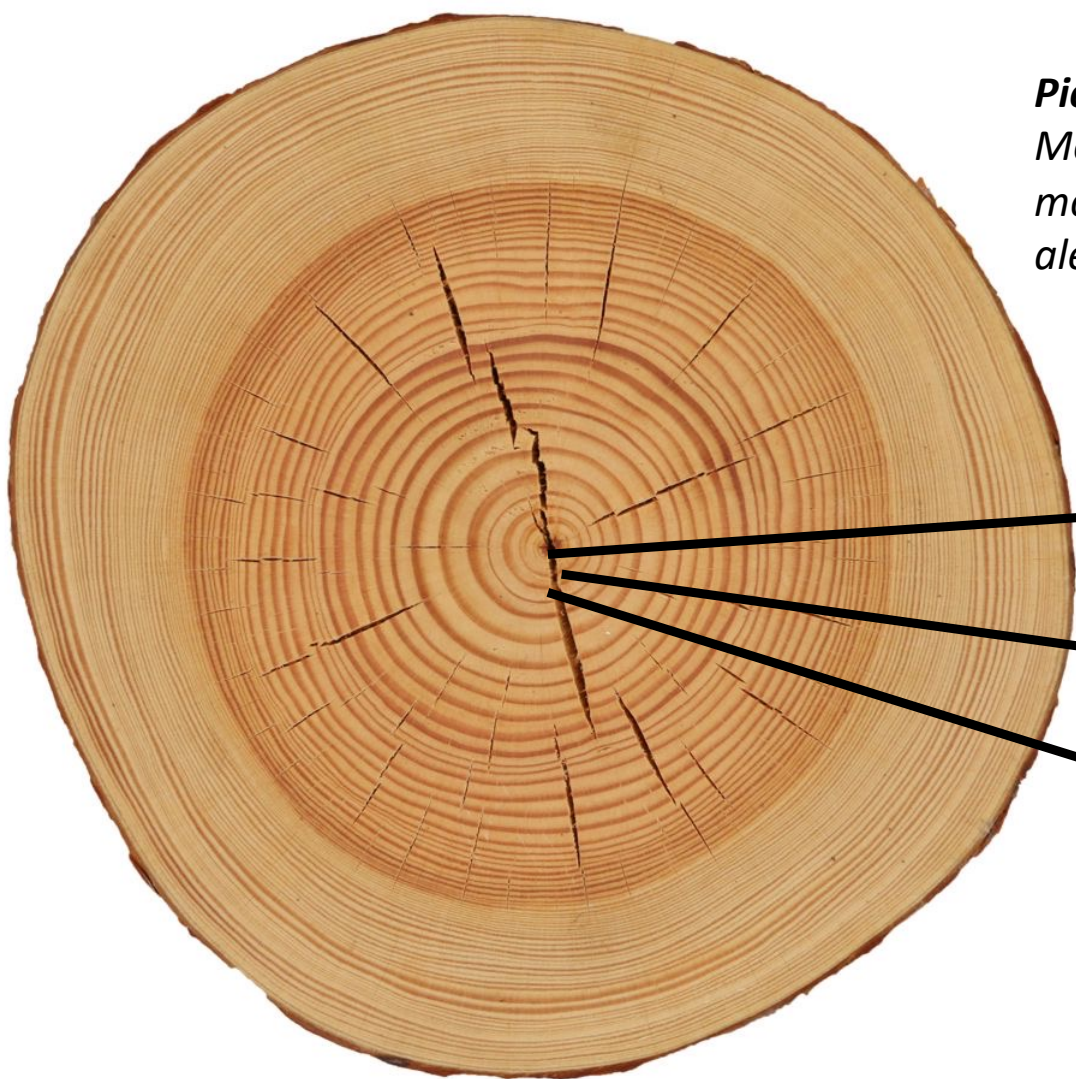


Cyberbezpieczeństwo na Politechnice Warszawskiej jako priorytetowy obszar badawczy i nowy kierunek studiów

Krzysztof Szczypiorski

Wydział Elektroniki i Technik Informatycznych PW



*Pieniądze są warte wyłącznie tyle, ile można z nimi zrobić.
Można je wydać na jedzenie,
można je przegrać w kasynie,
ale też można za nie posadzić **drzewa**.*

Centrum Badawcze POB Cyberbezpieczeństwo i Analiza Danych

2019: Złożenie projektu IDUB przez PW
i decyzja o przyznaniu finansowania

2020: Utworzenie **CB POB Cyber&DS**

2020: Pierwszy konkurs na granty CyberiADa

[Strona główna »](#)

Centra Badawcze POB

Technologie fotoniczne będą skoncentrowane na opracowaniu i badaniu nowej generacji materiałów fotonicznych oraz na rozwijaniu nowoczesnych technologii opartych na wykorzystaniu światła.

Sztuczna inteligencja i robotyka – prace skoncentrują się na przecięciu obszarów sztucznej inteligencji, robotyki i matematyki stosowanej. Celem prac będzie skonstruowanie robota kompana.

Cyberbezpieczeństwo i analiza danych, w tym analiza danych biomedycznych, przetwarzanie BigData i strumieniowa analiza danych, metody uczenia maszynowego, matematyczne podstawy analizy danych.

Biotechnologia i inżynieria biomedyczna w Politechnice Warszawskiej będzie rozwijać nowe metody diagnostyczne w terapii chorób cywilizacyjnych, zwłaszcza w obszarach onkologii oraz kardiologii.

Technologie materiałowe dotyczą zagadnień z zakresu rozwoju nowych materiałów i technologii o przełomowym znaczeniu dla nauki i gospodarki, w tym nanotechnologii i technologii przyrostowych.

Fizyka wysokich energii i technika eksperymentu oraz fizyka zderzeń jądrowych, fizyka plazmy, komputery kwantowe, ich elektroniczne, programistyczne, mechaniczne, konstrukcyjne techniki eksperymentalne.

Konwersja i magazynowanie energii dotyczy w szczególności zagadnień z obszaru baterii, ogniw paliwowych, przekształtników energoelektronicznych, fotowoltaiki oraz energetyki słonecznej.

Centra Badawcze POB

Technologie fotoniczne

Sztuczna inteligencja i robotyka

Cyberbezpieczeństwo i analiza danych

Biotechnologia i inżynieria biomedyczna

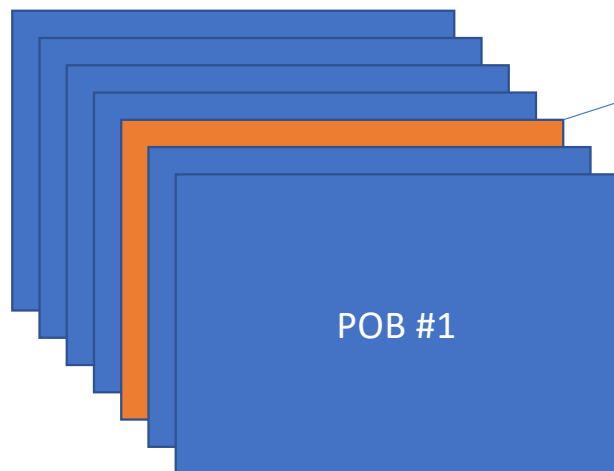
Technologie materiałowe

Fizyka wysokich energii i technika eksperymentu

Konwersja i magazynowanie energii

Cyberbezpieczeństwo i Analiza Danych

POB #1 - POB#7



POB #1

2.3 Informatyka Techniczna i Telekomunikacja

6.3 Matematyka

2.2 Automatyka, Elektronika i Elektrotechnika

2.4 Inżynieria Biomedyczna

Opis zakresu POB	"Cyberbezpieczeństwo i analiza danych", w tym analiza danych biomedycznych, przetwarzanie BigData i strumieniowa analiza danych, metody uczenia maszynowego, matem. podst. an. danych	
Dziedziny nauki i dyscypliny naukowe określone w rozporządzeniu Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r. w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz. U. poz. 1818), związane z POB	Obszary tematyczne zgodne z klasyfikacją subject categories (baza Web of Science) związane z POB	Obszary tematyczne zgodne z klasyfikacją all science journal classification (baza Scopus) związane z POB
<ul style="list-style-type: none"> • 2.3 - Dziedzina nauk inżyniersko-technicznych/informatyka techniczna i telekomunikacja • 6.3 - Dziedzina nauk ścisłych i przyrodniczych/matematyka 	<ul style="list-style-type: none"> - Computer Science, Hardware & Architecture - Computer Science, Information Systems - Computer Science, Interdisciplinary Applications - Computer Science, Software Engineering - Computer Science, Theory & Methods - Genetics & Heredity - Mathematical & Computational Biology - Mathematics, Interdisciplinary Applications - Medical Informatics 	<ul style="list-style-type: none"> - Genetics - Computational Theory and Mathematics - Hardware and Architecture - Signal Processing - Software - Information Systems and Management - Media Technology - Computational Mathematics - Modelling and Simulation
Kierunki studiów związane z POB	1. Cyberbezpieczeństwo; 2. Telekomunikacja; 3. Informatyka; 4. Informatyka i systemy informacyjne; 5. Inżynieria i analiza danych; 6. Matematyka i analiza danych.	

POB Cyberbezpieczeństwo i analiza danych



- **Cyberbezpieczeństwo:** zautomatyzowane systemy zarządzania bezpieczeństwem, systemy zapewnienia niezaprzeczalności, ochrona danych ze wsparciem technik uczenia maszynowego, wykrywanie nieznanym ataków, kryptografia postkwantowa



- **Przetwarzanie Big Data i strumieniowa analiza danych:** rozproszone składowanie, analiza strumieniowa, inteligentne miasta, systemy inteligentnego dynamicznego planowania połączeń
- **Analiza danych biomedycznych:** bioinformatyka, biostatystyka oraz medycyna obliczeniowa, wysokoprzepustowe metody sekwencjonowania następnej generacji, diagnostyka molekularna
- **Zaawansowane metody uczenia maszynowego:** modele predykcyjne z wyjaśnieniem decyzji, grupowanie, klasyfikacja i łączenie danych
- **Matematyczne podstawy analizy danych:** statystyka, metody stochastyczne, sieci złożone, systemy dynamiczne, równania różniczkowe, matematyka dyskretna, teoria grafów, zbiory rozmyte

$$\square + \square = \square$$

 Okręt flagowy

Mantra: “Data is the New Oil”

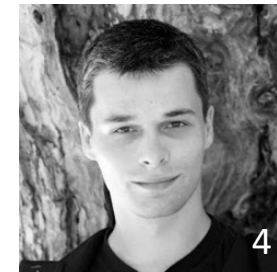
Zespół CB POB CyberDS czyli skład Rady Naukowej

1. dr hab. inż. **Krzysztof Szczypiorski**, prof. uczelni (WEiTI) – przewodniczący
 2. dr inż. **Andrzej Bartosiewicz** (Thales Polska)
 3. dr hab. inż. **Przemysław Biecek**, prof. uczelni (WMiNI)
 4. dr hab. inż. **Tomasz Gambin**, prof. uczelni (WEiTI)
 5. dr hab. inż. **Marcin Iwanowski**, prof. uczelni (WE)
 6. prof. dr hab. inż. **Zbigniew Kotulski** (WEiTI)
 7. prof. dr hab. inż. **Jan Maciej Kościelny** (WMech)
 8. dr hab. inż. **Wojciech Matysiak**, prof. uczelni (WMiNI)
 9. dr hab. **Robert Olszewski**, prof. uczelni (WGiK)
- oraz
10. mgr **Katarzyna Kamińska** (WEiTI) – sekretarz naukowy

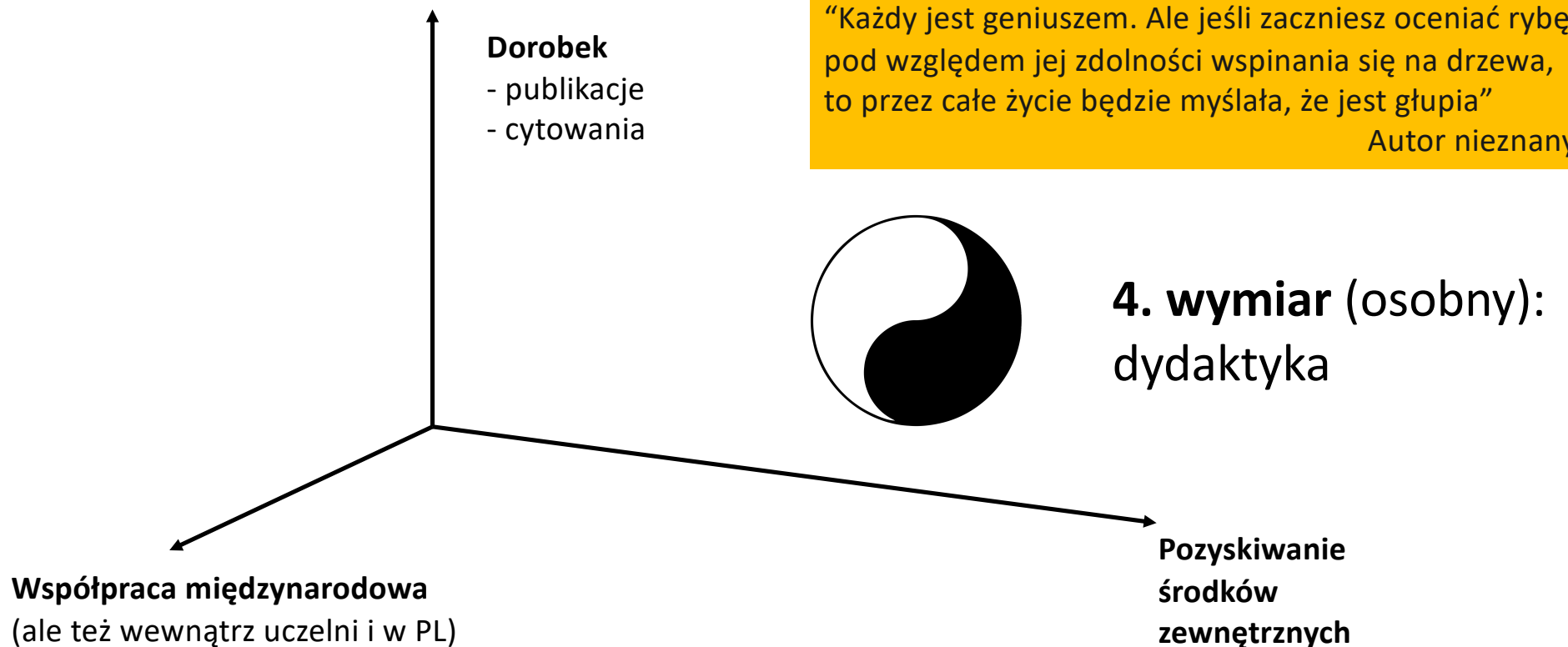
Kontakt:

pob.cyberds@pw.edu.pl

5 wydziałów
+ osoba z zewnątrz (biznes)



Uczelnia badawcza z perspektywy naukowca



Misja – wizja – strategia CB POB Cyber&DS

- **Innowacyjność** – odważne pomysły i pasja – model startupowy
- **Interdyscyplinarność:**
 - „na krawędzi” np. matematyka oraz informatyka techniczna i telekomunikacja (ITiT)
 - „nowe przekroje” np. nauki społeczne oraz ITiT – „psychoinformatyka”???
- **Współpraca wewnętrzna** – zespół, kooperacja między zespołami, kooperacja między centrami badawczymi POB [instytuty, wydziały, dyscypliny]
- **Kolaboracja z otoczeniem gospodarczym**, czyli z przemysłem i biznesem
- **Rozwój osobisty (zarządzanie zmianą)** – najlepsze momenty w życiu na akcelerację:
 - zaawansowany doktorat, a być może wcześniej
 - czas po obronie doktoratu
 - czas po życiowym kryzysie
- ☒ Okręt flagowy: „**Cyberbezpieczeństwo sieci przemysłowych i Internetu Rzeczy**”

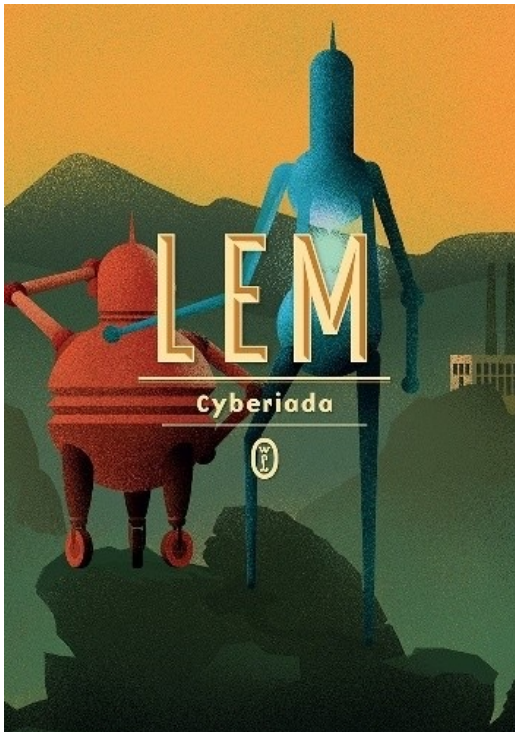
Cele strategiczne CB POB Cyber&DS

- **Cel główny (CG):**
Rozwój obszaru cyberbezpieczeństwo i analiza danych na PW w zakresie naukowym, dydaktycznym i kadrowym
- **Cele szczegółowe (CS):**
 - **CS 1:** Wspieranie kultu(ry) innowacyjności (jako głównego motor działań)
 - **CS 2:** Wspieranie interdyscyplinarności (jako dodatkowego motoru)
 - **CS 3:** Wsparcie współpracy wewnętrznej
 - **CS 4:** Wsparcie kolaboracji z otoczeniem gospodarczym
 - **CS 5:** Inwestycja w młodych (duchem, nie PESELeM) naukowców
 - **CS 6:** Rozwój kierunków studiów związanych z POB
 - **CS 7:** Powiązanie dydaktyki z badaniami naukowymi

Otoczenie: projekt IDUB z perspektywy zespołu badawczego



CyberiADa



Granty wewnętrzne motywujące do tworzenia i rozwoju zespołów badawczych ukierunkowane na zdobywanie funduszy zewnętrznych

- **trzy edycje** (dwie w 2020 i jedna w 2021)
- Wpłynęło **58 wniosków** o łącznej wartości **10,9 mln PLN**
- Ufundowano **27 projektów** o łącznej wartości **4,93 mln PLN** (średnia ok. 180k PLN)
- Max. czas trwania grantu – 2 lata

1. **Gry obronne Stackelberga w obszarze cyberbezpieczeństwa**
2. MARS - Opracowanie koncepcji i prototypu systemu symulacji procesu terratransformacji Marsa
3. **Obrona infrastruktury sieci teleinformatycznych przed ukierunkowanymi atakami niszczącymi – model optymalizacyjny**
4. **Algorytmy, projektowanie i testy cyberbezpieczeństwa w instalacjach przemysłowych**
5. Analiza danych sekwencjonowania DNA trzeciej generacji ze szczególnym uwzględnieniem jakości odczytanych symboli
6. **Grafowa reprezentacja zdarzeń i strumieni komunikacji na potrzeby detekcji cyberzagrożeń**
7. Modelowanie przebiegu epidemii z uwzględnieniem współchorobowości oraz nastawienia społecznego
8. [Con2Con] Od kontrowersji do konsensusu: Analiza konfliktu w dyskursie publicznym online
9. Analiza numeryczna i matematyczna modelu Kołmogorowa oraz przestrzenie Sobolewa
10. **Wielowymiarowe modele uczenia maszynowego do analizy ruchu sieciowego ze szczególnym uwzględnieniem sieci przemysłu 4.0**
11. Głęboka analiza regulacji dotyczących sztucznej inteligencji z wykorzystaniem modeli językowych, analizy sieciowej i gramatyki instytucjonalnej
12. **Analiza skutków i możliwości wykrywania ataków typu RoQ/DoS prowadzonych w sieciach optycznych za pomocą sprzęgacza przypinanego**

CyberSummer@WUT aka Solaris

Politechnika
Warszawska



[Strona główna](#) » [Konkursy](#) » [Wyniki konkursów](#) » [2021](#) »

Wyniki konkursu na granty badawcze CyberSummer@WUT

Opublikowano: 12.07.2021 13:02

W zakończonym konkursie na granty badawcze dla studentów CyberSummer@WUT do finansowania skierowano 7 wniosków.

Celem programu CyberSummer@WUT jest akceleracja włączania studentów w działalność badawczo-rozwojową prowadzoną na Politechnice Warszawskiej w ramach Centrum Badawczego POB Cyberbezpieczeństwo i analiza danych (CB POB Cyber&DS).



 [Lista laureatów CyberSummer@WUT](#) (.pdf, 132,53 kB)

Konkursy

[Aktualne konkursy](#)

[Archiwum konkursów](#)

Wyniki konkursów

2021

2020



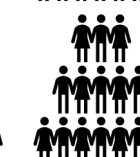
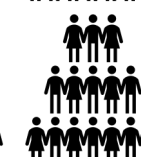
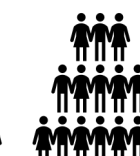
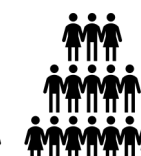
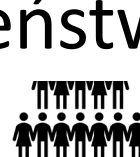
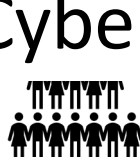
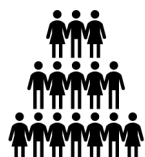
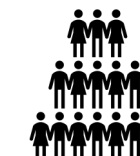
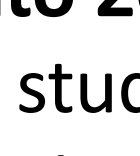
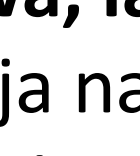
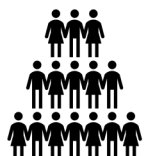
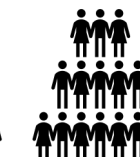
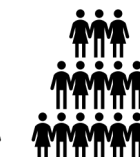
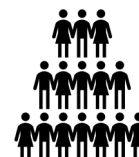
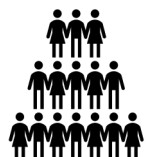
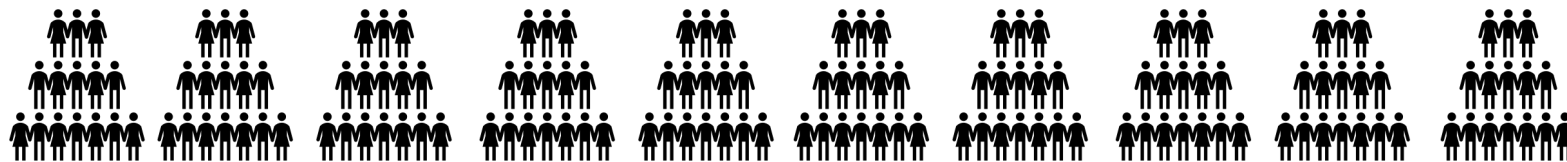
© 1998-2021 Politechnika Warszawska,
Pl. Politechniki 1, 00-661 Warszawa

Inne planowane działania 2022-2023

- **CyberiADa**
- **CyberEDU:**
 - CyberSummer@WUT aka Solaris
 - wsparcie nowych kierunków studiów
- **CyberLAB:** inwestycja aparaturowe
- **CyberDEMO:** projekty celowe np.:
 - system trenowania pracowników przed atakami typu phishing,
 - system ostrzegania przed cyberstalkingiem
- Opracowanie koncepcji niezależnego Instytutu Badawczego z modelem samodzielnego finansowania

1320

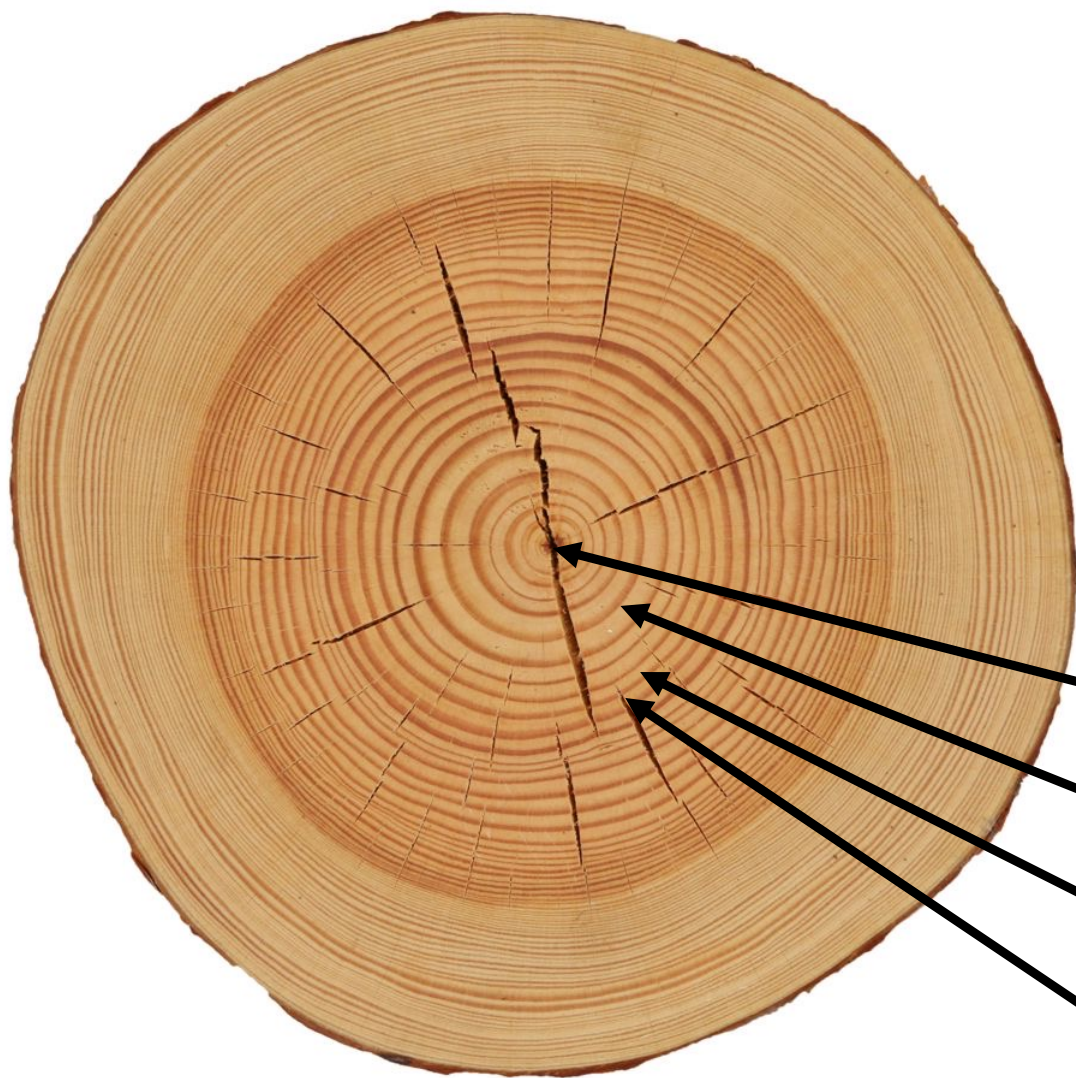
kandydatów



Warszawa, lato 2021:

rekrutacja na studia pierwszego stopnia

na kierunku Cyberbezpieczeństwo na PW



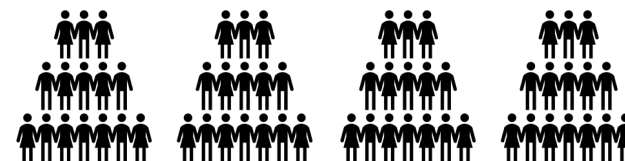
Cyberbezpieczeństwo to jeden z **najpopularniejszych** kierunków studiów na PW

Rekrutacja Cyber I°:

2019: 31 osób na miejsce - II miejsce na PW

2020: 20 osób na miejsce - II miejsce na PW

2021: 22 osoby na miejsce - I miejsce na PW



60 miejsc rocznie

2014: Początek prac nad projektem
finansowanym zewnętrznym od **2018**

2019: Start Cyber I°(19Z)

2023: Pierwsi absolwenci Cyber I°(22Z)
Start Cyber II° (23L)

2024: Pierwsi absolwenci Cyber II° (24L)

10 lat

Jak zbudować dobry program akademicki w zakresie cyberbezpieczeństwa?



USA jest światowym liderem w zakresie cyberbezpieczeństwa, ale też w edukacji.



Jaki jest właściwy model współpracy z otoczeniem społeczno-gospodarczym?

- Drugim liderem światowym w cyberbezpieczeństwie jest **Izrael**
- W Izraelu cyberbezpieczeństwo to **istotna gałąź przemysłu**, a izraelski model gospodarczy w tym zakresie bazuje na ścisłej **współpracy** między **biznesem**, **ośrodkami naukowymi** i **wojskiem**
 - Komentarz: jest to współczesna adaptacja **modelu amerykańskiego z czasów zimnej wojny**, który doprowadził do narodzin i rozwoju Doliny Krzemowej w Kalifornii



biznes.interia.pl/raport/polska_izrael/news/cyberbezpieczenstwo-doswiadczenia-izraela-w-kontekscie,2563971,86

Cyberbezpieczeństwo - doświadczenia Izraela w kontekście czwartej rewolucji przemysłowej i wojny hybrydowej - Biznes w INTERIA

INTERIA FAKTY BIZNES SPORT MOTO TECH GRY MUZYKA FILM KOBIETA MENWAY PLOTKI

interia BIZNES

Szukaj

Start Wiadomości Giełdy Waluty Praca Firma Nieruchomości Budownictwo Podatki Media Prasa Galerie Biz

Notowania GPW | Waluty online | Kredyty hipoteczne | Mapa serwisu | Newsroom | Makroekonomia | Ubezpieczenia

POLSKA-IZRAEL | KIERUNEK GOSPODARKA
פולין-ישראל: כיוון כלכלי

PARTNERZEM PROJEKTU
PFR
Polski Fundusz Rozwoju

Rozmiar tekstu: A A A

Cyberbezpieczeństwo - doświadczenia Izraela w kontekście czwartej rewolucji przemysłowej i wojny hybrydowej

Czwartek, 12 kwietnia (10:00)

Izrael jest drugim po Stanach Zjednoczonych państwem pod względem rozwoju systemów cyberbezpieczeństwa i jednym z najczęściej atakowanych przez hakerów. Siły Obrony Izraela (IDF) są doskonale przygotowane, aby bronić jego fizycznych i cyfrowych granic. Dlatego wojsko stało się kolebką innowacji dla całej gospodarki.





Search NIST

NIST MENU

Information Technology Laboratory / Applied Cybersecurity Division

NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION (NICE)

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development.



- About +
- News +
- Events +
- Resources +

CONNECT WITH US

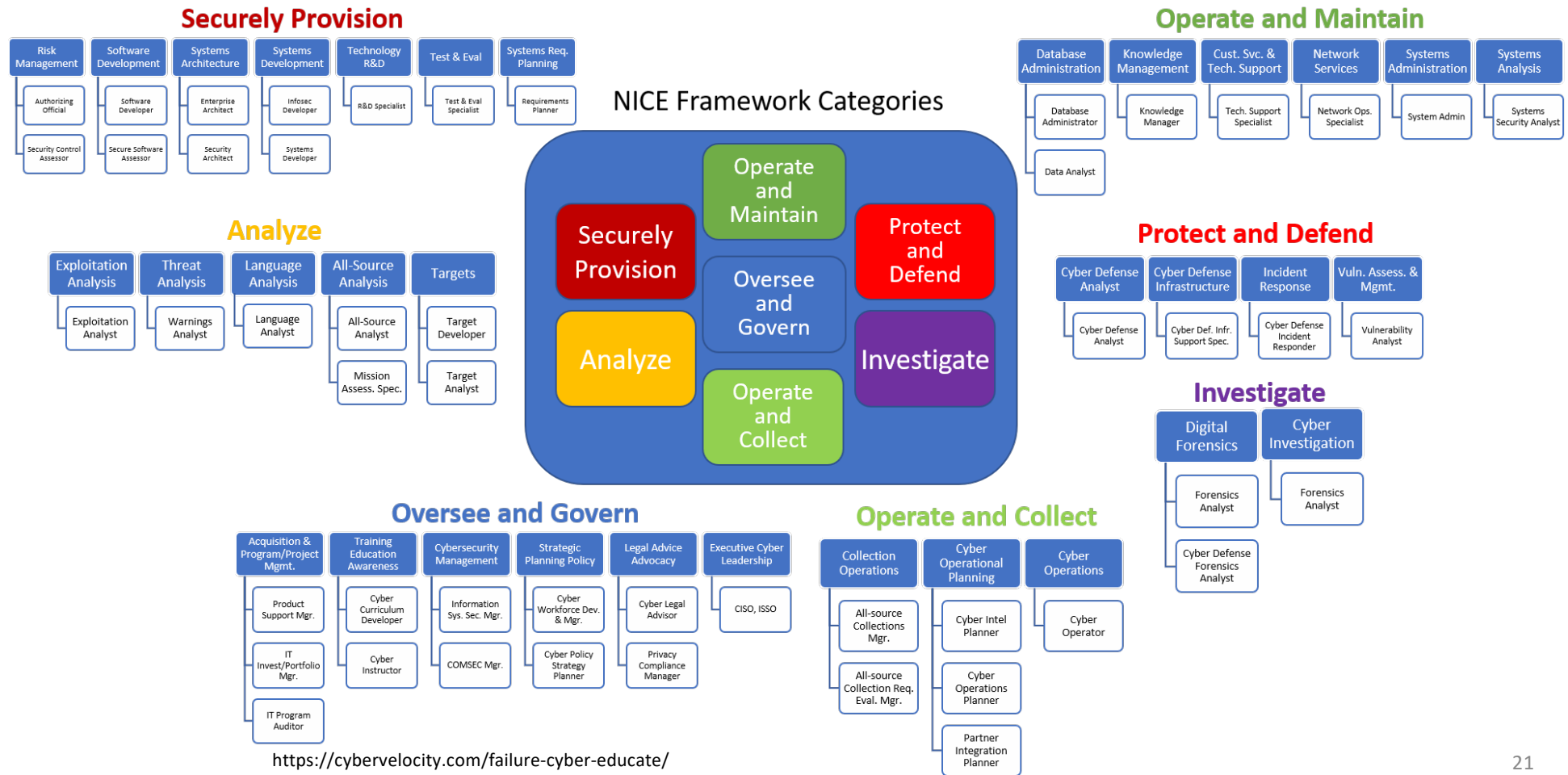


NICE
NATIONAL INITIATIVE FOR CYBERSECURITY EDUCATION

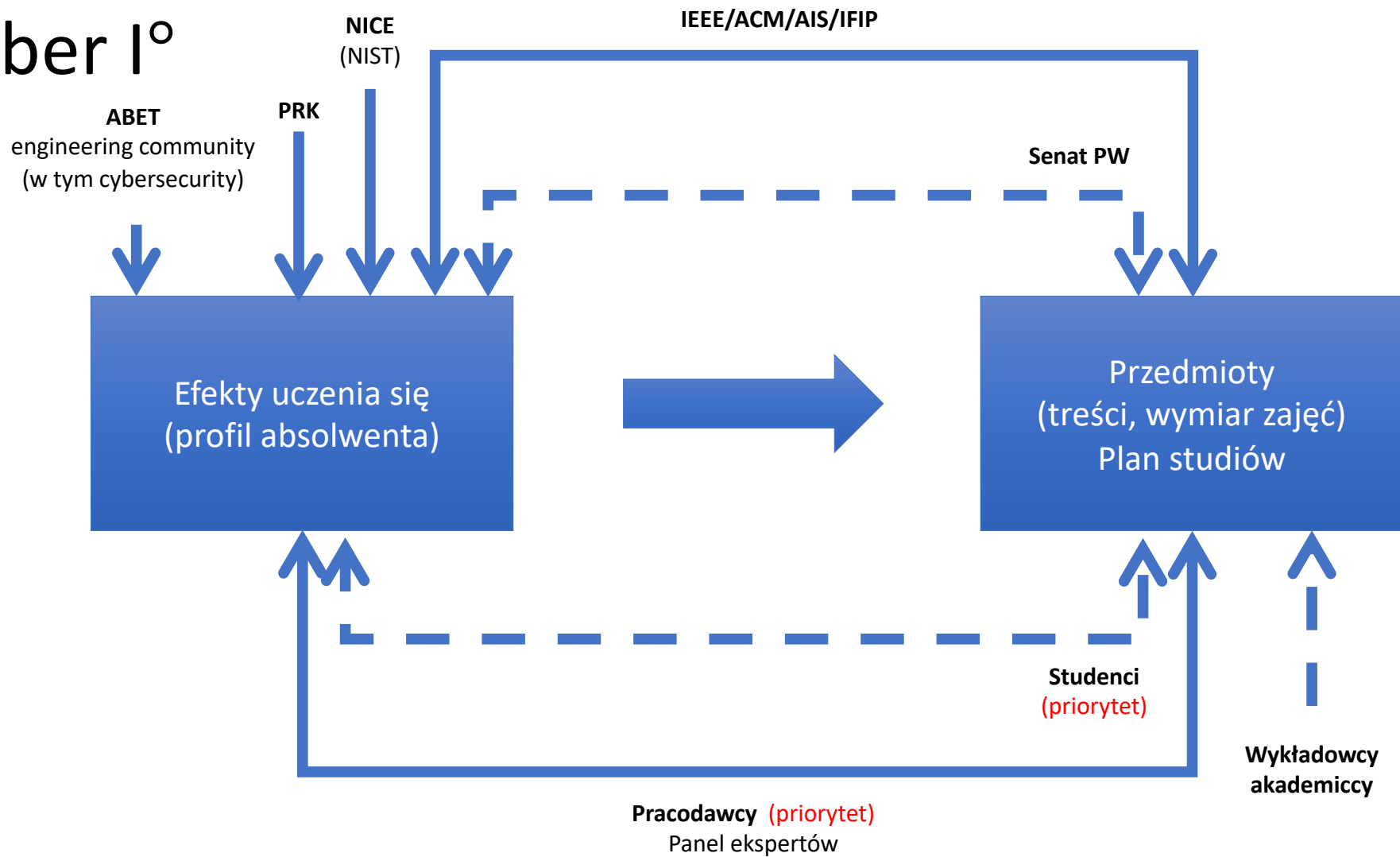
Careers
Cybersecurity Skills
Workforce Learning

Learn more about NICE

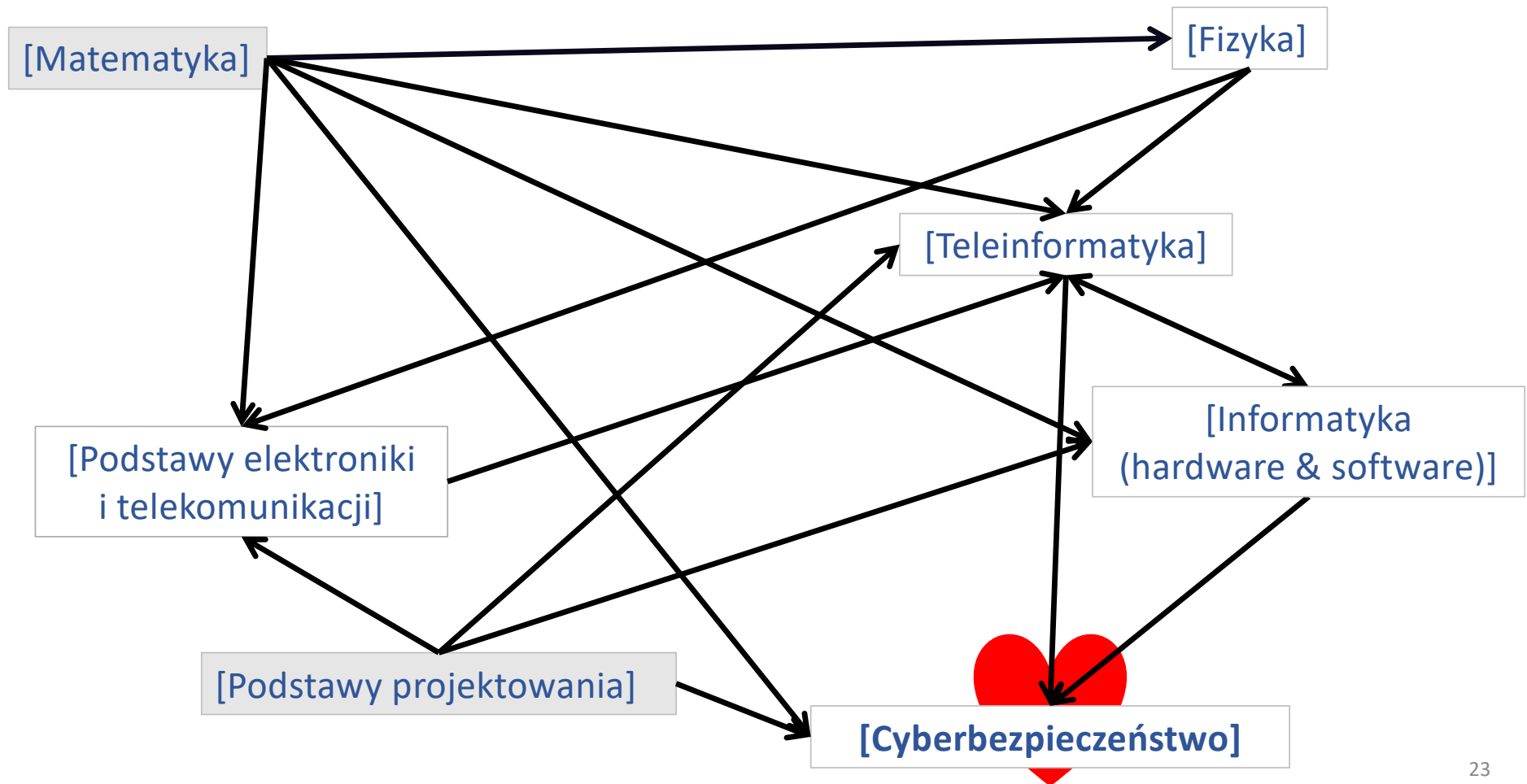
NICE: 52 cyber-zawody



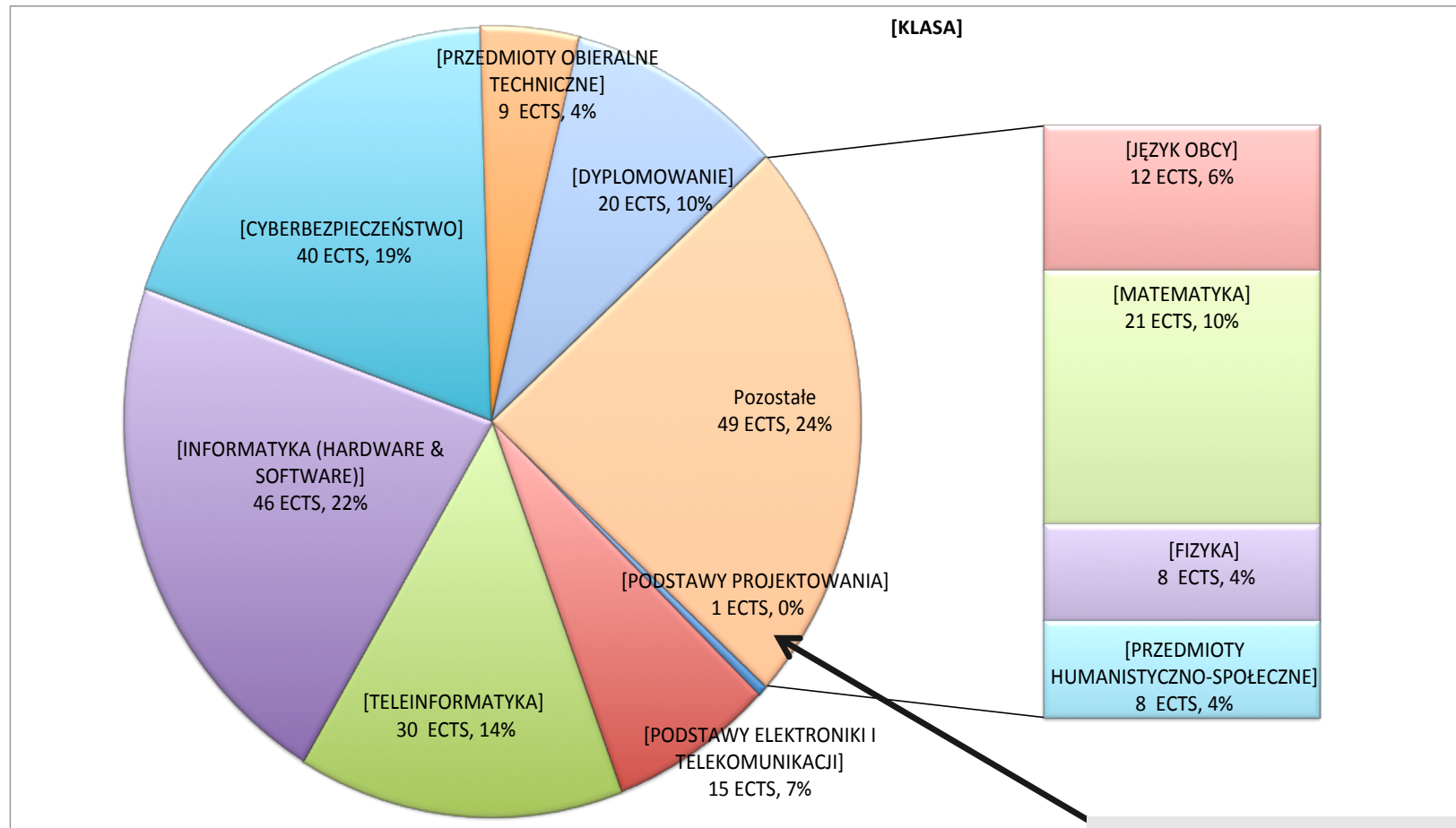
Cyber I°



Cyber I^o: 7 głównych klas



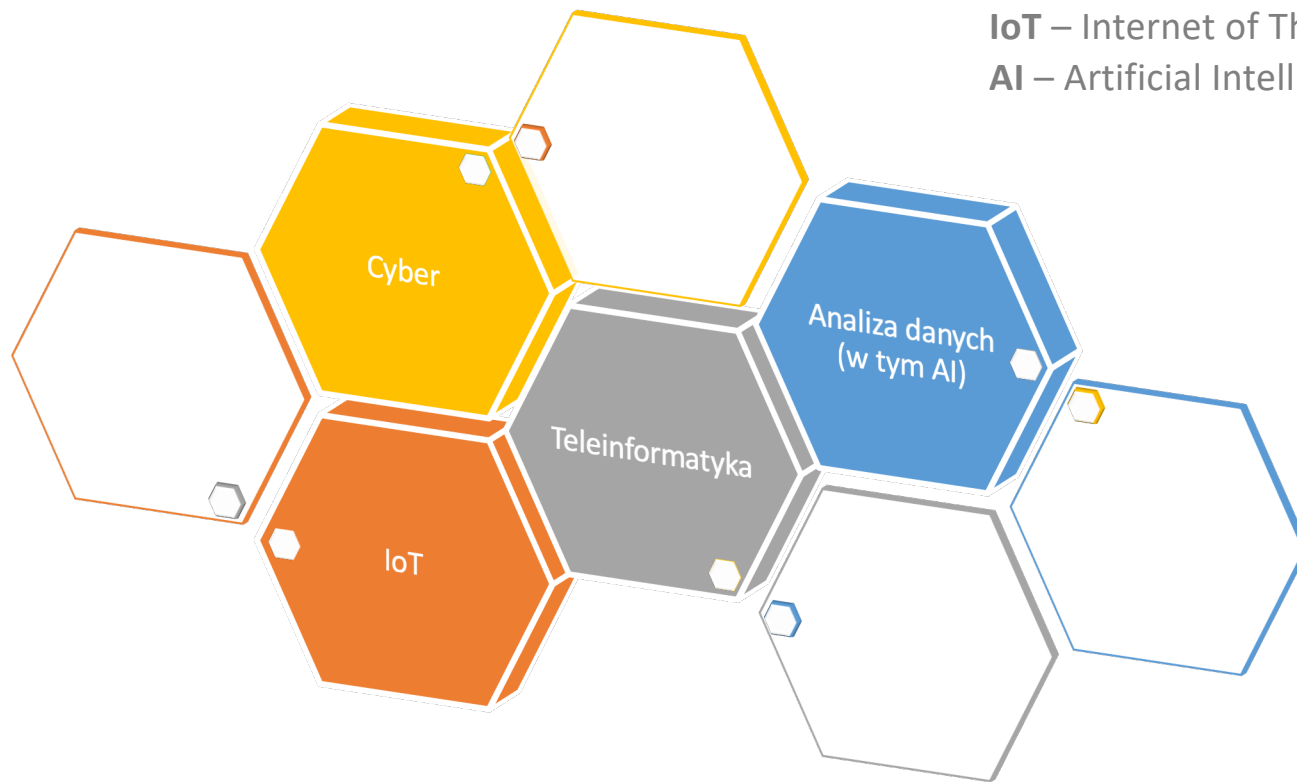
Wszystkie 12 klas (z WF)



Tu początek prezentowania klas (zgodnie ze wskazówkami zegara)

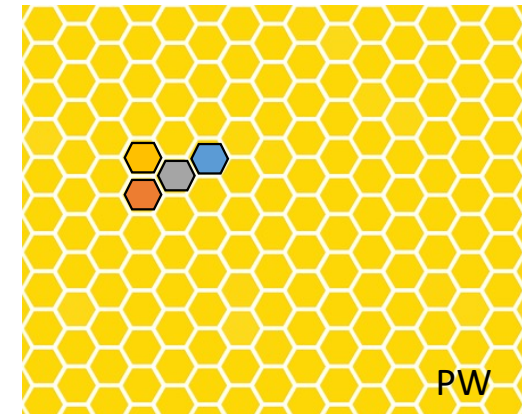
210 ECTS na 7 semestrów = 30 ECTS na semestr (WF – 0 ECTS)

Istotne obszary (także w dydaktyce) związane z nowymi technikami informacyjnymi



IoT – Internet of Things – Internet Rzeczy

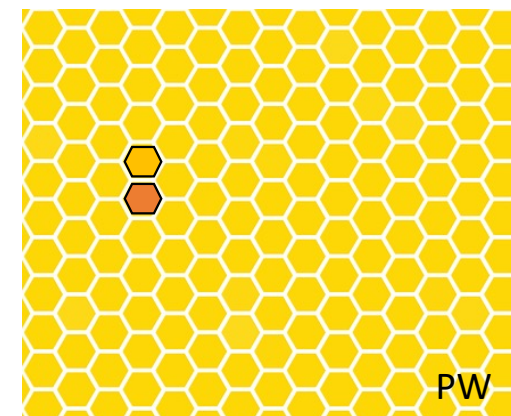
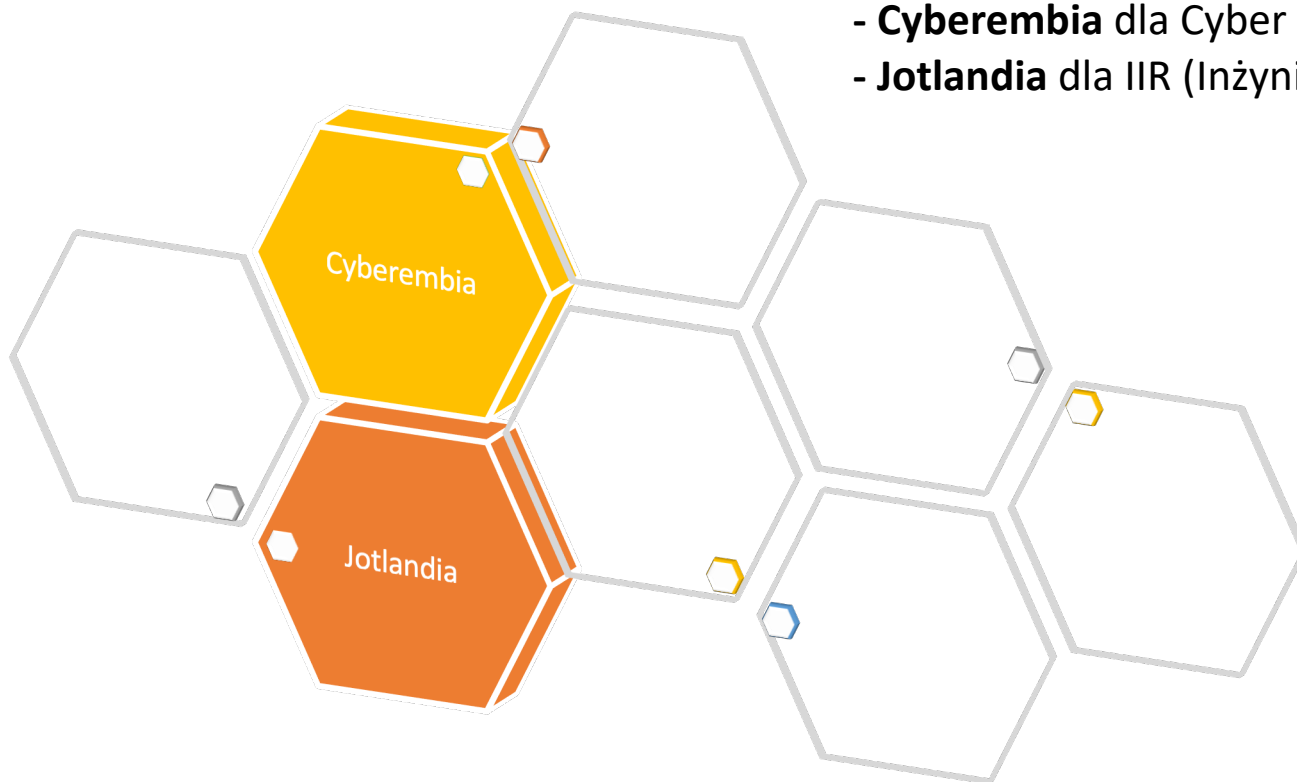
AI – Artificial Intelligence – Sztuczna inteligencja



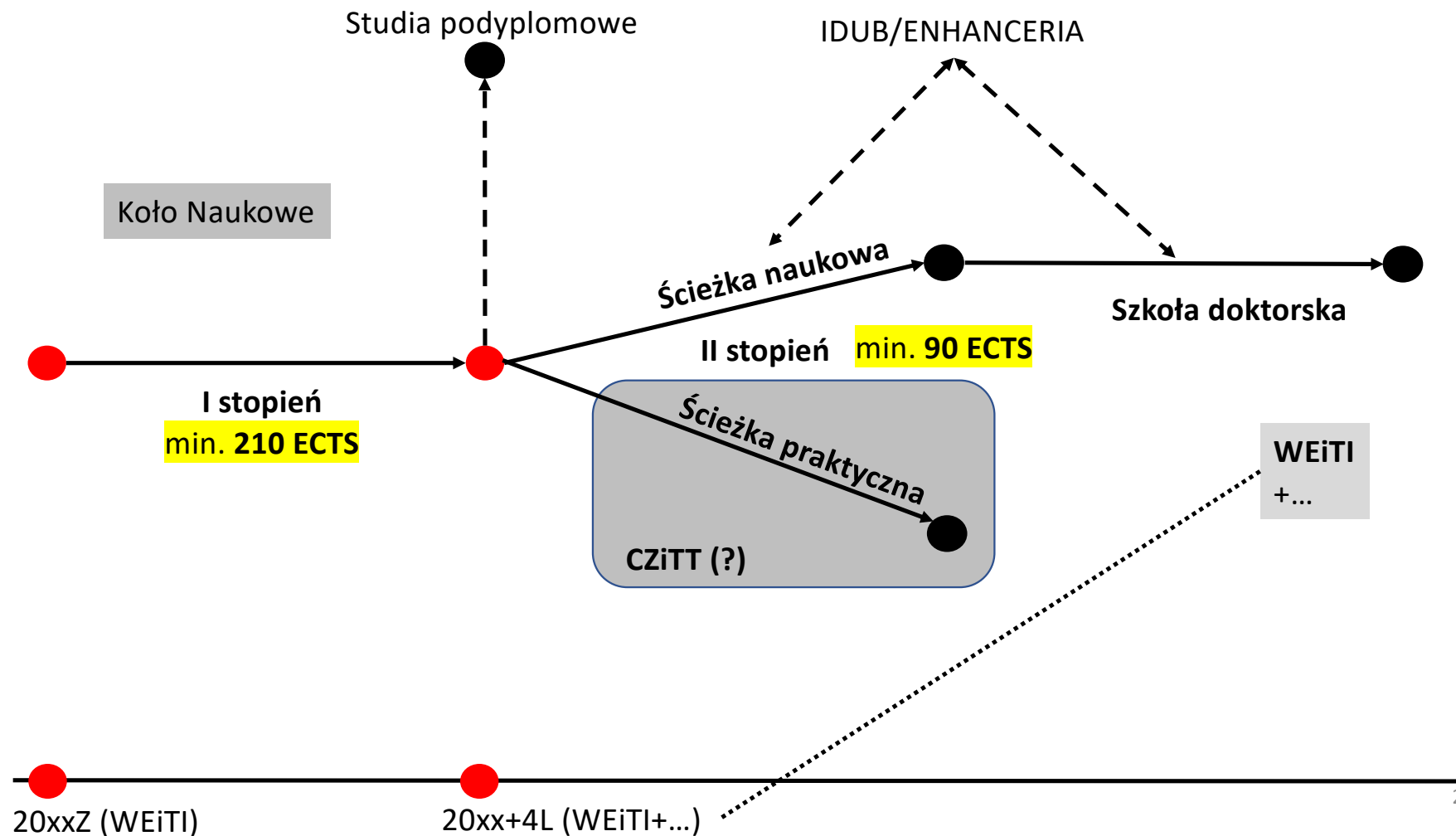
Ekosystem kooperujących wysp

Dwa programy rozwoju talentów wśród studentów:

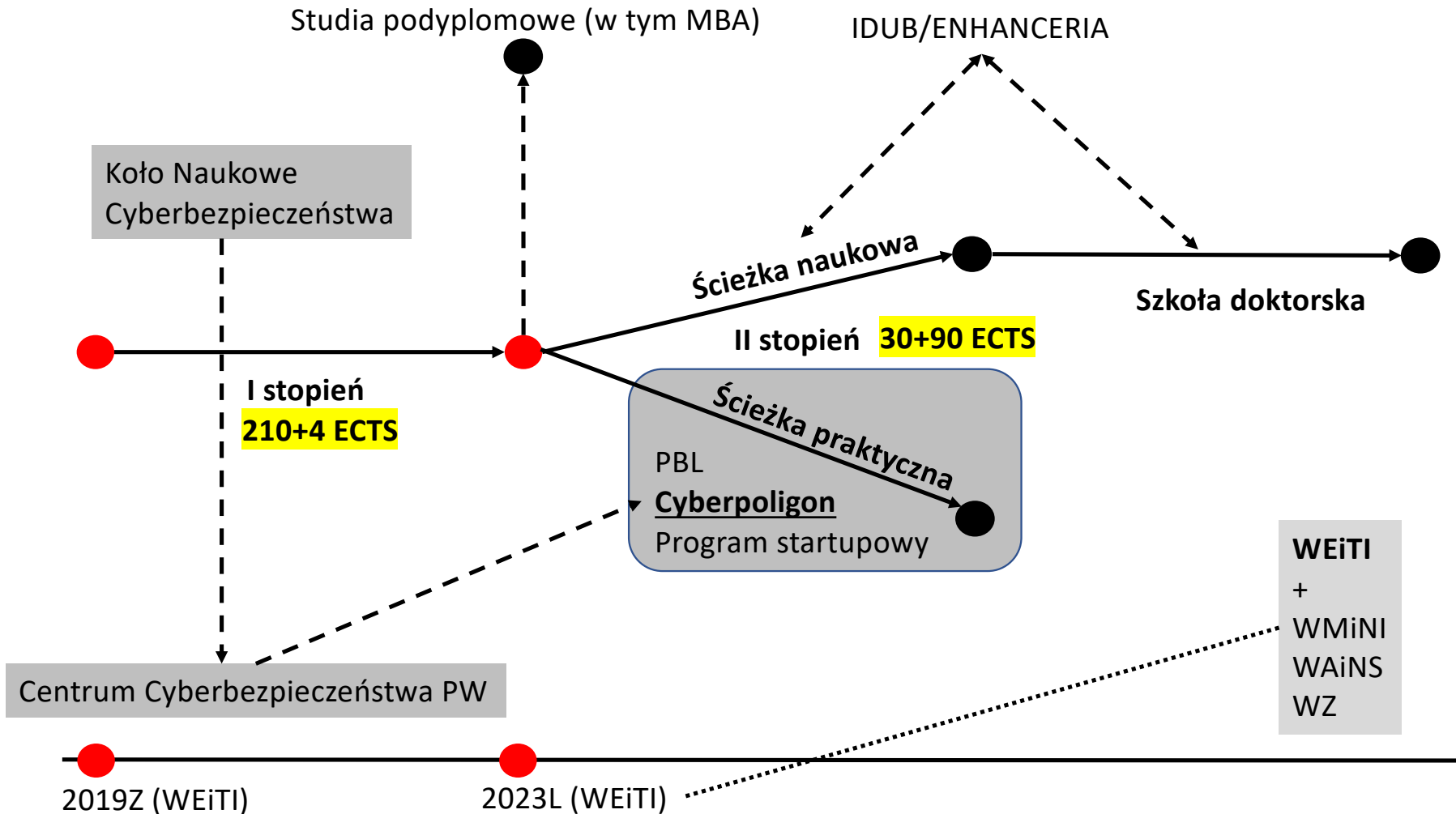
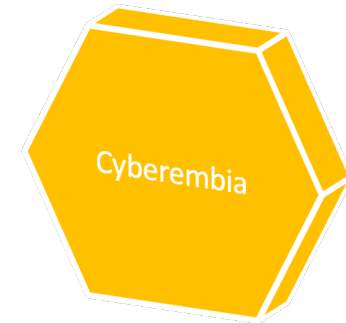
- **Cyberembia** dla Cyber
- **Jotlandia** dla IIR (Inżynieria Internetu Rzeczy)



Generyczny model programu rozwoju talentów wśród studentów (na przykładzie WEiTI)



Cyberembia: program rozwoju talentów wśród studentów Cyber



Cyberembia to rajska wyspa na Oceanie Spokojnym. Mieszka na niej plemię walecznych **Cyberosławów** – dzielnych studentów cyberbezpieczeństwa z PW.

Ich przywódczyni to **Cyberosława Śmiała** zrodzona w otchłani cyberprzestrzeni, aby chronić świat przed okrutnymi cyberprzestępcami.

Głównym miastem wyspy jest **CyberTown**.

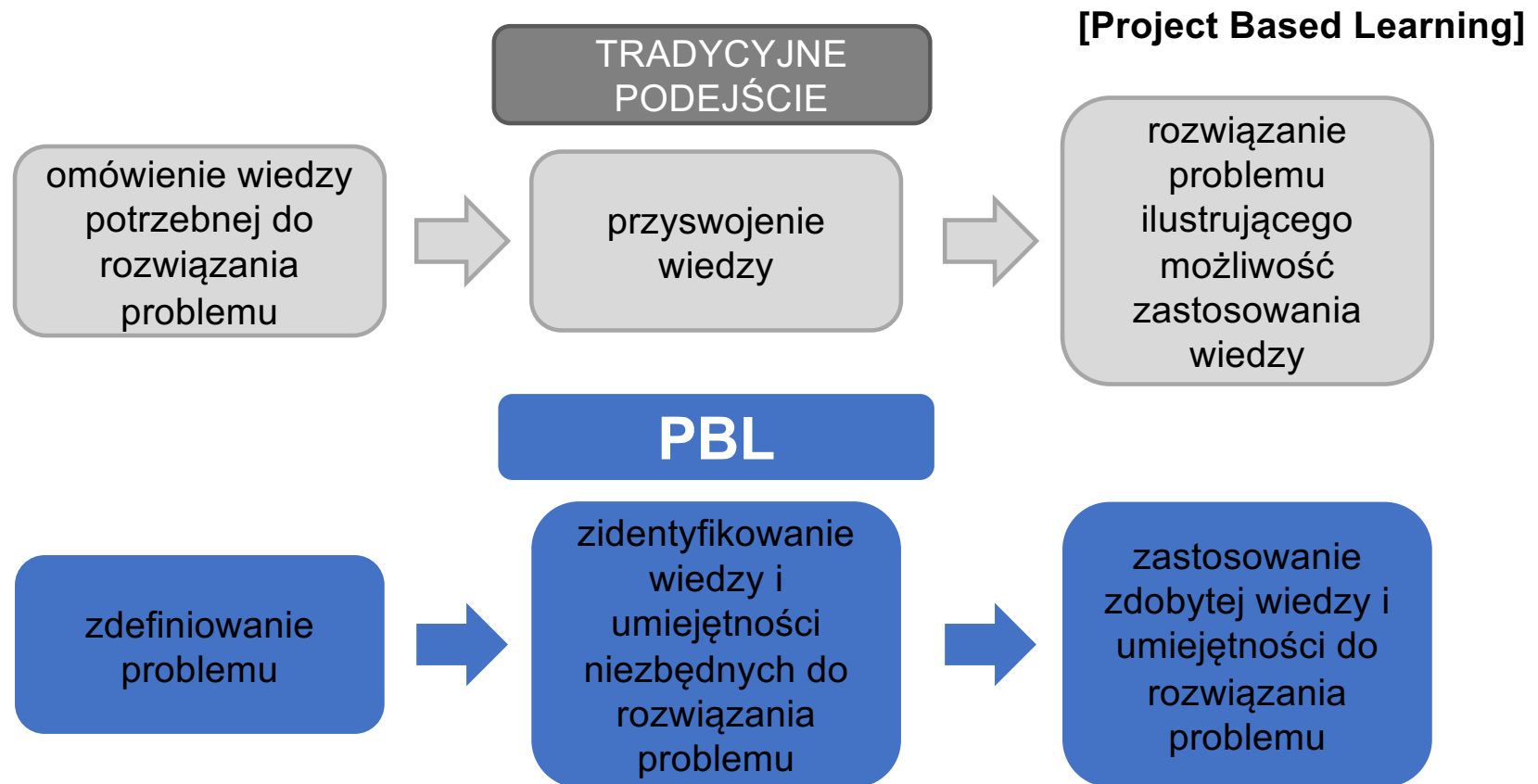
Klasyczne podejście vs. Cyberpoligon

- Tradycyjne szkolenia z technik hackingu i cyberprzestępczości
- Grywalizacja: szkolenia „niepoważne” i „poważne”
- Interaktywne filmy fabularne
- Symulacje ataków np. phishingowych

Wirtualne środowisko symulacyjne, które pozwala uczestnikom rozwinąć, udoskonalić i przetestować umiejętności potrzebne do odpierania prawdziwych cyberataków, w możliwie najbardziej realistycznych warunkach

- system do symulowania sieci
- samomodyfikujące się scenariusze cyberataku podatne na zmiany wprowadzane przez użytkownika
- generatory ruchu sieciowego

Tradycyjny model kształcenia vs. PBL



Program startupowy

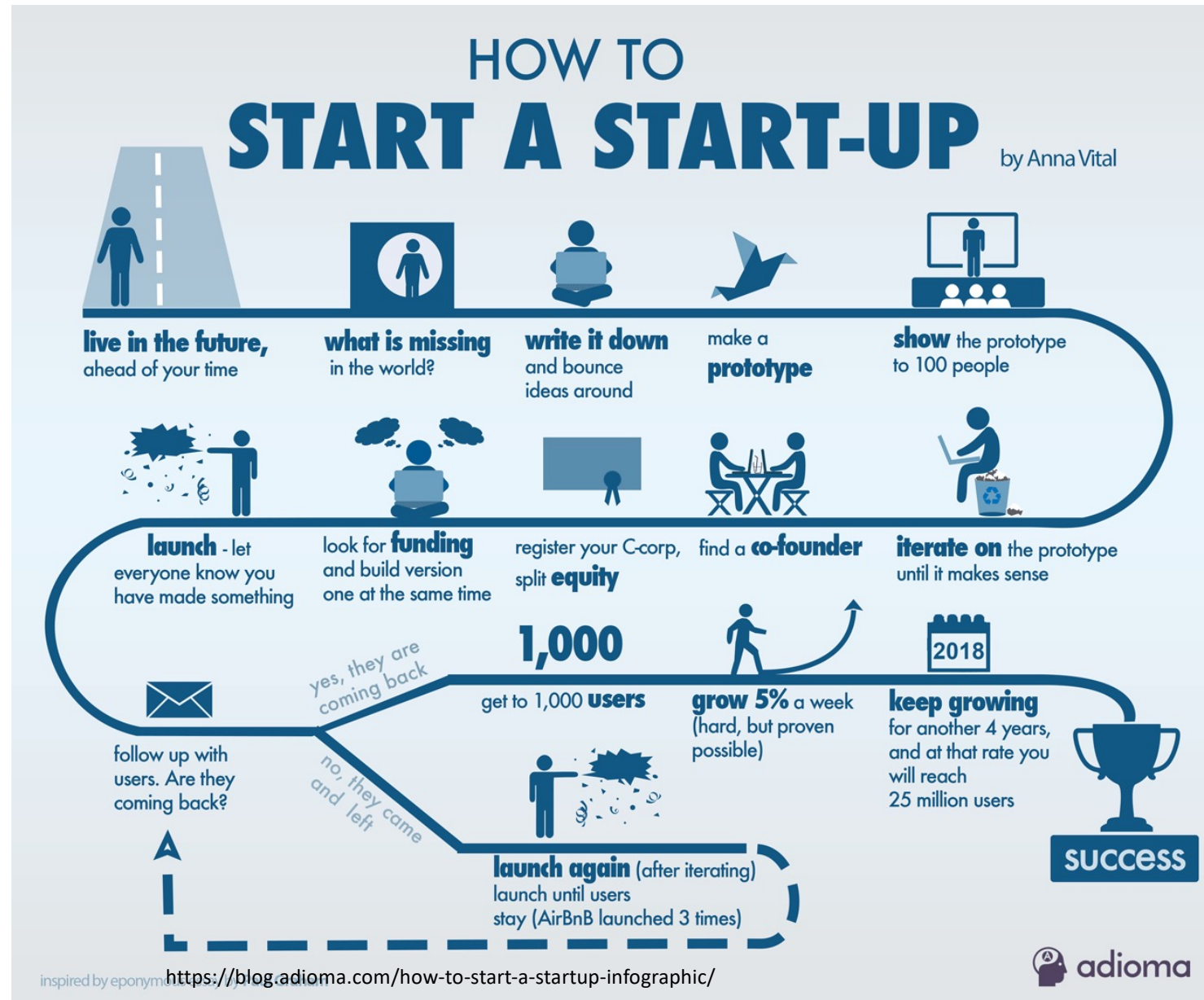
• Wartości

- pasja
- wytrwałość
- współpraca
- odpowiedzialność
- otwartość
- optymizm

• Umiejętności

- analiza rynku i potrzeb klientów
- auto-prezentacja
- budżetowanie
- podejmowanie ryzyka
- przeżywanie/akceptacja porażek, ale i sukcesów

• Efekt: wszechstronny rozwój



Cyber II°

Wersja: 6.12.2021

30+90 ECTS

ECTS	I	II	III	IV		
1	<p>Przedmioty Podstawowe</p> <p>grupa przedmiotów ze studiów I stopnia na kierunku Cyberbezpieczeństwo. Grupa przedmiotów nieobowiązkowa dla absolwentów WEiTI. Grupa przedmiotów obowiązkowa (30 ECTS lub mniej) dla innych kandydatów - nie WEiTI. Przedmioty dobrane tak, żeby większość była do zrobienia w ramach jednego semestru (max. 2).</p>	<p>PBL pierwszy (Analiza danych w cyber)</p>	<p>PBL drugi (bezpieczeństwo Internetu Rzeczy)</p>	<p>Ścieżka Cyber 4 ECTS: pozatechniczne aspekty</p>		
2				<p>Agentowe i aktorowe systemy decyzyjne</p>	<p>Przedmioty obieralne</p>	
3		<p>Techniki i technologie BigData</p>				<p>Seminarium</p>
4						<p>Ścieżka Cyber 5 ECTS: bezpieczeństwo hardware</p>
5		<p>Przedmioty obieralne</p>	<p>(PPMGR) - wstęp do prowadzenia badań naukowych</p>	<p>Przedmioty obieralne</p>	<p>PBL trzeci (PDYM): praca dyplomowa (20 ECTS)</p>	
6						<p>Lektorat B2+ (o nauce po ang.)</p>
7				<p>(PDMGR) - prowadzenie badań naukowych, wstęp do pracy dyplomowej</p>		
8						<p>Matematyka, 60 godzin (4 ECTS)</p>
9						
10						<p>NES: Cyberprzestępczość</p>
11						
12						<p>EDYM (0 ECTS)</p>
13						
14						<p>EDYM (0 ECTS)</p>
15		<p>EDYM (0 ECTS)</p>				
16			<p>EDYM (0 ECTS)</p>			
17		<p>EDYM (0 ECTS)</p>				
18			<p>EDYM (0 ECTS)</p>			
19		<p>EDYM (0 ECTS)</p>				
20			<p>EDYM (0 ECTS)</p>			
21		<p>EDYM (0 ECTS)</p>				
22			<p>EDYM (0 ECTS)</p>			
23		<p>EDYM (0 ECTS)</p>				
24			<p>EDYM (0 ECTS)</p>			
25		<p>EDYM (0 ECTS)</p>				
26			<p>EDYM (0 ECTS)</p>			
27		<p>EDYM (0 ECTS)</p>				
28			<p>EDYM (0 ECTS)</p>			
29		<p>EDYM (0 ECTS)</p>				
30			<p>EDYM (0 ECTS)</p>			

Pozostałe kierunki i specjalności na PW powiązane z Cyber

- **Wydział Elektryczny**
kierunek **Informatyka Stosowana II°**: specjalność *Cyberbezpieczeństwo*
- **Wydział Elektroniki i Technik Informacyjnych**
kierunek **Telekomunikacja II°**: specjalność *Teleinformatyka i cyberbezpieczeństwo*
- **Wydział Matematyki i Nauk Informacyjnych**
kierunek **Matematyka II°**: specjalność *Matematyka w cyberbezpieczeństwie*
- **Wydział Zarządzania**
kierunek **Zarządzanie Bezpieczeństwem Infrastruktury Krytycznej I° i II°**

*Nie bój się wielkiego kroku –
nie pokonasz przepaści
dwoma małymi*



<https://www.shutterstock.com/pl/image-vector/silhouette-man-jumping-over-gap-between-1257687481>

David Lloyd George (1863–1945)
Premier Wielkiej Brytanii w latach 1916–1922

**Don't be afraid to take a big step if one is indicated.
You can't cross a chasm in two small jumps*

Cyberbezpieczeństwo na Politechnice Warszawskiej jako priorytetowy obszar badawczy i nowy kierunek studiów

Krzysztof Szczypiorski

Wydział Elektroniki i Technik Informatycznych PW