalnych użytkowników;
- ocena zakresu programu CyberSecIdent w kontekście komplementarności/nakładania się z innymi programami realizowanymi w NCBR i innymi programami wspierającymi obszar cyfrowego bezpieczeństwa;
- rekomendacje zamian zakresu tematycznego lub sposobu realizacji programu pod kątem zdefiniowanych wyzwań i potrzeb rozwojowych.

Przedmiotem badania była realizacja ewaluacji on going programu CyberSecident "Cyberbezpieczeństwo i eTożsamość". Rezultatem prac badawczych jest ocena dotychczasowych efektów Programu i szans na osiągnięcie zakładanych celów. Wyniki w tym zakresie przedstawia niniejszy raport.

Program CSI koncentruje się na rozwiązaniach technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości. Z Programu wyłączono aspekty prawne i regulacyjne cyberbezpieczeństwa oraz inne pośrednie działania wpływające na bezpieczeństwo, zwłaszcza w postaci podnoszenia świadomości oraz edukacji. W zakresie cyfrowej tożsamości, w Programie założono odniesienie jedynie do niektórych metod i technik

identyfikacji i uwierzytelniania nie obejmując rozwiązań o większym zakresie, takich jak platformy zarządzania cyfrową tożsamością.[1]

Na realizację Programu założono budżet NCBR w wysokości 234 027 000 PLN (zwiększony na wniosek Komitetu Sterującego CSI, za zgodą Dyrektora NCBR, z kwoty 212 000 000 PLN). Wnioskodawcami w Programie mogły być Konsorcja naukowe w rozumieniu Ustawy o zasadach finansowania nauki – grupa jednostek organizacyjnych, w której skład wchodzi co najmniej jedna jednostka naukowa oraz co najmniej jeden przedsiębiorca, albo co najmniej dwie jednostki naukowe.[2]

W ramach Programu podpisano 23 umowy na dofinansowanie realizacji projektów[3], w wyniku rozstrzygnięcia czterech konkursów. Realizacja podjętych projektów przypada na lata 2017-2024. Niniejsze badanie objęło przedstawicieli wszystkich wnioskodawców skutecznych realizujących projekty z obszaru podniesienia bezpieczeństwa cyberprzestrzeni RP oraz przedstawicieli NCBR zaangażowanych we wdrażanie Programu. Ponadto, badania przeprowadzono także wśród wnioskodawców nieskutecznych. Do przeprowadzenia badań z powyższymi grupami badanych wykorzystano technikę jakościowych wywiadów. Dodatkowo, ważną częścią przeprowadzonej ewaluacji były też analizy danych zastanych – dokumentacji projektowych, dokumentów programowych, strategicznych, pozycji z literatury przedmiotu, opracowań, raportów z obszaru cyberbezpieczeństwa. W badanie zaangażowani byli też eksperci zajmujący się przedmiotową tematyką. Proces badawczy przedstawia Schemat 1.

[1] CyberSecIdent „Cyberbezpieczeństwo i eTożsamość" – założenia Programu B+R [aktualizacja nr 3], listopad 2020 r.
[2] Tamże
[3] W przypadku jednej umowy podjęto decyzję o rozwiązaniu umowy o wykonanie i finansowanie projektu wraz z wezwaniem do zwrotu środków z zachowaniem miesięcznego okresu wypowiedzenia. Wykonawca odwołał się od decyzji NCBR w tej sprawie, podważając jego stanowisko. Postępowanie wciąż się toczy.

Schemat 1. Schemat procesu badawczego

Źródło: opracowanie własne.

Cyberbezpieczeństwo jako element polityki państwa

Powszechny dostęp do informacji, a także jego wykorzystywanie w wielu aspektach życia – społecznym, gospodarczym, politycznym – warunkuje dziś szeroko rozumiany rozwój. Dlatego też, ważną rolę odgrywają w dzisiejszej rzeczywistości intensywne prace na rozwojem cyfrowych technologii istotnych dla różnych dziedzin świadczonych usług, np. handlu, usług finansowych, transportu, gałęzi gospodarki związanych z szeroko rozumianą komunikacją. Powstające systemy informatyczne tworzą cyberprzestrzeń, w której tworzą się różnorakie relacje, systemy powiązań, a co za tym idzie – wiążą się z tym coraz to nowe wyzwania w kwestii utrzymania bezpieczeństwa. Bezpieczeństwo to dotyczy takich zagadnień, jak

bezpieczeństwo obrotu gospodarczego, bezpieczeństwo obywateli, sprawność działania instytucji publicznych, przebieg procesów produkcyjnych i usługowych – wszystko to zaś składa się ogółem na bezpieczeństwo narodowe.[4]

Rozwijające się technologie informacyjne napędzają rozwój światowej gospodarki, ale jednocześnie pociągają za sobą coraz większe problemy z cyberbezpieczeństwem, ponieważ powstają nowe usługi, nowe środki komunikacji, nowe sposoby realizacji procesów biznesowych oraz społecznych. W związku z powyższym, wyzwaniem dla państwa staje się kwestia ochrony cyberprzestrzeni – systemów informacyjnych i przetwarzanych w nich informacji. Ważna w tym kontekście jest rola całego krajowego systemu cyberbezpieczeństwa, na który składają się podmioty gospodarcze świadczące usługi z wykorzystaniem systemów informacyjnych, organy władzy publicznej i odpowiedzialne za bezpieczeństwo narodowe oraz wyspecjalizowane podmioty zajmujące się cyberbezpieczeństwem w operacyjnym wymiarze. Bezpieczeństwo w tej sferze jest istotnym priorytetem dla Polski również ze względu na liczne powiązania z organizacjami międzynarodowymi, z którymi wchodzi we współpracę na różnych płaszczyznach (UE, NATO, ONZ, OBWE). Wspólne działania w ramach tych organizacji mają duże znaczenie z punktu widzenia zapewnienia odpowiedniego reagowania na naruszenia cyberbezpieczeństwa, których konsekwencje mogą powodować szeroko rozumiane straty.[5]

Przeniesienie dużej części działalności do wirtualnej rzeczywistości - zarówno jeśli chodzi o obywateli, jak i przedsiębiorców oraz inne podmioty uczestniczące w życiu społeczno-gospodarczym, niesie ze sobą nowe rodzaje zagrożeń dla bezpieczeństwa cyberprzestrzeni niż te, które istnieją w tradycyjnych sposobach świadczenia usług i kontaktach społecznych, a także w tradycyjnej terytorialnej organizacji państwa. Potrzebne są odpowiednio wypracowane mechanizmy ochrony tożsamości w cyberprzestrzeni, których rola wiąże się

[4] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024
[5] Tamże

z ochroną prywatności i bezpieczeństwa obywateli oraz bezpieczeństwem obrotu gospodarczego.[6]

Identyfikowane problemy z bezpieczeństwem w cyberprzestrzeni dotyczą zatem kilku sfer i wiążą się z różnymi wyzwaniami. Warto wymienić następujące kwestie:

- W wymiarze ekonomicznym, naruszenia bezpieczeństwa teleinformatycznego przynoszą straty finansowe przedsiębiorcom na coraz większą skalę, co potwierdzają dane dotyczące krajów UE[7], a także dane dotyczące światowej gospodarki[8][9]. Jest to problem obserwowany również w Polsce. Szacuje się, że w 2022 r. 58% polskich przedsiębiorstw odnotowało przynajmniej jeden incydent polegający na naruszeniu bezpieczeństwa[10].
- Zarówno w UE, jak i w Polsce, jedno z największych zagrożeń stanowi oprogramowanie szantażujące – uznaje się, że obecnie najczęstszym początkowym wektorem takich ataków jest phishing[11]. Poważnym zagrożeniem są także rozproszone ataki typu „odmowa usługi" (DDoS, ataki uniemożliwiające użytkownikom sieci lub systemu dostęp do informacji, usług lub innych zasobów).[12][13]
- Konflikt w regionie spowodował uaktywnienie się wielu haktywistów, cyberprzestępców i grup wspieranych przez państwo. Ataki mogą niszczyć infrastrukturę internetową, ale do coraz bardziej powszechnych działań w cyberprzestrzeni zagrażających bezpieczeństwu zaliczyć trzeba też dezinformację,

[6] CyberSecIdent „Cyberbezpieczeństwo i eTożsamość" – założenia Programu B+R [aktualizacja nr 3], listopad 2020 r.
[7] https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1
[8] https://www.consilium.europa.eu/pl/infographics/cyber-threats-eu/
[9] "Cost of a Data Breach Report 2022", IBM Security
[10] Raport „Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu", KPMG, 2023 i Raport „Barometr cyberbezpieczeństwa. Ochrona cyfrowej tożsamości", KPMG, 2022
[11] Wyłudzanie danych uwierzytelniających, czyli kradzież danych poprzez phishing (fałszywe wiadomości, dzięki którym oszuści próbują uzyskać informacje, takie jak nazwa użytkownika i hasło, aby zalogować się do kont użytkownika).
[12] https://www.consilium.europa.eu/pl/infographics/cyber-threats-eu/
[13] Raport „Barometr cyberbezpieczeństwa. Detekcja …", KPMG, 2023

czyli umyślny atak polegający na tworzeniu lub rozpowszechnianiu fałszywych i wprowadzających w błąd informacji w celu manipulowania opinią publiczną. Coraz bardziej groźne i intensywne stają się też ataki na łańcuchy dostaw.[14] Badania pokazują, że w związku z agresją Rosji na Ukrainę odnotowuje się wzrost intensywności cyberataków przeciwko polskim przedsiębiorstwom.[15]

- Problemy, które wiążą się z utrzymaniem cyberbezpieczeństwa, przekładają się na wymierne straty finansowe, w związku z tym mogą one też stanowić czynnik oddziałujący negatywnie na rozwój organizacji działających w różnych sferach, a w konsekwencji ograniczać też rozwój społeczno-gospodarczy w skali całego kraju.
- Bezpieczeństwo cyberprzestrzeni jest też kwestią problemową coraz bardziej zaznaczającą się w kontekście użytkowników cyberprzestrzeni. Według danych dotyczących UE, phishing był najczęściej zgłaszanym incydentem, drugim w kolejności był pharming (przekierowanie na fałszywe strony internetowe proszące o podanie danych osobowych). Polska należy do krajów, w których Eurostat odnotowuje najniższe odsetki w przedmiotowym zakresie.[16] Może to wynikać z niskiego poziomu świadomości i uwrażliwienia polskich użytkowników Internetu na problemy związane z cyberbezpieczeństwem. Mimo tego, również w Polsce obserwuje się wzrost zapotrzebowania zapewnienia ochrony przed niepożądanymi zjawiskami. Potwierdzają to raporty z działalności CERT Polska - zespołu reagowania na incydenty cyberbezpieczeństwa, działającego w strukturach NASK (Państwowego Instytutu Badawczego, prowadzącego działalność naukową, krajowy rejestr domen .pl i dostarczającego zaawansowane usługi teleinformatyczne). W 2021 r. CERT Polska zarejestrował łącznie 29 483 unikalne incydenty cyberbezpieczeństwa i jednocześnie odnotował wzrost obsłużonych incydentów o 182% w porównaniu do roku 2020.[17]

[14] https://www.consilium.europa.eu/pl/infographics/cyber-threats-eu/
[15] Raport „Barometr cyberbezpieczeństwa. Detekcja …", KPMG, 2023
[16] https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20200211-1
[17] „Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu 2021", NASK-PIB/CERT Polska

Podsumowując skrótowo opisane spostrzeżenia, masowe korzystanie z usług w cyberprzestrzeni, rodząc coraz to nowe problemy związane z bezpieczeństwem, przełoży się na coraz to nowe potrzeby w tym zakresie. Co za tym idzie, utrzyma się popyt na rozwiązania w obszarze cyberbezpieczeństwa.

Wciąż istniejące, zmieniające się potrzeby w zakresie tworzenia mechanizmów zapewniających bezpieczeństwo w cyberprzestrzeni, potwierdza także aktualizacja przyjętych kierunków strategicznego działania w tym zakresie. Pierwszym dokumentem w tym zakresie była zatwierdzona w 2013 r. Polityka Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Następnie, w 2017 r. przyjęto Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2020, które zostały zastąpione przez obecnie obowiązujący dokument – Strategię Cyberbezpieczeństwa RP na lata 2019-2024.

Dokument określa cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, które pozwolą osiągnąć cel główny przyjętej strategii – podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji. Będzie to możliwe dzięki założonym celom szczegółowym, jakimi są:[18]

1) rozwój krajowego systemu cyberbezpieczeństwa;
2) podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty;
3) zwiększanie potencjału narodowego w zakresie bezpieczeństwa w cyberprzestrzeni;
4) budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa;
5) zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa.

[18] Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

W ramach powyższych celów, w szczególności trzeciego z nich, wymieniano jako priorytet nastawienie na rozwój współpracy między sektorem publicznym i prywatnym, a przede wszystkim także, stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa - co warto zaznaczyć, wprost wskazuje na potrzebę wdrażania projektów i programów o takim charakterze, jak CSI, będący przedmiotem niniejszej ewaluacji. W zapisach Strategii ustalono, że „zachodzi konieczność intensyfikacji działań badawczych i rozwojowych oraz wytwórczych w zakresie cyberbezpieczeństwa. W tym celu wspólnie z Narodowym Centrum Badań i Rozwoju kontynuowane będą programy badawcze [w przypisie wskazano konkretnie, że kontynuowana będzie współpraca Ministerstwa Cyfryzacji z Narodowym Centrum Badań i Rozwoju m.in. w ramach Programu CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość], mające na celu przygotowanie i wdrożenie nowych metod ochrony przed cyberzagrożeniami”.[19]

Uwarunkowania, identyfikowane na przestrzeni lat potrzeby i wyzwania w obszarze cyberobronności, budzą konieczność wdrażania wsparcia dla inicjatyw na rzecz rozszerzania możliwości rozwoju w obszarze kreowania rozwiązań odpowiadających na problemy bezpieczeństwa cyberprzestrzeni. Dlatego też powstają takie programy, jak CSI, ale obok niego również działania na przykład w ramach Programu INFOSTRATEG, a także planowane do wdrożenia interwencje w ramach nowej perspektywy finansowania UE (takie jak ujęte w Funduszach Europejskich na Rozwój Cyfrowy – FERC).

[19] Tamże

I Opis wyników

1. CyberSecIdent przyczynia się do poprawy cyberbezpieczeństwa kraju

Kluczowe wnioski

- Program odpowiada na potrzeby państwa w obszarze cyberbezpieczeństwa.
- Rezultaty Programu wspierają wdrażanie nowych regulacji unijnych i krajowych związanych z cyberbezpieczeństwem. Co ważne, Program daje też możliwości tworzenia rodzimych rozwiązań z obszaru cyberbezpieczeństwa, co wpływa na budowanie polskiej niezależności w tym zakresie.
- Konstrukcja Programu w zakresie określonych obszarów tematycznych dla realizowanych projektów była trafna, nakreślona z zachowaniem odpowiedniej swobody poruszania się między różnymi zagadnieniami w ramach wskazanych dziedzin. Pozwalała na uwzględnienie szerokiego zakresu projektów, w ramach których pracowano nad różnymi rozwiązaniami branżowymi.
- Mimo tego, że duża część projektów jeszcze się nie zakończyła, można wskazać już pewne kluczowe korzyści, a także projekty/rozwiązania, które odznaczają się wysokim stopniem zaawansowania, poziomem skuteczności i użyteczności. Dotychczas największą skuteczność obserwuje się w I zakresie tematycznym Programu – technologie i rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa.
- Skutecznej realizacji Programu sprzyjają elastyczne założenia dotyczące jego wdrażania, doświadczenie realizatorów projektów, dobra komunikacja między Beneficjentami a NCBR oraz świadomość o istotnej roli Programu w ramach poprawy cyberbezpieczeństwa kraju.
- Do barier należy zaliczyć: dynamicznie przebiegające zmiany w branży informatycznej, negatywny wpływ pandemii COVID-19, trudności w dotarciu do specjalistów z obszaru cyberbezpieczeństwa, niejasne zasady dotyczące praw autorskich do wypracowanych rozwiązań i problemy z ich komercjalizacją.

1.1. Założenia Programu są trafne

W ramach Programu możliwe były do realizacji projekty nawiązujące do określonych tematów badawczych. Przyjęto w tym zakresie trzy obszary:[20]

I. technologie i rozwiązania w zakresie wykrywania, prezentacji oraz ochrony przed zagrożeniami w cyberprzestrzeni i skutkami ich wystąpienia na poziomie państwa;
II. technologie i rozwiązania w zakresie tożsamości cyfrowej, z uwzględnieniem aspektów prywatności;
III. metodyki, techniki i procesy w obszarze analizy cyberbezpieczeństwa i cyfrowej tożsamości oraz ich wdrożenia.

W ramach realizacji projektu, wnioskodawcy mogli prowadzić:[21]

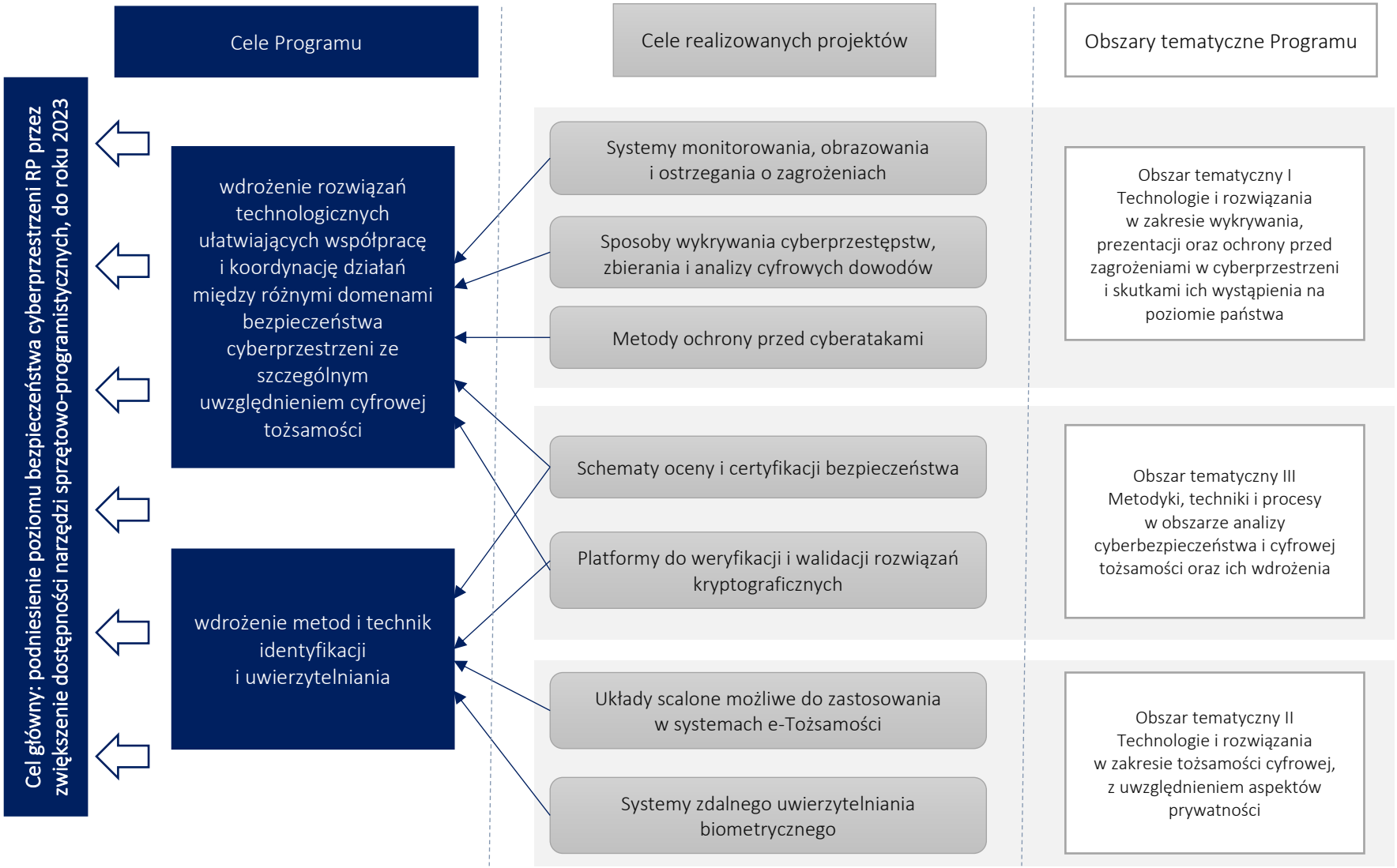
- badania przemysłowe;
- prace rozwojowe;
- przygotowanie wyników badań i prac rozwojowych do zastosowania w praktyce.

Natomiast wytyczne dotyczące podmiotów, które mogły ubiegać się o wsparcie w ramach Programu, wiązały się z następującymi wymogami:

- warunkiem udziału w konkursie konsorcjum naukowego jako Wnioskodawcy było jego formalne istnienie na dzień złożenia wniosku, potwierdzone zawarciem umowy konsorcjum w formie pisemnej już na etapie wnioskowania o dofinansowanie.;
- złożenie umowy konsorcjum w Centrum było warunkiem zawarcia umowy o wykonanie i finansowanie Projektu i było wymagane przed jej podpisaniem (NCBR udostępniało na swojej stronie internetowej niezbędne elementy umowy konsorcjum).

[20] CyberSecIdent „Cyberbezpieczeństwo i eTożsamość" – założenia Programu B+R [aktualizacja nr 3], listopad 2020 r. Pełna charakterystyka Programu została też opisana bardziej szczegółowo w załączniku 6 do niniejszego raportu (Analiza danych zastanych – kontekst badania i przegląd dokumentacji Programu).
[21] Tamże

Przeprowadzone w ramach niniejszego badania analizy wykazały przede wszystkim, że **zakres podejmowanych działań w Programie odpowiada jego celom**. Co najważniejsze **pozwala na osiągnięcie celu głównego, jakim jest podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP** przez zwiększenie dostępności narzędzi sprzętowo-programistycznych, do roku 2023 . Powiązania te przedstawia w syntetyczny sposób Rysunek 1.



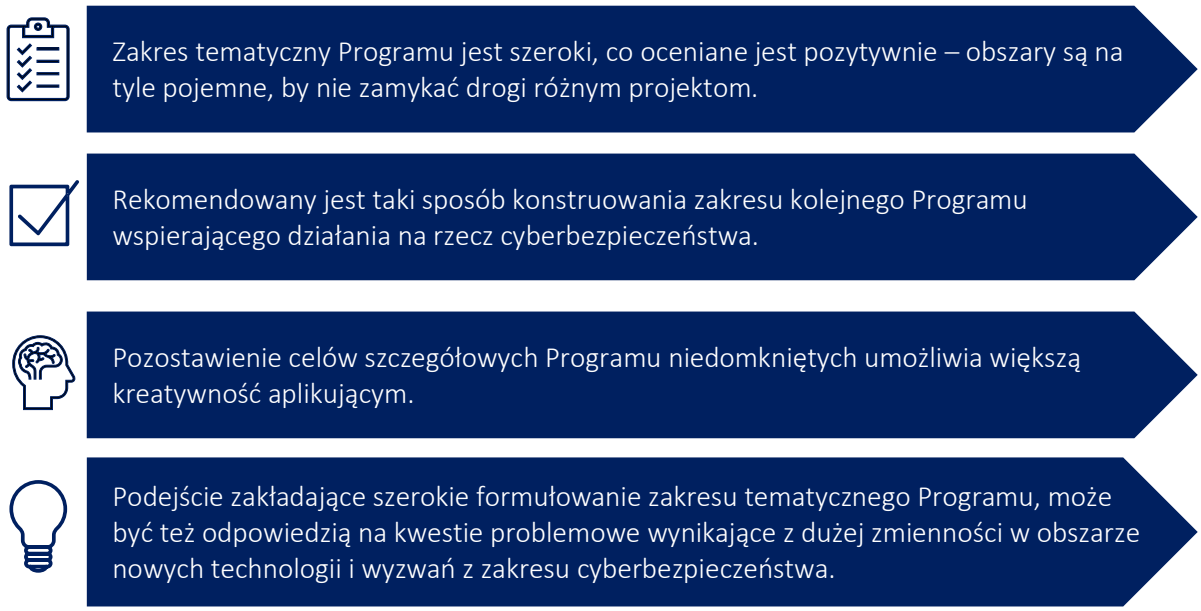
Rysunek 1. Schemat logiczny wiążący cele Programu z efektami projektów

Źródło: opracowanie własne

Należy podkreślić, że **założenia i tematyka Programu wynikają z odpowiednio zdiagnozowanych wyzwań,** co pozwala na opracowanie użytecznych rozwiązań, wpisujących się w zidentyfikowane potrzeby.

Ponadto, w założonych obszarach tematycznych Programu pozostawiono dużą swobodę w obieraniu celów dla projektu. Takie podejście pozwala podmiotom na elastyczne podejście podczas pracy. Taka opinia potwierdzana jest zarówno przez Beneficjentów, ekspertów oraz przedstawicieli NCBR, zaangażowanych w realizację Programu.

Wniosek w powyższym zakresie można podsumować w kilku szczegółowych punktach, które przedstawia **Błąd! Nie można odnaleźć źródła odwołania.**.



Schemat 2. Wnioski dotyczące zakresu Programu

Źródło: opracowanie własne.

Warto przytoczyć opinię eksperta, która ilustruje opisane wyżej spostrzeżenia.

> „Należy wskazywać obszary, wskazywać ramy formalno-prawne, natomiast nie zamykać bardzo szczegółowo, bo wtedy zabijemy kreatywność i będą

pojawiały się projekty, które są odtwórcze, a tego nie chcemy. Chcemy, żeby te projekty były innowacyjne.”

Źródło: panel ekspercki.

1.2. CyberSecIdent skutecznie wspiera rozwiązania na rzecz cyberbezpieczeństwa

W analizach skuteczności działań podejmowanych w ramach Programu należy wziąć pod uwagę to, że **duża część projektów jeszcze się nie zakończyła**, w związku z czym trudno mówić o ich efektach lub skuteczności. To też sprawia, że ogólna ocena poziomu realizacji celów Programu nie jest wysoka. Jednocześnie jednak, analizy dotyczące projektów, które jeszcze się toczą, pozwalają **wysoko oceniać ich potencjał i możliwości wypracowania rozwiązań zgodnie z założonymi celami.**

Dotychczas **8 projektów zostało już zakończonych. Rezultaty trzech z nich są już wykorzystywane w praktyce** i realnie przyczyniają się do budowania systemu cyberbezpieczeństwa.

Schemat 3. Zakończone projekty w ramach CyberSecIdent

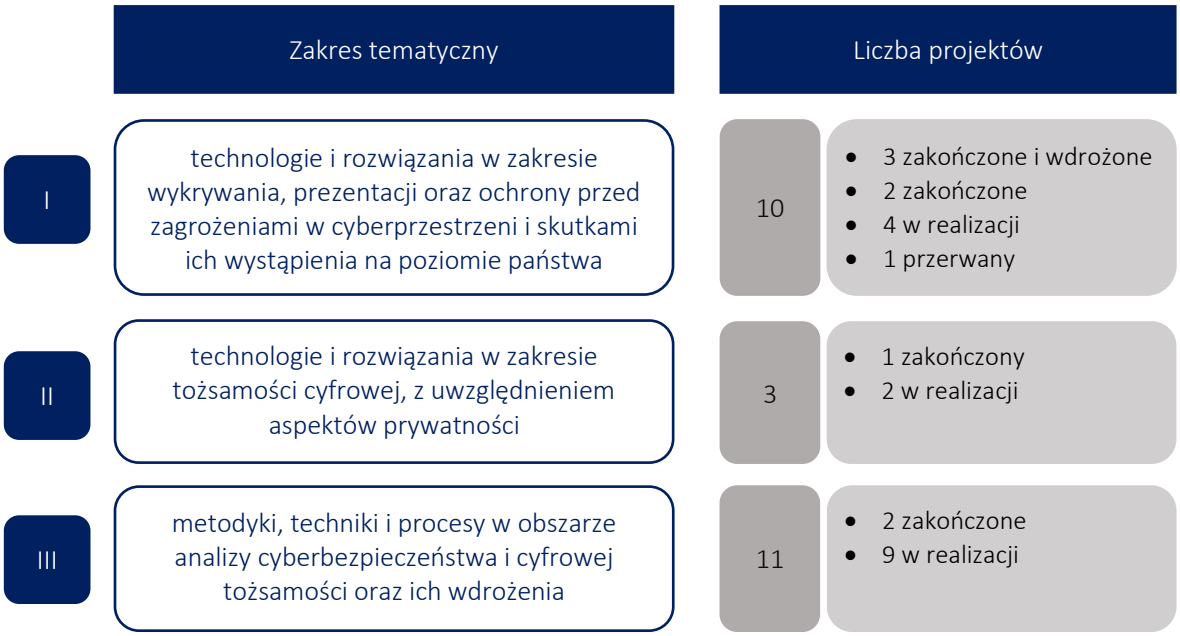
Źródło: opracowanie własne.

W ramach Programu podpisano 23 umowy na dofinansowanie realizacji projektów[22].

Dotyczyły one trzech wyróżnionych w Programie zakresów tematycznych,

[22] W przypadku jednej umowy podjęto decyzję o rozwiązaniu umowy o wykonanie i finansowanie projektu wraz z wezwaniem do zwrotu środków z zachowaniem miesięcznego okresu wypowiedzenia. Wykonawca odwołał się od decyzji NCBR w tej sprawie, podważając jego stanowisko. Postępowanie wciąż się toczy.

scharakteryzowanych na Rysunek 2. Jeden z projektów powiązany były jednocześnie z II oraz III obszarem tematycznym.



Rysunek 2. Tematyka projektów.

Źródło: opracowanie własne.

Na skuteczność Programu częściowo mogą też wskazywać informacje pochodzące z ostatniego sprawozdania z jego realizacji. Czytamy w nim, że zakontraktowane umowy w ramach wszystkich czterech konkursów korzystnie wpłyną na osiągnięcie założonych celów CSI.

Analiza danych sprawozdawczych pozwoliła też zapoznać się szczegółowo z osiągniętymi wartościami wskaźników przypisanych do Programu i poszczególnych typów projektów zakresów tematycznych. W połączeniu z pozostałymi pracami badawczymi, pozwala to na wysunięcie najważniejszych spostrzeżeń i wniosków.

1) Największą skuteczność zaobserwować można w I zakresie tematycznym Programu – prace związane z tym obszarem były też przedmiotem dużej części wszystkich

projektów. Do najważniejszych rezultatów, jakie dotąd osiągnięto, w znacznym stopniu przybliżając Program do realizacji jego celów należy zaliczyć wypracowanie metod skutecznego monitorowania i szybkiej identyfikacji zagrożeń oraz wypracowanie metod i technik wizualizacji zagrożeń w cyberprzestrzeni. Docelowe wartości wskaźników produktu związanych z powyższymi zadaniami zostały już osiągnięte w 100% lub przekroczone. Ponadto, na bardzo wysokim poziomie, bliskim 100% kształtuje się też wskaźnik produktu związany z metodami i technikami dla postępowania po incydencie (osiągnięte 91% wartości docelowej); inne wskaźniki przypisane do I zakresu tematycznego zostały osiągnięte co najmniej na poziomie 60%; w ramach tego zakresu tematycznego warto zwrócić uwagę na przykładowe projekty, w wyniku których:

- powstał system wdrożony przez Ministerstwo Cyfryzacji w KSC (Narodowa Platforma Cyberbezpieczeństwa), służący do monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w cyberprzestrzeni Państwa;
- opracowano rozwiązania komplementarne z powyższym, w postaci modelowego działania Regionalnego Centrum Bezpieczeństwa Cybernetycznego – jako elementy kompleksowego i wielopoziomowego systemu bezpieczeństwa cyberprzestrzeni RP;
- stworzono system ochrony przed atakami DDoS (TAMA).

2) Słabiej w porównaniu z I obszarem tematycznym przedstawiają się dotychczasowe osiągnięcia w ramach II obszaru; tutaj można wymienić, że największą skuteczność obserwuje się w zakresie zabezpieczenia i deidentyfikacji danych – w przypadku związanego z tym wskaźnika produktu osiągnięto już 100% wartości docelowej. Pozostałe kształtują się na poziomie w granicach 25-50%; należy podkreślić, że w zakres tego obszaru tematycznego Programu wpisują się tylko trzy projekty, z których jeden już się zakończył; w jego ramach:

- opracowano system BioMobi, który pozwala na zdalne uwierzytelnianie biometryczne przy wykorzystaniu prostych urządzeń (kamer i mikrofonu)

w urządzeniach mobilnych; system daje możliwość wykorzystania biometrii np. twarzy czy głosu w procesie weryfikacji tożsamości.

3) Biorąc pod uwagę poziom osiągniętych wartości wskaźników produktu, w ramach trzeciego obszaru tematycznego projektów obserwuje się na razie najmniejszą skuteczność; kwestie, które udało się zrealizować w docelowym wymiarze (100% wartości docelowej wskaźnika) dotyczą metod i technik weryfikacji bezpieczeństwa modułów kryptograficznych; wysoki jest też poziom wskaźnika związanego z metodami i technikami weryfikacji bezpieczeństwa dla różnych warstw struktur sprzętowo-programistycznych opartych na międzynarodowych standardach (67%); natomiast jak do tej pory nie udało się w żadnym stopniu zrealizować dwóch pozostałych wskaźników produktu przypisanych do III zakresu tematycznego (metody i wzorce projektowe security oraz privacy desing); efektem realizacji projektów w tym obszarze jest przykładowo:
    - utworzenie polskiego schematu oceny i certyfikacji – uruchomiono nowatorskie Laboratorium Oceny Bezpieczeństwa Produktów Informatycznych zgodne z Common Criteria[23] oraz powstał Ośrodek Standaryzacji i Certyfikacji, który ma pełnić funkcję Jednostki Certyfikującej; warto też dodać, że polski schemat oceny i certyfikacji uzyskał formalny status autoryzowanego uczestnika międzynarodowych porozumień, który wydaje certyfikaty bezpieczeństwa uznawane przez innych uczestników tych porozumień.

[23] Norma pozwalająca w sposób formalny weryfikować bezpieczeństwo systemów teleinformatycznych.

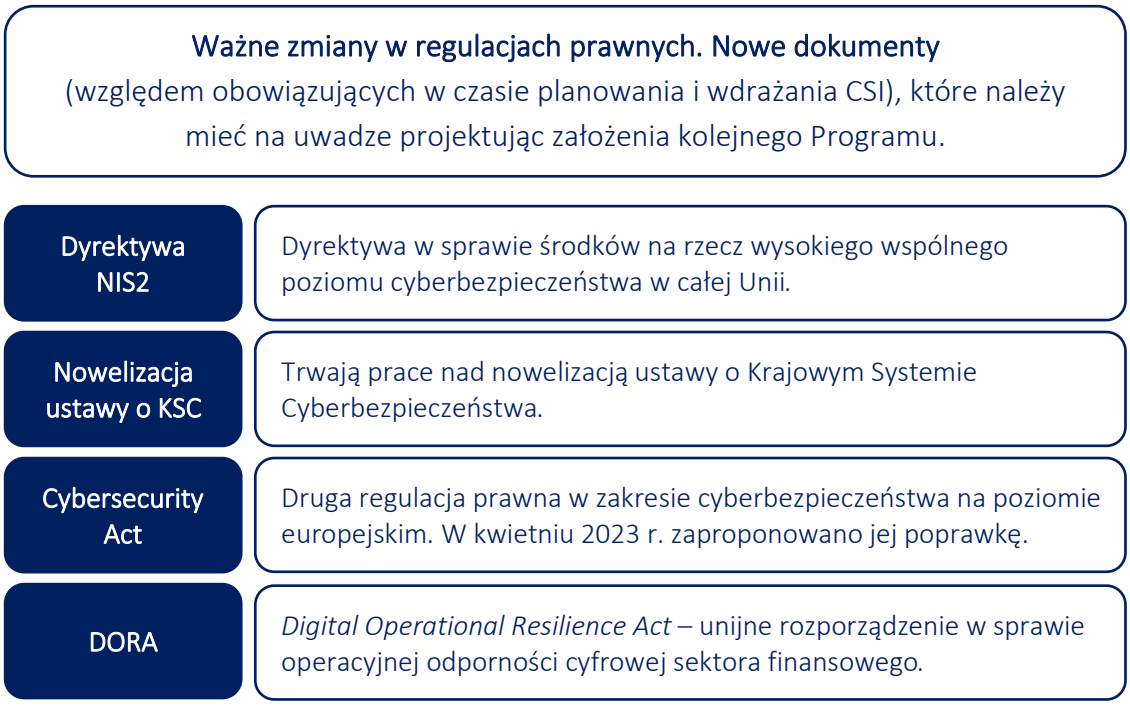
1.3. Realizacja Programu przynosi korzystne efekty w wielu wymiarach

Dokonując syntezy informacji pochodzących z różnych źródeł, można wymienić różne pozytywne rezultaty realizowanych działań w ramach Programu. Prowadzone projekty przyczyniły się do uzyskania efektów wskazanych i opisanych w kolejnych akapitach.

Opracowane rozwiązania w ramach projektów wpływają na podniesienie bezpieczeństwa cyberprzestrzeni. Podjęte działania przyczyniają się przede wszystkim do realizacji potrzeb Ministra Cyfryzacji w zakresie rozwiązań sprzętowo – programowych możliwych do zastosowania w systemach e-Tożsamości. Co ważne, w wyniku Programu opracowywane i wdrażane są bezpieczne produkty lub usługi teleinformatyczne w cyberprzestrzeni.

Rezultaty Programu wspierają wdrażanie nowych regulacji unijnych i krajowych związanych z cyberbezpieczeństwem. Projekty przyczyniają się do zapewnienia adekwatnego do potrzeb i możliwości udziału Polski w działaniach UE na rzecz wspólnych rozwiązań w zakresie cyberbezpieczeństwa. Podkreśla się jednocześnie, by w przyszłych rozwiązaniach uwzględnić wprowadzane zmiany, wymogi dokumentów strategicznych, dyrektyw, wytycznych odnoszących się do kształtowania polityki cyberbezpieczeństwa.

Warto podkreślić przy tym, że rezultaty projektów wspomagają realizację potrzeb polskich przedsiębiorców zaangażowanych w świadczenie tzw. usług kluczowych zgodnie z Dyrektywą NIS oraz użytkujących systemy teleinformatyczne wspierające funkcjonowanie infrastruktury krytycznej.



Schemat 4. Najważniejsze akty prawne w zakresie cyberbezpieczeństwa

Źródło: opracowanie własne.

Program daje możliwość tworzenia rodzimych rozwiązań z obszaru cyberbezpieczeństwa, co wpływa na budowanie polskiej niezależności w tym zakresie. Wątek poruszany przez Beneficjentów, ale również mocno podkreślany przez ekspertów. W opinii badanych, takie wsparcie, jak CyberSecIdent, daje szansę na budowę rozwiązań konkurencyjnych dla dostępnych rozwiązań spoza kraju. Przyczynia się to do tworzenia krajowego systemu cyberbezpieczeństwa, wykorzystującego rozwiązania wysokiej jakości, projektowane przez rodzimych specjalistów. W związku z tym, można też mówić o wpływie rozwiązań opracowanych w ramach projektów na **podniesienie konkurencyjności gospodarki, w obszarach związanych z ICT**. Dzięki realizacji Programu nastąpił zdecydowany wzrost poziomu innowacyjności produktów informatycznych opracowywanych w polskich przedsiębiorstwach i jednostkach naukowo-badawczych, a przez to również wzrost konkurencyjności oferowanych produktów. Ważnym aspektem osiąganych rezultatów Programu jest też pobudzenie aktywności badawczej prywatnego sektora gospodarczego w obszarach związanych z

cyberbezpieczeństwem i **rozwój współpracy między jednostkami badawczymi i podmiotami zewnętrznymi.**

Potwierdzają się też **pozytywne efekty w zakresie rozwoju wiedzy** w obszarach związanych z cyberbezpieczeństwem. Efektem Programu jest uzyskanie nowych kompetencji przez jednostki naukowo-badawcze pozwalające im lepiej funkcjonować na rynku produktów bezpieczeństwa teleinformatycznego.

Rozszerzenie zakresu wiedzy i kompetencji wśród zespołów projektowych, było jednym z najbardziej podkreślanych przez respondentów rezultatów. Wielu badanych wskazywało, że taki rozwój nie byłby możliwy do uzyskania w inny sposób. Dla ilustracji tych spostrzeżeń przytoczono poniższą wypowiedź badanego.

> „Jeśli chodzi o korzyści dla nas jako konsorcjantów, to jest ogromna ilość praktycznej i teoretycznej wiedzy i rozwoju tych ludzi. […] praca od roku do trzech lat w projekcie badawczym z zespołem ekspertów, programistów i ekspertów cyberbezpieczeństwa, pozwala migrować tę wiedzę pomiędzy ludźmi, bo każdy się zajmuje czymś innym. I w efekcie potencjał zespołu badawczego urósł nawet nie wiem ilokrotnie w ciągu tego półtora roku, jak ten projekt funkcjonuje. To jest bez porównania."

Źródło: wywiady jakościowe z realizatorami projektów.

Z wypowiedzi Beneficjentów wynika, że **realizacja podobnych przedsięwzięć byłaby w większości przypadków niemożliwa w takim samym zakresie bez wsparcia Programu.** W głównej mierze chodzi o brak wsparcia finansowego, które jest kluczowe. Realizatorzy projektów szukają tego rodzaju źródeł wsparcia.

W ramach badania prowadzono też rozmowy z wnioskodawcami nieskutecznymi. Na ich podstawie można wskazać, że nie udaje się wykonać projektów w takim samym zakresie, w którym planowali je zrealizować ze wsparciem Programu. Projekty te były duże, ich założenia

zakładały pracę na wielu poziomach, nad różnymi komponentami składającymi się na większe systemy rozwiązań. W związku z tym, realizacja całej wizji wymaga też sporego nakładu finansowego – bez wsparcia Programu realizatorzy mogą pracować nad poszczególnymi elementami osobno, moduł po module, rozdrabniając pracę nad całościowym przedsięwzięciem na kilka mniejszych projektów, rozproszonych w czasie.

Beneficjenci Programu wyrażali liczne pozytywne opinie na temat jego realizacji i deklarowali jednocześnie dalsze duże zainteresowanie podobną inicjatywą w przyszłości.

1.4. Największe trudności wynikają z dynamicznych zmian technologicznych

Przeprowadzone badania wykazały kilka kwestii problemowych, które wpływały na realizację wytyczonych celów zarówno na poziomie założeń dotyczących całego Programu, jak i na poziomie pracy projektowej.

W związku z założeniami wyznaczającymi zasady realizacji Programu, należy zwrócić uwagę na:

- kwestię środków na sfinansowanie podatku VAT – Beneficjenci występowali o dofinansowania na podatek od towarów i usług (VAT) od wysokości przekazanego przez NCBR dofinansowania na realizację poszczególnych projektów; zabezpieczanie środków na sfinansowanie podatku VAT należnego może wpłynąć na obniżenie dostępnych środków finansowych dla bezpośrednich kosztów realizacji projektów;
- kwestię praw autorskich – przeprowadzone badania wskazują na niedoskonałości konstrukcji umów zawieranych z Beneficjentami na dofinansowanie ich projektów, w których niejasno określone zostały zasady przejmowania praw majątkowych przez Ministra Cyfryzacji; rodzi to problemy związane przede wszystkim z komercjalizacją rozwiązań wypracowanych w projektach przez Beneficjentów – w sytuacji, gdy większość praw autorskich do nich posiada Minister.

Ponadto, zidentyfikowano występowanie kilku rodzajów trudności i barier występujących w czasie prac prowadzonych w ramach projektów. Najważniejsze wiążą się z dynamicznymi zmianami w branży informatycznej – badani z różnych grup podkreślali, że rozwiązania aktualne na początku realizacji projektów, szybko stają się przedawnione. Utrudnia to opracowywanie pożądanych, użytecznych rozwiązań i generuje trudności z rozliczeniem wydatków ponoszonych na projekt, ponieważ nie da się przewidzieć, które elementy będą wymagały zmiany za rok lub dwa.

Biorąc pod uwagę wnioski płynące z całego przeprowadzonego badania, należy też wskazać następujące czynniki oddziałujące negatywnie, jak:

- trudności w dotarciu do specjalistów z obszaru cyberbezpieczeństwa (nie są zbyt liczni, co sprawia, że ich zatrudnienie jest bardzo drogie);
- pandemia COVID-19, która powodowała opóźnienia w realizacji projektów;
- ograniczona dostępność wymaganego sprzętu – trudności w pozyskiwaniu potrzebnych komponentów, zaburzone łańcuchy dostaw; było to skutkiem wymienionej wyżej pandemii, ale również konsekwencją sytuacji geopolitycznej;
- choć wskazuje się na wiele korzyści płynących z aktywnej współpracy jednostek ze środowiska naukowo-badawczego z podmiotami prywatnymi, to należy też zwrócić uwagę na różnice w trybie pracy tych dwóch sektorów; mogą one utrudniać odpowiednią synchronizację poszczególnych prac prowadzonych we współpracy.

1.5. Współpraca kluczem do sukcesu

W wyniku badania zidentyfikowano też czynniki, które sprzyjają skutecznej realizacji projektów, niwelując oddziaływanie występujących barier. Przedstawia je Schemat 5.

Schemat 5. Czynniki sprzyjające skutecznej realizacji projektów

Źródło: opracowanie własne.

Warto w tym kontekście zwrócić uwagę na kwestię **współpracy, która stanowi pewnego rodzaju motyw przewodni skutecznych prac nad projektami**. Dotyczy ona kilku poziomów: relacji między Beneficjentami a opiekunami ze strony NCBR, relacji między konsorcjantami, ale także w niektórych przypadkach włączania w prace nad kreowanymi rozwiązaniami przedstawicieli instytucji rządowych. W przypadku komunikacji na linii Beneficjent – NCBR warto podkreślić, że doceniane było wsparcie Centrum, czego wyrazem jest przykładowy cytat:

„Mi bardzo dobrze się realizowało projekt, wsparcie opiekuna z NCBR-u było moim zdaniem bardzo dobre, dobry kontakt, bardzo dobre finansowanie, jakby harmonogram płatności, ja nie mam żadnych zastrzeżeń, dla mnie to było bardzo dobra współpraca”

Źródło: wywiady jakościowe z realizatorami projektów.

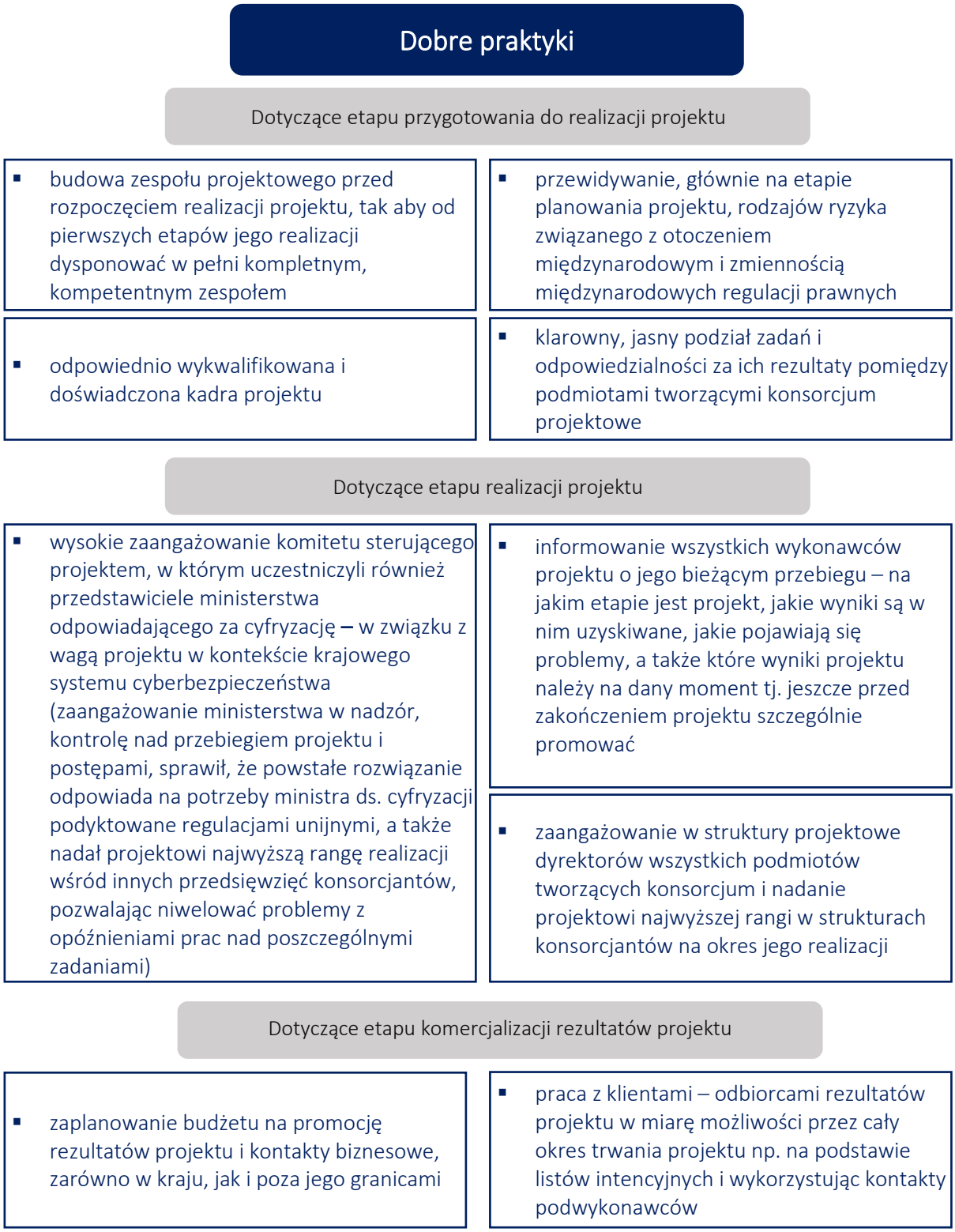
Szczegółowo przyglądając się kooperacji między członkami konsorcjów realizujących projekty, warto wyróżnić główny wniosek płynący z badań, że **współpraca w ich ramach oceniana jest na bardzo wysokim poziomie.** Badani przyzwali, że w znacznym stopniu ułatwiała ona realizację projektu i wpłynęła na wysoką efektywność podjętych działań. Było to możliwe głównie dzięki temu, że partnerzy projektu będący członkami konsorcjum posiadali bardzo duże kompetencje oraz byli przygotowani merytorycznie do prowadzenia współpracy. Ponadto, wyniki badań wskazują, że:

- w większości przypadków do nawiązania współpracy dochodziło poprzez odnowienie starych kontaktów z instytucjami, które wspomagały się wzajemnie w przeszłości;
- główne trudności wynikały ze skomplikowanej tematyki zagadnienia, jakim jest cyberbezpieczeństwo oraz przestrzegania narzuconych odgórnie protokołów[24];
- podmioty są zainteresowane dalszą współpracą w ramach projektów o podobnej tematyce (niektórzy wskazują już konkretne kolejne pomysły, w tym na kontynuację tematów podjętych w dotychczasowych projektach – przykładowo: wykorzystanie opracowanych rozwiązań sprzętowych i programistycznych w innych obszarach związanych z dziedziną cyberbezpieczeństwa, badania adresujące nowe wyzwania technologiczne w zakresie kryptografii kwantowej, przygotowanie rozwiązań dot. ochrony dla podmiotów infrastruktury krytycznej).

[24] Protokoły zakładają utworzenie bezpiecznych kanałów komunikacji oraz infrastruktury potrzebnej do skutecznego działania.

Wiele ciekawych wniosków dotyczących dobrych praktyk, które wspierają skuteczną realizację projektów, zidentyfikowano dzięki przeprowadzonym studiom przypadku – pogłębionym badaniom skupionym na czterech przedsięwzięciach podjętych w ramach Programu[25], odznaczających się dużym stopniem zaawansowania prac, skutecznością, użytecznością oraz dużym potencjałem wypracowanych rozwiązań w kontekście ich wykorzystania na rzecz cyberbezpieczeństwa kraju. Szczegółowe opisy znajdują się w załączniku 7 do niniejszego raportu (Studia przypadków), natomiast Schemat 6 przedstawia najciekawsze kwestie, wspierające sukces projektu.

[25] Projekty: Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria (KSO3C), Narodowa Platforma Cyberbezpieczeństwa (NPC), TAMA – skalowalne i wydajne rozwiązanie programistyczne chroniące sieci operatorskie przed atakami typu DDoS (Distributed Denial of Service, Regionalne Centrum Bezpieczeństwa Cybernetycznego (RegSOC)



Schemat 6. Dobre praktyki związane z realizacją projektów

Źródło: opracowanie własne.

2. Wysoka komplementarność CyberSecIdent z innymi programami[26]

Kluczowe wnioski

- Poza Programem CyberSecIdent, identyfikuje się inne inicjatywy o zasięgu ogólnopolskim, realizowane przez NCBR oraz poza Centrum, które w różnym stopniu dotyczą obszaru cyberbezpieczeństwa. Żaden z nich nie ma jednak takiego istotnego statusu, jaki ma CyberSecIdent, w ramach kluczowego dokumentu strategicznego dotyczącego cyberbezpieczeństwa państwa, jakim jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

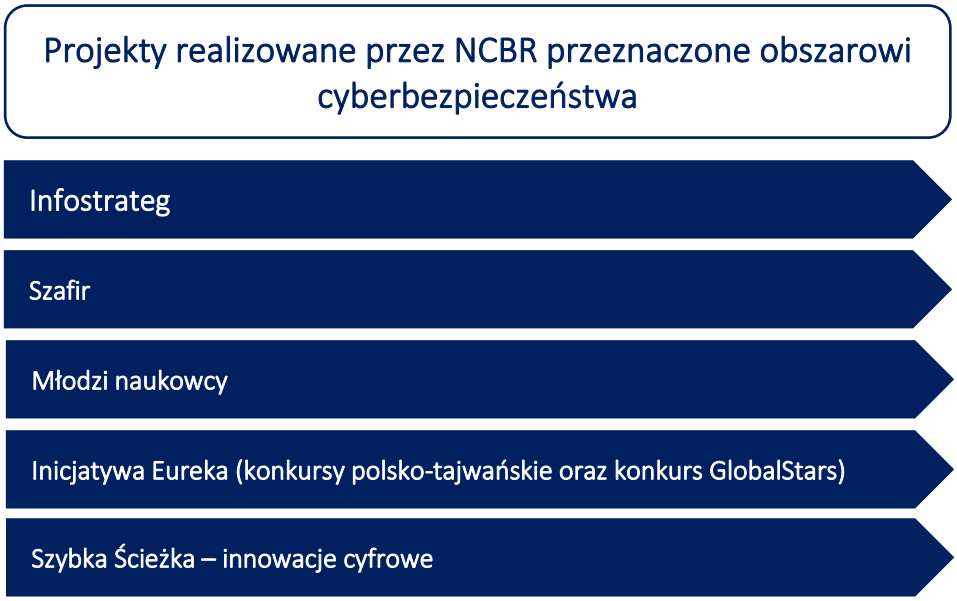
- Program CyberSecIdent względem zidentyfikowanych programów przeznaczonych obszarowi cyberbezpieczeństwa charakteryzuje przede wszystkim komplementarność, w której projekty/programy uzupełniają się przedmiotowo albo przestrzennie, a osiągnięcia efektów poszczególnych projektów/programów nie są uzależnione od realizacji drugiego z projektów/programów.

- Beneficjenci Programu CyberSecIdent mogliby skutecznie realizować w pierwszej kolejności swoje projekty w ramach Szybkiej ścieżki – innowacje cyfrowe. Nie oznacza to, że nie byłoby to możliwe w ramach innych programów (w szczególności międzynarodowych, w ramach inicjatywy Eureka). Wymagałoby to jednak znacznego przemodelowania sposobu realizacji projektu (m.in. w zakresie posiadania zagranicznego partnera). W przypadku Szybkiej Ścieżki – innowacje cyfrowe nie byłoby to konieczne.

[26] Cały zakres przeprowadzonych analiz został przedstawiony w załączniku nr 4 do niniejszego raportu (Analiza danych zastanych – komplementarność Programu).

2.1. NCBR realizuje inne inicjatywy wspierające obszar cyberbezpieczeństwa

Przeprowadzając niniejsze analizy, zidentyfikowano kilka programów realizowanych przez NCBR, które w różnym stopniu dotyczą obszaru cyberbezpieczeństwa (poza CyberSecIdent). W związku z tym, dokonano ich charakterystyki.



Schemat 7. Projekty realizowane przez NCBR przeznaczone obszarowi cyberbezpieczeństwa

Źródło: opracowanie własne.

W kontekście zagadnienia komplementarności istotny jest status programu CyberSecIdent w kluczowym dokumencie strategicznym w obszarze cyberbezpieczeństwa jakim jest Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024[27]. CyberSecIdent wymieniany jest w przypadku dwóch celów szczegółowych tj.:

- numer 1 (Rozwój krajowego systemu cyberbezpieczeństwa) w punkcie 5.5 (Wypracowanie i wdrożenie metodyki szacowania ryzyka na poziomie krajowym);

[27] Patrz: (https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024)

- numer 3 (Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa) w punkcie 7.3 (Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa).

Jednocześnie wśród inicjatyw koordynowanych przez NCBR dotyczących tematyki cyberbezpieczeństwa, w obszarze programów krajowych nie zidentyfikowano takich, które odwoływały się bezpośredniego do tego obszaru. Jedynie CyberSecIdent, według stanu na III kwartał 2023 roku, stanowi program bezpośrednio dedykowany tej tematyce[28].

Wśród programów strategicznych problematyka cyberbezpieczeństwa pojawia się incydentalnie tylko w przypadku jednego z siedmiu z nich tj. programu Infostrateg[29]. Tematy dotyczące cyberbezpieczeństwa obecne są w przypadku programów i projektów zakwalifikowanych do obszaru obronność i bezpieczeństwo. Są to inicjatywy realizowane przez NCBR w porozumieniu z Ministerstwem Obrony Narodowej oraz Ministerstwem Spraw Wewnętrznych. Do programów, które odwołują się do kwestii cyberbezpieczeństwa zaliczyć należy program Szafir (edycje 1-4 realizowane w latach 2020-2021 – w szczególności należy zwrócić uwagę na pierwszą edycję, która była najbardziej zbliżona tematycznie do CyberSecIdent)[30].

Wymienić należy także konkurs „Młodzi Naukowcy" – realizowany w latach 2014-2017 – na wykonanie i finansowanie projektów badań naukowych na rzecz obronności i bezpieczeństwa państwa w ramach programu pn. „Przyszłościowe technologie dla obronności – konkurs

[28] Patrz: Informacje na temat programu CyberSecIdent; (https://www.gov.pl/web/ncbr/cybersecident).
[29] Patrz: Programy strategiczne; (https://www.gov.pl/web/ncbr/programy-strategiczne).
[30] Patrz: Informacje na temat programu Szafir; (https://www.gov.pl/web/ncbr/4szafir2021).

młodych naukowców”[31]. Jego celem było opracowanie przełomowych, innowacyjnych rozwiązań technologicznych oraz zdobycie lub rozwijanie zdolności operacyjnych Sił Zbrojnych RP (SZ RP) i służb odpowiedzialnych za bezpieczeństwo m.in. w obszarach cyberobrony oraz technologii informacyjnych i sieciowych.

Zagadnienia z obszaru cyberbezpieczeństwa zaplanowano również w programach międzynarodowych koordynowanych przez NCBR w ramach inicjatywy Eureka[32]. Są to regularnie ogłaszane konkursy polsko-tajwańskie[33]. Zakładają one realizacje dwustronnych projektów badawczych, które skierowane są do organizacji badawczych i innowacyjnych przedsiębiorstw z Polski i Tajwanu. Wśród programów międzynarodowych dedykowanych bezpośrednio obszarowi cyberbezpieczeństwa wskazać należy również drugi typ konkursu w ramach inicjatywy Eureka, czyli GlobalStars z udziałem Tajwanu[34], którego zakres tematyczny obejmuje m.in. obszar High Tech - ICT and Cyber Security.

Obszarowi cyberbezpieczeństwa przeznaczony jest również konkurs realizowany przez NCBR w ramach szybkiej ścieżki (I Oś Priorytetowa POIR, dla której NCBR jest Instytucją Pośredniczącą)[35]. Po raz pierwszy, od października do listopada 2022 roku trwał nabór na

---

[31] Patrz: (https://archiwum.ncbr.gov.pl/o-centrum/aktualnosci/szczegoly-aktualnosci/news/ogloszenie-konkursu-nr-2p2017-mlodzi-naukowcy-2017-na-wykonanie-i-finansowanie-projektow-badan-n/).
[32] Celem tej inicjatywy jest Celem inicjatywy EUREKA jest zwiększanie nowoczesności, produktywności i konkurencyjności przemysłu europejskiego; (https://www.eurekanetwork.org/about-us/eureka).
[33] Patrz: Informacje na temat konkursu polsko-tajwańskiego; (https://www.gov.pl/web/ncbr/xi-polsko-tajwanski-konkurs).
[34] Patrz: Informacja GlobalStars z udziałem Tajwanu; (https://www.gov.pl/web/ncbr/globalstars-z-udzialem-tajwanu).
[35] Narodowe Centrum Badań i Rozwoju jest Instytucją Pośredniczącą dla dwóch spośród czterech osi priorytetowych tj. I Oś priorytetowa POIR: Wsparcie prowadzenia prac B+R przez przedsiębiorstwa oraz IV Oś priorytetowa POIR: Zwiększenie potencjału naukowo-badawczego; (https://www.gov.pl/web/ncbr/program-operacyjny-inteligentny-rozwoj).

projekty w ramach Szybkiej ścieżki przeznaczonej wyłącznie innowacjom cyfrowym (1/1.1.1/2022)[36]**.** Cieszył się on bardzo dużym zainteresowaniem, o czym świadczy m.in. zwiększenie alokacji tego konkursu[37]. Wśród projektów były również te z obszaru cyberbezpieczeństwa (w tym również takie, które zaliczać można do zakresu tematycznego Programu CyberSecIdent)[38].

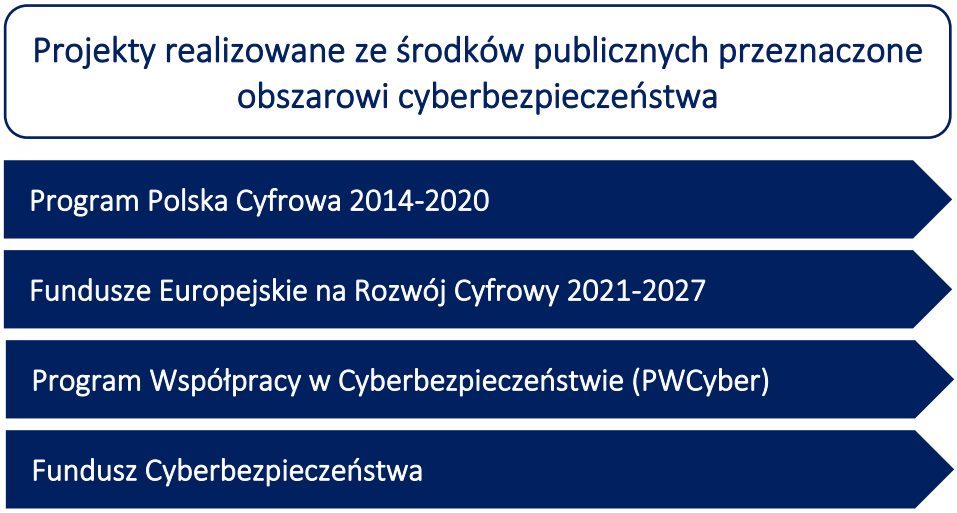
W przypadku zakresu POIR realizowanego przez NCBR istniała potencjalna możliwość składania projektów dotyczących różnorodnych aspektów cyberbezpieczeństwa zarówno w przypadku Osi Priorytetowej (OP) I (np. w ramach szybkiej ścieżki[39]) jak i Osi III (w jej przypadku NCBR jest również Instytucją Pośredniczącą). Programy te nie są jednak bezpośrednio dedykowane tej tematyce.

---

[36] Patrz: (https://www.gov.pl/web/ncbr/11112022-szybka-sciezka-innowacje-cyfrowe).
[37] Jednocześnie należy podkreślić, że Najwyższa Izba Kontroli w przypadku tego konkursu stwierdziła w wystąpieniu pokontrolnym opublikowanym w dniu 13.10.2023 (…) *liczne nieprawidłowości zarówno w procesie przygotowania i organizacji naboru wniosków o dofinansowanie, jak również na etapie wyboru projektów w Konkursie. Naruszenia ustawy wdrożeniowej oraz wytycznych w zakresie wyboru projektów dotyczyły braku niezwłocznego i indywidualnego powiadomienia każdego wnioskodawcy o zmianach Regulaminu Konkursu, a także niepodania do publicznej wiadomości uzasadnienia jednej ze zmian. Stwierdzono również brak transparentności i przejrzystości działań podejmowanych w celu wyłonienia ekspertów na etapie tworzenia składów paneli. Z kolei dokonując wyboru projektów do dofinansowania NCBR nie zachował zasad przejrzystości, rzetelności i bezstronności, o których mowa w art. 37 ust. 1 ustawy wdrożeniowej. Przy ocenie jednego z dwóch analizowanych przez NIK projektów nie dochowano przez ekspertów oceniających wniosek należytej staranności w zakresie kryterium budżetu* [S/23/003 - Organizacja i przyznawanie środków w ramach konkursu Szybka ścieżka – Innowacje cyfrowe (1/1.1.1/2022) realizowanego przez NCBR; (https://www.nik.gov.pl/kontrole/S/23/003/LBI/)]. Zastrzeżenia formułowane przez NIK sprawiają, że zasadne są wątpliwości w zakresie rzeczywistej jakości realizowanych projektów konkursowych przez beneficjentów w tym również w obszarze cyberbezpieczeństwa.
[38] Dotyczy to w szczególności wdrożenia metod i technik identyfikacji i uwierzytelniania.
[39] Dla konkursu nie ma określonego zakresu tematycznego. Projekt dofinansowany w konkursie musi wpisywać się w co najmniej jedną Krajową Inteligentną Specjalizację (KIS).

2.2. Cyberbezpieczeństwo jest też wspierane przez inne inicjatywy publiczne

Przeprowadzając niniejsze analizy, zidentyfikowano też kilka projektów realizowanych poza NCBR, które w różnym stopniu wspierają obszar cyberbezpieczeństwa ze środków publicznych. W związku z tym, dokonano ich charakterystyki.



Schemat 8. Projekty realizowane ze środków publicznyc przeznaczone obszarowi cyberbezpieczeństwa

Źródło: opracowanie własne.

Kwestie cyfrowe pojawiły się w Programie Polska Cyfrowa 2014-2020 (POPC), dla którego Instytucją Pośredniczącą jest Centrum Projektów Polska Cyfrowa, w 2021 roku. Związane było to z nadzwyczajną sytuacją epidemiologiczną wywołaną pandemią COVID-19. Zagadnienia te znalazły się w ramach dodatkowej Osi V – Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia – REACT-EU.

Zagadnienia z obszaru cyberbezpieczeństwa obecne są również w ramach nowej perspektywy finansowej (2021-2027), w Programie Fundusze Europejskie na Rozwój Cyfrowy 2021-2027

(FERC)[40]. Jednym z celów głównych programu jest zapewnienie cyberbezpieczeństwa poprzez wsparcie w ramach nowego dedykowanego obszaru interwencji. Wsparcie w tym obszarze koncentruje się na dwóch działaniach, dla których Instytucją Pośredniczącą będzie Centrum Projektów Polska Cyfrowa[41]:

- Działanie FERC.02.02 Wzmocnienie krajowego systemu cyberbezpieczeństwa; zgodnie z założeniami działania te będą zgodne z polityką cyberbezpieczeństwa UE i wytycznymi Agencji UE ds. cyberbezpieczeństwa. W ramach działania przewidywane są projekty m.in. na rzecz wzmocnienia krajowego systemu cyberbezpieczeństwa. Grupą docelową jest administracja publiczna (w tym rządowa) oraz podległe jej organy i jednostki organizacyjne, podmioty kluczowe dla zapewnienia cyberbezpieczeństwa.
- Działanie FERC.02.05 Wsparcie umiejętności cyfrowych; zgodnie z założeniami, w działaniu przewidziano realizacje projektów mających na celu podnoszenie kompetencji kadr zaangażowanych w świadczenie usług, produktów lub procesów cyfrowych, w tym m.in. wsparcie zaawansowanych kompetencji specjalistycznych z zakresu cyberbezpieczeństwa i gospodarki danych, jak również dostępności cyfrowej. W ramach działania przewidziane są kampanie edukacyjno-informacyjne na rzecz m.in. promowania podnoszenia kompetencji cyfrowych, korzyści wynikających z korzystania z nowoczesnych technologii i e-usług publicznych, rozwijania świadomości dotyczących dostępności cyfrowej i cyberbezpieczeństwa. Grupą docelową jest administracja publiczna (w tym rządowa) oraz podległe jej organy i jednostki organizacyjne, instytucje kultury, jednostki sektora finansów publicznych,

[40] Informacje na temat Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027; (https://www.rozwojcyfrowy.gov.pl/strony/dowiedz-sie-wiecej-o-programie/o-programie/).
[41] Na podstawie Szczegółowego Opisu Priorytetów Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027; (https://www.rozwojcyfrowy.gov.pl/strony/dowiedz-sie-wiecej-o-programie/prawo-i-dokumenty/szczegolowy-opis-priorytetow-programu-fundusze-europejskie-na-rozwoj-cyfrowy-2021-2027/)

obywatele, podmioty kluczowe dla zapewnienia cyberbezpieczeństwa, podmioty lecznicze, pracownicy, przedsiębiorcy.

W przypadku drugiej grupy programów tj. realizowanych ze środków publicznych w obszarze cyberbezpieczeństwa wymienić należy także Program Współpracy w Cyberbezpieczeństwie (PWCyber)[42]. Jego zainicjowanie wynika z wejścia w życie w 2018 roku ustawy o krajowym systemie cyberbezpieczeństwa (Dz.U z 2022 r. poz.1863), która implementuje do polskiego porządku prawnego dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE. L. z 2016 r. nr 194). Ustawa nakłada szereg nowych obowiązków na określone podmioty, w tym m.in. na organy administracji publicznej i wybranych przedsiębiorców, których celem jest zapewnianie niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług. Podmioty wchodzące w skład krajowego systemu cyberbezpieczeństwa tworzą spójny system pozwalający na podejmowanie działań zarówno przeciwdziałających zagrożeniom, jak i zapewniających skuteczne reagowanie na incydenty cyberbezpieczeństwa; PWCyber został uruchomiony w 2019 r. Jest to przedsięwzięcie niekomercyjne o charakterze partnerstwa publiczno-prywatnego, realizowane na rzecz krajowego systemu cyberbezpieczeństwa.

Kolejną z inicjatyw jest Fundusz Cyberbezpieczeństwa. W dniu 19 stycznia 2022 r. Rada Ministrów przyjęła rozporządzenia w sprawie wysokości świadczenia teleinformatycznego osób realizujących zadania z zakresu cyberbezpieczeństwa. Świadczenie będzie mogło zostać przyznane osobom realizującym zadania: w organach i podmiotach, o których mowa w art. 26,

[42] Program Współpracy w Cyberbezpieczeństwie (https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa).

art. 41, art. 44 lub art. 60 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, w zakresie zapewnienia cyberbezpieczeństwa w:

1) Agencji Bezpieczeństwa Wewnętrznego,
2) Agencji Wywiadu,
3) Centralnym Biurze Antykorupcyjnym,
4) jednostkach organizacyjnych podległych Prezesowi Rady Ministrów lub ministrom,
5) Kancelarii Prezesa Rady Ministrów oraz w urzędach obsługujących ministrów,
6) Kancelarii Prezydenta Rzeczypospolitej Polskiej,
7) Kancelarii Sejmu,
8) Kancelarii Senatu,
9) Policji,
10) prokuraturze,
11) Służbie Kontrwywiadu Wojskowego,
12) Służbie Wywiadu Wojskowego,
13) Straży Granicznej,
14) Służbie Ochrony Państwa.

Do zadań z zakresu cyberbezpieczeństwa, za których wykonywanie będzie przysługiwało świadczenie należą m.in. analiza złośliwego oprogramowania, analiza powłamaniowa (forensic), wykrywanie zagrożeń lub incydentów (cyber threat intelligence), czy tworzenie rekomendacji technicznych.

2.3. CyberSecIdent uzupełnia się z pozostałymi inicjatywami

Podsumowując wszystkie powyższe analizy, Program CyberSecIdent względem zidentyfikowanych programów będących zarówno w ofercie NCBR jak i tych realizowanych ze środków publicznych przeznaczonych obszarowi cyberbezpieczeństwa charakteryzuje przede wszystkim typ komplementarności tj. dotyczący sytuacji, w której projekty/programy uzupełniają się przedmiotowo albo przestrzennie, a osiągnięcia efektów poszczególnych

projektów/programów nie są uzależnione od realizacji drugiego z projektów/programów. Ponadto, z przeprowadzonych analiz wynika, że tylko w części obszarów tematycznych realizacja Programu CyberSecIdent ma bezpośredni wpływ na efekty innych programów z obszaru cyberbezpieczeństwa. W szczególności dotyczy to inicjatyw, wskazanych w dokumencie strategicznym Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, przypisanych do Programu CyberSecIdent. Jednocześnie Program ten charakteryzuje względnie wysoka komplementarność uwzględniając zarówno programy będące w ofercie NCBR oraz realizowane ze środków publicznych na poziomie przede wszystkim celu głównego (tj. Podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP przez zwiększenie dostępności narzędzi sprzętowo-programistycznych do roku 2023) oraz w mniejszym stopniu celu szczegółowego numer 1 wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości. Potencjalny brak komplementarności dotyczy jedynie Szybkiej Ścieżki – innowacje cyfrowe, która ma bardzo zbliżone założenia konkursowe (w tym pokrywające się celem Programu CyberSecIdent). Ze względu jednak na fakt, że ostatni IV konkurs Programu CyberSecIdent został zrealizowany w 2020 roku (nabór czerwiec-lipiec), a w przypadku Szybkiej Ścieżki – innowacje cyfrowe pierwszy nabór odbywał się dopiero w III kwartale 2022 roku możliwe jest zidentyfikowanie komplementarności „historycznej".

Podsumowanie analiz w zakresie komplementarności, stanowi tabela numer 1 w przypadku programów realizowanych przez NCBR oraz tabela numer 2, która koncertuje się na programach realizowanych ze środków publicznych.

Tabela 1. Matryca zbieżności programów realizowanych przez NCBR z Programem CyberSecIdent[43]

Nazwa programu	Cele programu	Obszary tematyczne programu	Adresaci wsparcia
Infostrateg	Pokrywają się częściowo	Nie pokrywają się	Nie pokrywają się
Szafir	Pokrywa się częściowo	Pokrywają się częściowo	Nie pokrywają się
Młodzi naukowcy	Pokrywają się częściowo	Pokrywają się częściowo	Nie pokrywają się
Konkurs polsko-tajwański w ramach inicjatywy Eureka	Pokrywają się częściowo	Pokrywają się częściowo	Nie pokrywają się
Konkurs GlobalStars w ramach inicjatywy Eureka	Pokrywają się częściowo	Pokrywają się częściowo	Nie pokrywają się
Szybka ścieżka – innowacje cyfrowe	Pokrywają się	Pokrywają się	Pokrywają się
Pozostałe Podziałania (Oś I i Oś III POIR)	Pokrywają się częściowo	Pokrywają się częściowo	Pokrywają się częściowo

Źródło: opracowanie własne.

[43] Legenda kolorów użytych w matrycy: [ciemnozielony] – pełne pokrywanie się, [zielony] – częściowe pokrywanie się, [jasnozielony] – brak pokrywania się.

Tabela 2. Matryca zbieżności programów realizowanych ze środków publicznych[44]

Nazwa programu	Cele programu	Obszary tematyczne programu	Adresaci wsparcia
Program Polska Cyfrowa 2014-2020	Pokrywają się częściowo	Pokrywają się częściowo	Pokrywają się częściowo
Program Współpracy w Cyberbezpieczeństwie	Pokrywają się częściowo	Pokrywają się częściowo	Nie pokrywają się
Fundusz Cyberbezpieczeństwa	Nie pokrywają się	Nie pokrywają się	Nie pokrywają się
Fundusze Europejskie na Rozwój Cyfrowy[45]	Pokrywają się częściowo	Pokrywają się częściowo	Pokrywają się częściowo

Źródło: opracowanie własne.

Przedstawione analizy skłaniają do wniosku, że **beneficjenci Programu CyberSecIdent mogliby skutecznie realizować w pierwszej kolejności swoje projekty w ramach Szybkiej ścieżki – innowacje cyfrowe.** Możliwe byłoby to również w ramach innych programów (w szczególności międzynarodowych w ramach inicjatywy Eureka). Wymagałoby to jednak znacznego przemodelowania sposobu realizacji projektu (m.in. w zakresie posiadania zagranicznego partnera). W przypadku Szybkiej Ścieżki – innowacje cyfrowe nie byłoby to konieczne. Wynika to w pierwszej kolejności z faktu, że jest to program o charakterze cywilnym[46] o zasięgu

[44] Legenda kolorów użytych w matrycy: [ciemnozielony] – pełne pokrywanie się, [zielony] – częściowe pokrywanie się, [jasnozielony] – brak pokrywania się.
[45] Ze względu na brak szczegółowych danych, ocena ma charakter wstępny/roboczy.
[46] Nie oznacza to jednak, że nie jest możliwe wykorzystanie technologii cywilnych w wojsku. Potwierdzają to technologie dual-use, czyli technologie podwójnego zastosowania tj.

krajowym oraz bardzo podobnej tematyce i przeznaczeniu jak CyberSecIdent (tj. dedykowany jest badaniom przemysłowym, pracom rozwojowym - eksperymentalnym oraz przedwdrożeniowym). Zbliżone są również wymagania dotyczące podmiotów, które mogłyby starać się o dofinansowanie. Istotnym argumentem za wyborem Szybkiej Ścieżki – innowacje cyfrowe (zwłaszcza gdy konsorcjum przygotowujące się do złożenia wniosku składa się z mniejszej liczby podmiotów) jest to, że charakteryzuje się w tej kwestii mniejszymi wymaganiami w zakresie minimalnej liczby wnioskodawców w porównaniu do Programu CyberSecIdent, który zakłada konieczność utworzenia konsorcjum, w składa którego musi wejść minimalnie jedna jednostka naukowa). Dodatkową zaletą Szybkiej ścieżki – innowacje cyfrowe jest to, że daje ona większe możliwości finansowe realizacji projektów większych budżetowo. W IV konkursie CyberSecIdent[47], maksymalna wartość dofinansowania projektu wynosiła 20 milionów PLN, podczas gdy w ramach Szybkiej ścieżki – innowacje cyfrowe maksymalna wartość kosztów kwalifikowalnych to 50 mln euro. Z drugiej strony CyberSecIdent gwarantuje realizację mniejszych projektów. W przypadku Szybkiej ścieżki - innowacje cyfrowe minimalna kwota to 5 milionów PLN, a dla CyberSecIdent – 2 miliony PLN. Zaletą Programu CyberSecIdent jest natomiast maksymalny okres realizacji projektu, który mógł wynieść nawet 36 miesięcy (przy czym realizacja FAZY B nie może trwać dłużej niż 18 miesięcy), a Szybkiej Ścieżki-innowacje cyfrowe - projekt może być realizowany do 31 grudnia 2023 r., w sytuacji gdy termin naboru wniosków miał miejsce na przełomie października-listopada 2022 roku. Stanowi to znaczące utrudnienie dla projektów z obszaru

---

rozwiązania, które mogą być używane zarówno do celów cywilnych, jak i wojskowych. Brak jest jednak programu, który pozwalałby na wykorzystanie efektów realizowanych cywilnych projektów na rzecz wojska opracowanych w ramach zidentyfikowanych programów dotyczących cyberbezpieczeństwa będących zarówno w ofercie NCBR czy innych finansowanych ze środków publicznych w Polsce. Takie inicjatywy należą w Polsce do rzadkości; patrz: (https://startup.pfr.pl/pl/aktualnosci/technologie-dual-use-co-jest-i-jak-moga-na-tym-polu-dzialac-start-upy/)/

[47] Patrz: (https://archiwum.ncbr.gov.pl/aktualne-konkursy/szczegoly-konkursu/competition/iv-konkurs-cybersecident-cyberbezpieczenstwo-i-e-tozsamosc/).

cyberbezpieczeństwa o większym stopniu złożoności czy o wyższym stopniu ryzyk, które mogą potencjalnie wydłużyć okres jego realizacji.

3. Potrzeba rozszerzenia zakresu wsparcia obszaru cyberbezpieczeństwa[48]

Kluczowe wnioski

- Dostępne wsparcie w przyszłości powinno w większym stopniu adresować cyberzagrożenia dotykające obywateli, przedsiębiorców – umożliwiać opracowanie narzędzi i zasad współpracy służb składających się na systemowe wsparcie obywatela w przypadku incydentu. Potrzebne jest też stworzenie portalu, systemu, narzędzi, które będą skupiały w jednym miejscu wszystkie najważniejsze dla obywatela informacje z zakresu cyberbezpieczeństwa – w tym przedstawiały scenariusze/ścieżki pomocy dla osoby/podmiotu, która jej potrzebuje w związku z wystąpieniem cyberincydentu. Taki system jednocześnie może agregować i dostarczać zbiorczych statystyk decydentom. Jednak tematyka ta nie powinna być objęta zakresem kolejnego CSI – może zostać ujęta w innych dostępnych programach.
- Obecne wyzwania w obszarze cyberbezpieczeństwa mocno wiążą się z technikami dezinformacji. Działania wspierające rozwiązania z zakresu cyberbezpieczeństwa powinny być też nakierowane na opracowanie procedur i narzędzi dla obywateli do zgłaszania przypadków dezinformacji służbom.
- Sygnalizuje się też potrzebę wsparcia dla rozwiązań pomagających pozyskiwać i motywować kandydatów na specjalistów z zakresu cyberbezpieczeństwa.
- Zdecydowanie też powinno utrzymać się zakres zagadnień związanych z koordynacją działań między różnymi domenami bezpieczeństwa cyberprzestrzeni oraz z wdrażaniem metod i technik identyfikacji i uwierzytelniania.

Podsumowując przeprowadzone analizy, można wskazać, że aktualna koncepcja Programu CSI, jego cel główny i cele szczegółowe, w mocny, zdecydowany sposób odnoszą się i korzystają ze strategii, polityk i wizji wypracowanych na szczeblu krajowym, a także europejskim. Choć trudno o to, by Program uwzględniał dynamiczne, niespodziewane zmiany

[48] Cały zakres przeprowadzonych analiz został przedstawiony w załączniku nr 5 do niniejszego raportu (Analiza danych zastanych – kontekst badania i przegląd dokumentacji Programu).

w trendach lub wystąpienie skokowego rozwoju określonych technologii, to **zapewnia najlepsze możliwe planowanie i prognozowanie w oparciu o obecną wiedzę.**

To podejście należy podtrzymywać i weryfikować względem najnowszych, najmniejszych nawet zmian w strategiach, politykach lub sposobie patrzenia na określone zjawiska lub zagrożenia. Warto zatem zauważyć, że społeczność specjalistów z zakresu cyberbezpieczeństwa uważa za bardzo ważne i istotne, szczególnie poniższe, wspominane już wcześniej, dwa nowe (względem daty uruchomienia IV konkursu w ramach CSI) dokumenty:

1) Dyrektywę NIS2[49]
2) oraz ustawę o krajowym systemie cyberbezpieczeństwa, która jest w procesie nowelizacji[50].

Jednym z rozwiązań na określenie przedmiotu kolejnego programu jest w związku z tym wykorzystanie zakresu tematycznego do stymulowania badań/działań w jednym z kierunków naświetlonych w tych dokumentach. Aczkolwiek, jak sugerują wyniki niniejszego badania, pozostawienie celów szczegółowych niedomkniętych umożliwia większą kreatywność aplikującym, dając więcej wniosków, spośród których można wybierać finansowane obszary. Co ważne, obecny cel główny i cele szczegółowe Programu są napisane na tyle ogólnie, że nie mijają się z wyżej wymienionymi dokumentami.

[49] Komisja Europejska: Dyrektywa NIS 2 (Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, 2023, dostępne online (2023-08-31): https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive

[50] Ministerstwo Cyfryzacji: Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, 2023, dostępne online (2023-08-31): https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw.html

Analizując obecne trendy w porównaniu z założeniami CSI, można wskazać kilka najważniejszych spostrzeżeń dotyczących tego, jakie działania można i należy podjąć w celu aktualizacji zakresu tematycznego dla przyszłych działań wspierających obszar cyberbezpieczeństwa.

W pierwszej kolejności trzeba dostrzec zmiany w trendach w zakresie cyberzagrożeń. Dynamiczny rozwój obszarów technologii takich jak AI, LLM, spear phishing, smishing, vishing, FineTuned-voice-DeepFakes, znacząco zmienia obserwowane spektrum cyberzagrożeń, a także ich efektywność. Co za tym idzie, rośnie też ich popularność, a więc i negatywny wpływ na podmioty i gospodarkę. Analizy eksperckie sugerują, że obecny zakres Programu zdaje się nie adresować ani zagrożeń, ani obywatela, skupiając się na działaniach na najwyższym poziomie abstrakcji, strategicznym. Tymczasem wiele zagrożeń ma miejsce „u Kowalskiego", powodując że jego komputer (lub firma) traci czas na rozwiązywanie problemów których można było uniknąć, a ponadto stanowi zagrożenie dla danych i dla innych urządzeń w sieci. Jednocześnie jednak należy wskazać, że jest możliwość zaadresowania tego rodzaju wyzwań w innych, komplementarnych programach i inicjatywach.

Biorąc pod uwagę aktualne uwarunkowania, należy też zaakcentować zmiany w cyberprzestrzeni wynikające z geopolityki. Wojna Rosji przeciw Ukrainie, a także groźby i ataki Rosji w kierunku zachodu, ale przede wszystkim bardzo konkretna i zauważalna narastająca intensywność działań rosyjskich grup cyberprzestępczych na terenie Polski powodują, że każdy obywatel powinien mieć świadomość swoich działań i zaniedbań, a także schematów działań cyberprzestępców i właściwych procedur reagowania.

Podsumowując analizy materiałów pochodzących z różnych źródeł, w tym przede wszystkim opracowań dotyczących aktualnych trendów, badań z zakresu cyberbezpieczeństwa oraz wiedzę i opinie eksperckie, wskazano identyfikowane w tym obszarze wyzwania. Znalazły się one w Tabela 3, wraz z odniesieniem do aktualnych założeń CSI i informacją, czy pokrywają się one ze zdiagnozowanymi potrzebami rozwojowymi. Warto podkreślić, że w tabeli znajdują się obszary zagadnień, które stanowią rozbieżność między zapisami i intencjami Programu a

rzeczywistością obserwowaną w strategiach, politykach i dokumentach (niewiele rozbieżności), a także między zapisami Programu a dostrzeżonymi wyzwaniami rozwojowymi w obszarze cyberbezpieczeństwa (spore rozbieżności). Informacje te, w powiązaniu z wynikami analiz dotyczących komplementarności Programu z innymi działaniami, stanowią główne źródło rekomendacji określających kierunki rozwoju ewentualnej kontynuacji CSI.

Tabela 3. Dostrzeżone wyzwania i potrzeby rozwojowe w obszarze bezpieczeństwa cyberprzestrzeni RP

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
1.	Koordynacja domen	Wdrożenie rozwiązań technologicznych ułatwiających współpracę i koordynację działań między różnymi domenami bezpieczeństwa cyberprzestrzeni ze szczególnym uwzględnieniem cyfrowej tożsamości.	Temat już istniejący w CSI. Ważne: warto zastanowić się nad ujednoliceniem wizji tego obszaru z koncepcją przedstawioną w dyrektywie NIS2 oraz zsynchronizować z planowaną nowelizacją KSC.	Temat już istniejący w CSI. Temat ważny również z uwagi na możliwość zgłaszania w jego zakresie innych ciekawych i istotnych (często innowacyjnych) pomysłów.	Zagadnienie nadal aktualne. Rekomendacja: pozostawić.
2.	Uwierzytelnianie i identyfikacja	Wdrożenie metod i technik identyfikacji i uwierzytelniania.	Temat już istniejący w CSI. Ważne: warto zastanowić się nad ujednoliceniem wizji tego obszaru z koncepcją	Temat już istniejący w CSI. Ważny i aktualny, potwierdzony przez CSRB w	Zagadnienie nadal aktualne. Rekomendacja: pozostawić.

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
			przedstawioną w dyrektywie NIS2 oraz zsynchronizować z planowaną nowelizacją KSC	raporcie[51] po atakach grupy Lapsus$, jako wymagający priorytetowego traktowania.	
3.	Cyberoszustwa	Opracowanie narzędzi i zasad współpracy umożliwiających służbom systemowe wsparcie obywatela w przypadku incydentu (malware,	Wiele uwagi poświęcono analizie kodu malware, mechanizmów psychologicznych phishingu, czy fałszywym bramkom	Spośród znalezionych zasobów, działań i literatury, wybitnie pozytywne i profesjonalne wrażenie daje witryna NCSC.gov.uk[52], która	CSI obecnie nie obejmuje wprost cyberzagrożeń

[51] Cyber Safety Review Board: CSRB Review: Attacks Associated With Lapsus$ and Related Threat Groups – Key Findings and Recommendations, 2022, dostępne online (2023-08-31): https://www.cisa.gov/sites/default/files/2023-08/Review%20Of%20The%20Attacks%20Associated%20with%20Lapsus%24%20And%20Related%20Threat%20Groups%20Executive%20Summary_508c.pdf

[52] National Cyber Security Centre: NCSC blog, 2023, dostępne online (2023-08-31): https://www.ncsc.gov.uk/section/keep-up-to-date/ncsc-blog

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
		ransomware, kradzież, phishing, ...). Badania dotyczące systemów eksperckich i AI centralizujących działania i wspomagających współpracę służb w odniesieniu do cyberzagrożeń.	płatności. Tym czasem obywatele nadal są oszukiwani, nadal nie wiedzą jak zareagować, gdzie zgłosić incydent. Względem zagrożeń które zmaterializują się w latach 2023-2024, takich jak [następcy 16Shop], [LLM-based spear phishing],	podejmuje skuteczną próbę przyciągnięcia uwagi jako krajowy competence hub z zakresu cyberbezpieczeństwa („Helping to make the UK the safest place to live and work online"). W Polsce mamy stronę incydent.cert.pl, ale należy zadbać o rozpowszechnianie informacji	(wnioskodawcy muszą „ryzykować naciąganie" celu szczegółowego 1). Nowelizacja KSC[53] wspomina zagadnienie „zgłaszania incydentów".

[53] Ministerstwo Cyfryzacji: Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, 2023, dostępne online (2023-08-31): https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw.html

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
			[WormGPT], albo [profilowany DeepFake vishing „na wnuczka" autentycznym głosem „wnuczka"] obywatele zdają się być bezbronni.	o niej i jej działaniu wśród przedsiębiorców i obywateli (wzmacniać obrany kierunek prowadzonych kampanii społecznych). Ponadto, mamy też w Polsce atmosferę osamotnienia i braku zaufania do Policji w kontekście cyberoszustw, co w efekcie powoduje negatywny wpływ na poziom cyberbezpieczeństwa RP.	Rekomendowane rozszerzenie.
4.	Dezinformacja i AntiTroll	Opracowanie procedur i narzędzi dla obywateli do	Wiele osób dostrzega istnienie wpływów obcych państw w cyberprzestrzeni.	Empirycznym przykładem reakcji jest działanie BBC.com w 2021 – całkowite usunięcie	CSI obecnie nie obejmuje wprost dezinformacji.

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
		zgłaszania przypadków dezinformacji służbom. Badania dotyczące możliwości ustandaryzowania zgłaszania dezinformacji i oznaczania poziomu zaufania wpisów (dezinformacja, konta piszące z egzotycznych IP, z VPN, z farm trolli). Destabilizacja w drodze dezinformacji może być analizowana w celu szacowania intencji organizacji finansującej dezinformację.	Ważna w tym zakresie jest świadomość, że te wpływy używane są, by formować nastroje i modyfikować opinie. Dostrzega się w związku z tym problem polaryzacji społeczeństwa, rosnących niepokojów społecznych, destabilizacji. Wciąż jednak nie są to problemy dostatecznie zauważane i doceniane, co nie jest w interesie Państwa. Wiąże się to z powszechnym stosunkiem do działań podejmowanych w	sekcji komentarzy, zalewanej prorosyjskimi komentarzami propagandowymi (w związku z wspieraniem Ukrainy przez UK). Podobnie nieco wcześniej (czasowo) postąpiła stacja/dziennik Fox News, gdy komentarze polaryzowały społeczeństwo w okresie wyborów. Walka z dezinformacją na forach i w mediach społecznościowych może być prowadzona w połączeniu z obszarem tożsamości i identyfikacji, ale również na	CSI obecnie nie obejmuje wprost systemów Big Data analizy wpisów i komentarzy. (wnioskodawcy musieliby „ryzykować naciąganie” celu szczegółowego 1). Rekomendowane rozszerzenie.

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
		Zbierając treści z artykułów prasowych i co ważniejsze komentarzy pod nimi można na nich budować bazę do określania trendów i wykrywania anomalii, przez co lepszego określania zleceń dezinformacji.	Internecie, do zachowań, wyrażanych opinii (obserwowana jest większa bezkarność w porównaniu z sytuacjami, które mają miejsce w rzeczywistości, np. osoba wykrzykująca kłamstwa pod budynkiem ratusza może być w mniejszym stopniu ignorowana przez przechodzących ludzi, zanim zostanie wylegitymowana przez Policję). W czasach coraz tańszych modeli LLM, (już dziś także	wiele innych sposobów (crowd-review, anomaly detection, punkty zaufania, …). By zaproponować system, który się sprawdzi, trzeba przeprowadzić badania, a później przekonać do niego dostawców informacji. Wypracowanie rozwiązania w tym obszarze jest warte o wiele więcej niż uświadamianie w zakresie dezinformacji i jej wpływu na	

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
			darmowych – on-premise), nie będziemy w stanie powstrzymać automatyzacji farm trolli oraz coraz mniej rozpoznawalnego stylu. Obecnie znane są w literaturze systemy klasyfikacji „fake news", a także systemy „sentiment analysis" do określania nastroju czy emocji. Są również znane i używane systemy kategoryzujące użytkowników pod względem preferencji	poziom (cyber)bezpieczeństwa RP.	

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
			zakupowych, a nawet politycznych.		
5.	CyberSpace	Analiza możliwych scenariuszy użycia (use case) dla podmiotu/osoby potrzebującej pomocy lub informacji z zakresu cyberbezpieczeństwa i zaproponowanie portalu, systemu, narzędzi, które będą agregowały akcje w odpowiednich instytucjach by skutecznie pomóc obywatelowi, a dodatkowo	Instytucje i obywatele, którzy doświadczyli incydentu lub jego skutków, lub chcą się przed nim uchronić, muszą szukać informacji w wielu miejscach rozrzuconych po różnych instytucjach.	Warto w drodze badań określić precyzyjnie potrzeby podmiotów, a później zaproponować system (w tym portal), którym mogłaby się zajmować którąś z obecnie istniejących do tego celu instytucji (MC/MSWiA/NASK-PIB, CSIRT). Dodatkowo systematycznie wypełniając go wartościowymi artykułami i wpisami, przyciągającymi uwagę i utrzymującymi	CSI obecnie nie obejmuje wprost wspierania podmiotów. (wnioskodawcy musieliby „ryzykować naciąganie” celu szczegółowego 1 „pod przykrywką” budowania systemu

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
		dostarczyć zbiorczych statystyk decydentom.	(Anty)przykład: strona MSWiA[54].	zaangażowanie czytelników (osób zainteresowanych cyberprzestrzenią). Przykład ciekawej strony prowadzonej przez taką instytucję: NCSC[55];	„łączącego domeny ...”). Nowelizacja KSC[57] wspomina zagadnienie „zgłaszania incydentów”.

[54] Ministerstwo Spraw Wewnętrznych i Administracji: Cyberbezpieczeństwo, dostępne online (2023-08-31): https://www.gov.pl/web/mswia/cyberbezpieczenstwo
[55] National Cyber Security Centre: NCSC blog, 2023, dostępne online (2023-08-31): https://www.ncsc.gov.uk/section/keep-up-to-date/ncsc-blog
[57] Ministerstwo Cyfryzacji: Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, 2023, dostępne online (2023-08-31): https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw.html

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
				przykład prowadzonej przez korporację: Akamai blog[56].	Rekomendowane rozszerzenie.
6.	CyberForce	Opracowanie systemowych rozwiązań pomagających w pozyskiwaniu, wspieraniu, motywowaniu i docenianiu wybitnych kandydatów na specjalistów z zakresu cyberbezpieczeństwa.	Obecnie słyszana w służbach narracja (również Interpol, czy Secret Service) dotycząca kandydatów mówi, że zauważalnie niższe zarobki i zawężony zakres obowiązków/wyzwań utrudnia pozyskiwanie talentów; średnie firmy	Jednocześnie ten problem wydaje się nie istnieć w Izraelu, który w niesamowicie dynamiczny sposób stał się cyber-potęgą zarówno militarnie jak i biznesowo. Warto zapoznać się z modelem ich pozyskiwania talentów i promowania	CSI obecnie nie obejmuje spójnej koncepcji kreowania przyszłej kadry cyber-specjalistów, zakładając, że wśród studentów znajdą się pasjonaci bez

[56] Akamai: Akamai blog, 2023, dostępne online (2023-08-31): https://www.akamai.com/blog

Lp.	Obszar tematyczny	Opis identyfikowanych wyzwań, zakresu problemów, zagadnień z obszaru	Powiązane aktualne trendy w cyberprzestrzeni, społeczeństwie, kulturze i badaniach	Przykładowe opracowania związane z tematem, rozwiązania istniejące, działania z których można czerpać inspirację, możliwości poprawy sytuacji danego obszaru	Ocena aktualnych założeń CSI pod kątem zakresu, w jakim odpowiadają na zidentyfikowane obszary problemowe
		Wspieranie działań i aktywności oraz kultury CyberResilience.	narzekają na sporą rotację nisko- i wysokowykwalifikowanych pracowników; małe firmy narzekają na brak specjalistów	„cyber-odporności”[58] i zaproponować rozwiązania które pomogą budować cyber-ekosystem[59], który pomoże zwiększać poziom cyberbezpieczeństwa polskich firm i służb.	systemowego wspierania. Rekomendowane rozszerzenie.

Źródło: opracowanie własne.

[58] Cyberspatial: What Makes Israel So Good at Hacking? [6:15] How Israel recruits the best hackers, 2022, dostępne online (2023-08-31): https://youtu.be/IluKcbamqfk?t=365

[59] Cyberspatial: What Makes Israel So Good at Hacking? [13:29] How does a country create a cyber ecosystem?, 2022, dostępne online (2023-08-31): https://youtu.be/IluKcbamqfk?t=809

Podsumowując, dynamiczny rozwój obszarów technologii takich jak AI, LLM, voice-DeepFake znacząco zmienia oblicze zagrożeń typu phishing i podobnych; także drugi czynnik – narastająca intensywność działań rosyjskich grup cyberprzestępczych na terenie również naszego kraju – stanowią bardzo ważne argumenty w kierunku zasygnalizowania potrzeby rozszerzenia zakresu tematycznego Programu CSI.

Inwestycja w cyberbezpieczeństwo kraju nie powinna się ograniczać do kilku systemów lub narzędzi opracowanych na szanowanych uczelniach. Inwestycja w cyberbezpieczeństwo RP będzie efektywna wtedy, gdy podejmowane działania będą się w stanie spotkać z nieprzewidywalną przyszłością, a to możliwe będzie gdy:

1) **wspierane projekty będą korzystały z najnowszych technologii, w tym AI, Big Data**, będą potrafiły wskazać nietypowe zachowania w sieci lub w systemach i w porę zareagować;
2) **wspierane będą też projekty które wytworzą wizję cyber-ekosystemu** – mechanizmu wspierania i stymulowania kompetencji z zakresu cyberbezpieczeństwa, zarówno jako rozwiązań holistycznych, jak w Izraelu[60], jak i w sposób „olimpijski" (BugBounty/CTF/Hackathon), np. amerykańskie [HackNYU],[HackMIT];
3) **wspierane będą też projekty proponujące narzędzia i działania umożliwiające podmiotom/ obywatelom zgłaszanie incydentów oraz wyszukiwanie informacji i pomocy** w zakresie cyberbezpieczeństwa (owszem istnieje kilka stron, np. incydent.cert.pl, ale nigdzie przedsiębiorca/ obywatel nie znajduje konkretnych kompleksowych informacji/pomocy dostosowanych do swoich bardzo realnych potrzeb.

[60] Cyberspatial: What Makes Israel So Good at Hacking? [6:15] How Israel recruits the best hackers, 2022, dostępne online (2023-08-31): https://youtu.be/IluKcbamqfk?t=365

II Podsumowanie

Wyzwania w obszarze cyberzagrożeń będą pogłębiać się, biorąc pod uwagę zarówno rozwój nowych technologii, jak i globalne zmiany o charakterze geopolitycznym. Dlatego ważne jest, aby śledzić zachodzące trendy oraz nauczyć się rozpoznawać powiązane z nimi zagrożenia w cyberprzestrzeni, dążyć do ich zrozumienia i przeciwdziałać im. W tym obszarze niezbędne jest pogłębianie wiedzy oraz rozwój innowacyjnych rozwiązań z zaangażowaniem specjalistów o odpowiednich kompetencjach, ale również szerokiego, interdyscyplinarnego grona decydentów. Tematyka cyberbezpieczeństwa wiąże się bowiem w mniej lub bardziej pośredni sposób z wieloma dziedzinami – nie tylko z informatyzacją, ale również działaniem administracji państwa na różnych szczeblach, obronnością kraju, gospodarką oraz działalnością edukacyjną i naukową. W związku z powyższym, niezwykle istotne jest finansowanie działań związanych z obszarem cyberbezpieczeństwa w różnych wymiarach – przy czym należy zadbać, by podejmowane interwencje z wykorzystaniem różnych środków i źródeł były wobec siebie komplementarne. Ważnym elementem systemu działań na rzecz cyberbezpieczeństwa powinny być programy wspierające prace B+R – i w takim właśnie kierunku powinna rozwijać się ewentualna kontynuacja CSI. Wyniki badania pokazują, że taki Program jest potrzebny, jednak jego realizacja powinna przebiegać z zachowaniem wyżej wskazanego założenia o koordynacji współpracy z różnymi resortami – tylko wtedy wdrożenie programu przyniesie o wiele większą skuteczność oraz użyteczność wypracowanych rozwiązań.

Załączniki

1. Metody i techniki badawcze
2. Tabela rekomendacji
3. Analiza danych zastanych – komplementarność Programu
4. Analiza danych zastanych – zakres Programu a nowe wyzwania
5. Studia przypadków

Źródła

1. CyberSecIdent „Cyberbezpieczeństwo i eTożsamość" – założenia Programu B+R [aktualizacja nr 3], listopad 2020 r.
2. NCBiR: https://archiwum.ncbr.gov.pl/programy/programy-krajowe/cybersecident/
3. NCBiR: CyberSecIdent, 2022, dostępne online (2023-08-31): https://www.gov.pl/web/ncbr/cybersecident
4. NCBiR: IV konkurs CyberSecIdent – Cyberbezpieczeństwo i e-Tożsamość, 2020, dost. online (2023-08-31): https://www.gov.pl/web/ncbr/iv-konkurs-cybersecident--cyberbezpieczenstwo-i-e-tozsamosc
5. Ministerstwo Cyfryzacji: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, 2019, dostępne online (2023-08-31): https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2019-2024 (wersja opublikowana w Monitorze Polskim)
6. Wojsko Polskie: Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, 2019, dostępne online (2023-08-31): https://www.wojsko-polskie.pl/aszwoj/u/93/94/9394db01-d323-4635-b798-ac4effa0a822/polska.pdf (wersja z komentarzami, z szatą graficzną)
7. Sejm.gov.pl: Ustawa z dnia 5 lipca 2018 o krajowym systemie cyberbezpieczeństwa, 2018, dostępne online (2023-08-31): https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560
8. Ministerstwo Cyfryzacji: Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa, 2023, dostępne online (2023-08-31): https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-niektorych-innych-ustaw.html
9. NASK: Polityka Unii Europejskiej w zakresie obrony cyberprzestrzeni (EU Policy on Cyber Defence, EPCD), 2022, dostępne online (2023-08-31):

https://cyberpolicy.nask.pl/polityka-unii-europejskiej-w-zakresie-obrony-cyberprzestrzeni-eu-policy-on-cyber-defence/
10. Komisja Europejska: Dyrektywa NIS 2 (Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, 2023, dostępne online (2023-08-31): https://digital-strategy.ec.europa.eu/pl/policies/nis2-directive
11. Parlament Europejski: Rezolucja Parlamentu Europejskiego z dnia 10 czerwca 2021 r. w sprawie strategii UE w zakresie cyberbezpieczeństwa na cyfrową dekadę, 2021, dostępne online (2023-08-31): https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_PL.html
12. Komisja Europejska: Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) 2019/881 as regards managed security services, 2023, dostępne online (2023-08-31): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023PC0208
13. NASK: Analizy rozwiązań legislacyjnych i strategicznych w zakresie cyberbezpieczeństwa i nowoczesnych technologii, 2023, dostępne online (2023-08-31): https://cyberpolicy.nask.pl/category/analizy/
14. PIB NASK: Biuletyn CyberPOLICY, ISSN 2657-8425, 2023, dostępne online (2023-08-31): https://cyberpolicy.nask.pl/
15. PIB NASK: Biuletyn CyberPolicy Review, ISSN 2657-8360, 2020, dostępne online (2023-08-31): https://cyberpolicy.nask.pl/category/biuletyn/
16. NASK: Raporty z serii Cyberbezpieczeństwo A.D., 2020, dostępne online (2023-08-31): https://cyberpolicy.nask.pl/category/cyberbezpieczenstwo-ad/
17. NASK: Wywiady eksperckie z zakresu cyberbezpieczeństwa i nowoczesnych technologii, 2023, dostępne online (2023-08-31): https://cyberpolicy.nask.pl/category/wywiady-eksperckie/
18. NASK: Materiały dotyczące tematyki partnerstw publiczno-prywatnych w obszarze cyberbezpieczeństwa, 2023, dostępne online (2023-08-31): https://cyberpolicy.nask.pl/category/partnerstwa-publiczno-prywatne/
19. Ministerstwo Cyfryzacji: Krajowy system cyberbezpieczeństwa, 2018, dostępne online (2023-08-31): https://www.gov.pl/web/cyfryzacja/krajowy-system-cyberbezpieczenstwa-
20. Ministerstwo Spraw Wewnętrznych i Administracji: Cyberbezpieczeństwo, dostępne online (2023-08-31): https://www.gov.pl/web/mswia/cyberbezpieczenstwo
21. CSIRT.gov.pl: Publikacje Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT), 2021, dostępne online (2023-08-31): https://csirt.gov.pl/cer/publikacje

22. Rada Europejska: Polityki – Cyberbezpieczeństwo, 2023, dostępne online (2023-08-31): https://www.consilium.europa.eu/pl/policies/cybersecurity/
23. European Union Agency for Cybersecurity: ENISA Reports, 2023, dostępne online (2023-08-31): https://www.enisa.europa.eu/publications
24. Cybersecurity & Infrastructure Security Agency: Resources, 2023, dostępne online (2023-08-31): https://www.cisa.gov/resources-tools/resources
25. Warszawski Instytut Bankowości: Raport Cyberbezpieczny Portfel 2022, Związek Banków Polskich, 2022, dostępne online (2023-08-31): https://zbp.pl/aktualnosci/wydarzenia/Raport-Cyberbezpieczny-Portfel-2022
26. Microsoft: Cybersecurity, 2023, dostępne online (2023-08-31): https://www.microsoft.com/en-us/cybersecurity
27. Google: Safety Center, 2023, dostępne online (2023-08-31): https://safety.google/intl/en_us/
28. IBM: Cybersecurity, 2021, dostępne online (2023-08-31): https://www.ibm.com/topics/cybersecurity
29. PARP: Mapa rozwoju rynku i technologii dla obszaru cyberbezpieczeństwa, 2022, dostępne online (2023-08-31): https://smart.gov.pl/images/BTR_Cyberbezpieczestwo_FINAL_19.01.22.pdf
30. NASK-PIB, CERT Polska: Raport roczny z działalności CERT Polska 2022: Krajobraz bezpieczeństwa polskiego internetu, 2023, dostępne online (2023-08-31): https://cert.pl/uploads/docs/Raport_CP_2022.pdf
31. EY Polska: Ochrona sektorów kluczowych przed atakami cyberprzestępców, 2022, dostępne online (2023-08-31): https://www.ey.com/pl_pl/cybersecurity/ochrona-sektorow-kluczowych-przed-atakami-cyberprzestepcow
32. KPMG: Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu, 2023, dostępne online (2023-08-31): https://kpmg.com/pl/pl/home/insights/2023/02/barometr-cyberbezpieczenstwa-2023-detekcja-i-reakcja-na-zagrozenia-w-czasie-podwyzszonego-alertu.html , https://assets.kpmg.com/content/dam/kpmg/pl/pdf/2023/02/pl-raport-kpmg-w-polsce-barometr-cyberbezpieczenstwa-2023-secured.pdf
33. Eurostat: ICT security measures used by EU enterprises in 2022, 2022, dostępne online (2023-08-31): https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20221208-2
34. National Cyber Security Centre: NCSC blog, 2023, dostępne online (2023-08-31): https://www.ncsc.gov.uk/section/keep-up-to-date/ncsc-blog
35. Cyber Safety Review Board: CSRB Review: Attacks Associated With Lapsus$ and Related Threat Groups – Key Findings and Recommendations, 2022, dostępne online

(2023-08-31): https://www.cisa.gov/sites/default/files/2023-08/Review%20Of%20The%20Attacks%20Associated%20with%20Lapsus%24%20And%20Related%20Threat%20Groups%20Executive%20Summary_508c.pdf
36. Akamai: Akamai blog, 2023, dostępne online (2023-08-31): https://www.akamai.com/blog
37. Cyberspatial: What Makes Israel So Good at Hacking? [6:15] How Israel recruits the best hackers, 2022, dostępne online (2023-08-31): https://youtu.be/IluKcbamqfk?t=365
38. Cyberspatial: What Makes Israel So Good at Hacking? [13:29] How does a country create a cyber ecosystem?, 2022, dostępne online (2023-08-31): https://youtu.be/IluKcbamqfk?t=809
39. Eurostat: https://ec.europa.eu/eurostat/web/products-eurostat-news/w/edn-20230214-1
40. Rada Europejska: https://www.consilium.europa.eu/pl/infographics/cyber-threats-eu/
41. IBM Security: Cost of a Data Breach Report 2022", IBM Security
42. Rada Europejska: https://ec.europa.eu/eurostat/web/products-eurostat-news/-/edn-20200211-1
43. Ministerstwo Spraw Wewnętrznych i Administracji: https://www.gov.pl/web/mswia/dotychczas-wprowadzane-stopnie-alarmowe-i-stopnie-alarmowe-crp-na-terytorium-rp
44. KPMG: Raport „Barometr cyberbezpieczeństwa. Detekcja i reakcja na zagrożenia w czasie podwyższonego alertu", 2023, Raport „Barometr cyberbezpieczeństwa. Ochrona cyfrowej tożsamości", 2022
45. NASK-PIB/CERT Polska: „Raport roczny z działalności CERT Polska. Krajobraz bezpieczeństwa polskiego Internetu 2021"
46. NCBiR: Programy strategiczne; (https://www.gov.pl/web/ncbr/programy-strategiczne
47. O NPC: https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2088,Narodowa-Platforma-Cyberbezpieczenstwa-NPC.html
48. NIK, Informacja o wynikach kontroli „Strategiczne programy badań naukowych", 2020; (https://www.nik.gov.pl/plik/id,23485,vp,26211.pdf).
49. Informacje na temat programu Infostrateg; (https://www.gov.pl/web/ncbr/infostrateg).
50. https://www.gov.pl/web/cyfryzacja/krajowe-ramy-polityki-cyberbezpieczenstwa
51. Informacje na temat programu Szafir; (https://www.gov.pl/web/ncbr/4szafir2021).
52. https://archiwum.ncbr.gov.pl/o-centrum/aktualnosci/szczegoly-aktualnosci/news/ogloszenie-konkursu-nr-2p2017-mlodzi-naukowcy-2017-na-wykonanie-i-finansowanie-projektow-badan-n/
53. https://www.eurekanetwork.org/about-us/eureka
54. Informacje na temat konkursu polsko-tajwańskiego; (https://www.gov.pl/web/ncbr/xi-polsko-tajwanski-konkurs)

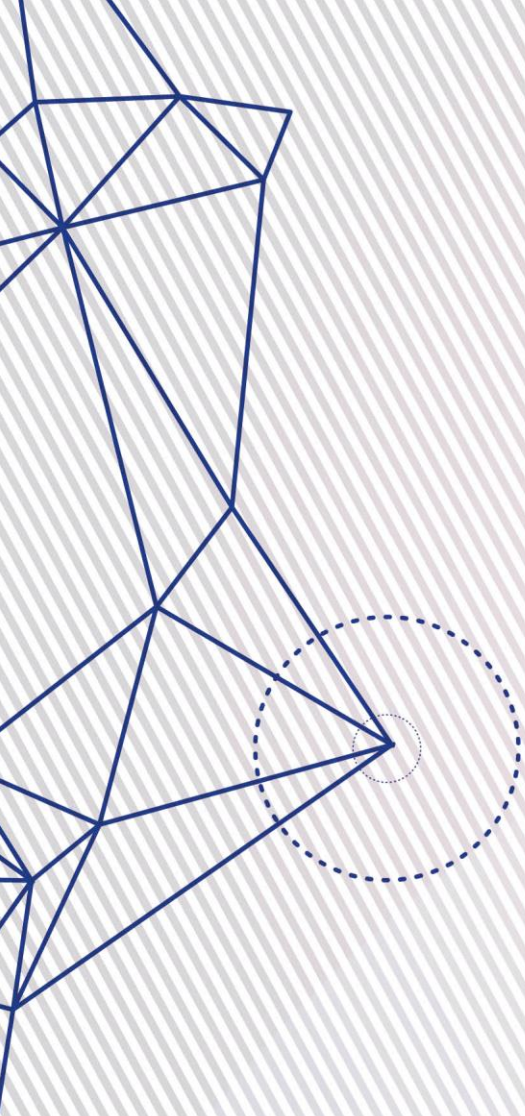
55. Informacja GlobalStars z udziałem Tajwanu; https://www.gov.pl/web/ncbr/globalstars-z-udzialem-tajwanu
56. https://www.gov.pl/web/ncbr/program-operacyjny-inteligentny-rozwoj
57. https://www.gov.pl/web/ncbr/11112022-szybka-sciezka-innowacje-cyfrowe
58. Ewaluacja ex-ante Projektu pozakonkursowego pn. „Monitoring Krajowej Inteligentnej Specjalizacji" Programu Operacyjnego Inteligentny Rozwój 2014-2020; https://www.parp.gov.pl/storage/publications/pdf/Raport-mid-term-Monitoring-KIS.pdf
59. https://smart.gov.pl/images/Opisy-KIS_13.02.2023_accepted.pdf
60. „Krajowa Inteligentna Specjalizacja (KIS) - aktualizacja 2020 r.; https://smart.gov.pl/images/Krajowa_Inteligentna_Specjalizacja_-_za_nr_2.pdf
61. Lista projektów realizowanych z Funduszy Europejskich w Polsce w latach 2014-2020; https://www.funduszeeuropejskie.gov.pl/strony/o-funduszach/projekty/lista-projektow/lista-projektow-realizowanych-z-funduszy-europejskich-w-polsce-w-latach-2014-2020/
62. Informacje na temat Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027; https://www.rozwojcyfrowy.gov.pl/strony/dowiedz-sie-wiecej-o-programie/o-programie/
63. Szczegółowy Opis Priorytetów Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027; (https://www.rozwojcyfrowy.gov.pl/strony/dowiedz-sie-wiecej-o-programie/prawo-i-dokumenty/szczegolowy-opis-priorytetow-programu-fundusze-europejskie-na-rozwoj-cyfrowy-2021-2027/)
64. Program Współpracy w Cyberbezpieczeństwie (https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber--partnerstwo-publiczno-prywatne-na-rzecz-krajowego-systemu-cyberbezpieczenstwa).
65. (https://startup.pfr.pl/pl/aktualnosci/technologie-dual-use-co-jest-i-jak-moga-na-tym-polu-dzialac-start-upy/)/

Spisy elementów

Spis tabel

Spis schematów

Spis rysunków



Narodowe Centrum
Badań i Rozwoju

ul. Chmielna 69,
00-801 Warszawa
Polska

ncbr.gov.pl
sekretariat@ncbr.gov.pl
+48 22 39 07 170