Konferencja

LEKSYKON CYBERBEZPIECZEŃSTWA

Warszawa, 31 lipca 2020 r., godz. 10.00-13.00

Platforma komunikacyjna PTI - MS Teams PTI

„Cyberbezpieczeństwo a cybernetyka – pułapki pojęciowe”

B. Szafrański, prof. WAT

Uwagi wstępne:

- **Cybernetyka**, to:
  1. Interdyscyplinarna nauka o sterowaniu rozumianym jako oddziaływanie mające przynieść określony cel, zmierzająca do zrozumienia funkcji, procesów, mechanizmów kontroli i komunikacji w systemach z przypływem informacji tworzącym pętle w relacjach przyczynowo–skutkowych.
  2. Nauka zajmująca się analizą analogii między zasadami działania organizmów żywych, układów społecznych i maszyn (układów elektronicznych) — co w potocznym rozumieniu kojarzone jest zwłaszcza z dopatrywaniem się podobieństw między człowiekiem a maszynami.
- Współcześnie cybernetyka w podstawowym ujęciu jest nauką o sterowaniu oraz związanym z tym przetwarzaniu i przekazywaniu informacji lub inaczej pisząc cybernetyka, to nauka o procesach sterowania oraz przekazywania i przekształcania informacji w systemach takich jak np. maszyna, organizm żywy, społeczeństwo.
- **Biorąc powyższe pod uwagę, aparat pojęciowy i badawczy cybernetyki może być pomocny nie tylko w opisywaniu ale także badaniu problemów cyberbezpieczeństwa, bowiem w obu dziedzinach centralne znaczenie ma informacja i ponadto w obu dziedzinach w szerokim zakresie korzysta się z analogii do zjawisk w świecie organizmów żywych.**

Uwagi wstępne:

- Prezentacja ma charakter inicjalny, przyczynkarski i tym samym nie aspiruje do kompleksowego przedstawienia pojęcia cyberbezpieczenstwa w naukach pozaprawnych.
- Celem prezentacji jest potwierdzenie potrzeby stworzenia leksykonu cyberbezpieczeństwa i zasygnalizowanie wątpliwości i wielu wątków, które z punktu widzenia informatyki i cybernetyki powinny mieć wpływ na jego zawartość, powinny być w nim uwzględnione.
- Przedstawiony w prezentacji materiał odnosi się do wspólnej dla wszystkich dziedzin nauki bazy pojęciowej dotyczącej cyberbezpieczeństwa. Wynika to z przekonania, że bez istnienia na „najwyższym” poziomie wspólnej bazy pojęciowej dla wszystkich dziedzin nauki opracowanie leksykonu okaże się porażką.
- Pierwszym istotnym problemem będzie uzgodnienie kryteriów doboru pojęć, które powinny należeć do tej wspólnej bazy pojęciowej.
- W prezentacji celowe nie będą przytaczane definicje zawarte w aktach prawnych, zwłaszcza w ustawie o Krajowym Systemie Cyberbezpieczeństwa.

Wg „Słownika języka polskiego” PWN:
Leksykon, to:
1. «słownik o charakterze encyklopedycznym»
2. «pierwotnie: uporządkowany zbiór objaśnionych wyrazów i terminów jednego języka, dotyczących określonej dziedziny»
3. «słownictwo, zwłaszcza jakiejś osoby lub grupy osób»

Jeśli ma być opracowany wspólnie przez specjalistów różnych dziedzin (co najmniej prawników, informatyków, zarządzających i np. cybernetyków), to musi odpowiadać zgodnie z założeniem przedstawionym na poprzednim slajdzie definicji nr 2.

Pytanie otwarte:
Czy leksykon ma być opracowaniem końcowym, czy etapem wstępnym do opracowania w przyszłości formalnej ontologii dla dziedziny cyberbezpieczeństwa. W sytuacji rosnącego znaczenia sztucznej inteligencji i uczenia maszynowego takie etapowe podejście jest w pełni uzasadnione.

- **Wśród specjalistów informatyki do dzisiaj istnieją opinie kwestionujące potrzebę wprowadzania do dziedziny bezpieczeństwa systemów informatycznych pojęć z przedrostkiem cyber, takich, jak cyberbezpieczeństwo, cyberprzestrzeń, cyberzagrożenie, cyberatak, cyberobrona, …,**

- **Uważają oni, że wprowadzenia cyberbezpieczeństwa nie wnosząc do dziedziny bezpieczeństwa systemów informatycznych nowych wartości, przyczynia się do pogłębienia chaosu pojęciowego, w tym prawnego (w starszych aktach prawnych nadal funkcjonują pojęcia sprzed ery cyberbezpieczeństwa).**

- **Opinia autora prezentacji:**
  - obecnie nie ma już odwrotu od pojęcia cyberbezpieczeństwo, bowiem zostało ono z sukcesem wprowadzone do obiegu publicznego ze względu na brak, we właściwym czasie, skutecznej odpowiedzi technicznej czy prawnej, w ramach dotychczas obowiązującego systemu pojęć, na dynamikę rosnącej nieufności wywołanej:
  -- koniecznością cywilizacyjną korzystania z sieci internet,
  -- powszechnością występowania w sieci wielorakich, coraz to nowych zagrożeń, o naturze niezrozumiałej dla znacznej liczby aktywnych członków społeczeństwa informatycznego (krótkie uzasadnienie na następnym slajdzie).

Wraz z rozwojem systemów informatycznych i internetu obserwujemy stały wzrost zagrożeń dla bezpieczeństwa informacyjnego. Z drugiej strony nowoczesne technologie teleinformatyczne rewolucjonizują nie tylko metody organizacji przedsiębiorstw i instytucji ale także wpływają na relacje między obywatelami, podmiotami gospodarczymi i publicznymi. Coraz więcej osób i organizacji staje się, z własnego wyboru lub z konieczności, aktywnymi uczestnikami społeczeństwa informacyjnego wiążąc te okoliczności z nieuchronnością procesów cywilizacyjnych.

- Zadania (usługi) publiczne muszą być realizowane przy bezwzględnym respektowaniu ograniczeń dostępu do informacji prawnie chronionych i jednocześnie nie można sztucznie zatrzymać tendencji do zwiększania otwartości i interoperacyjności systemów informacyjnych.

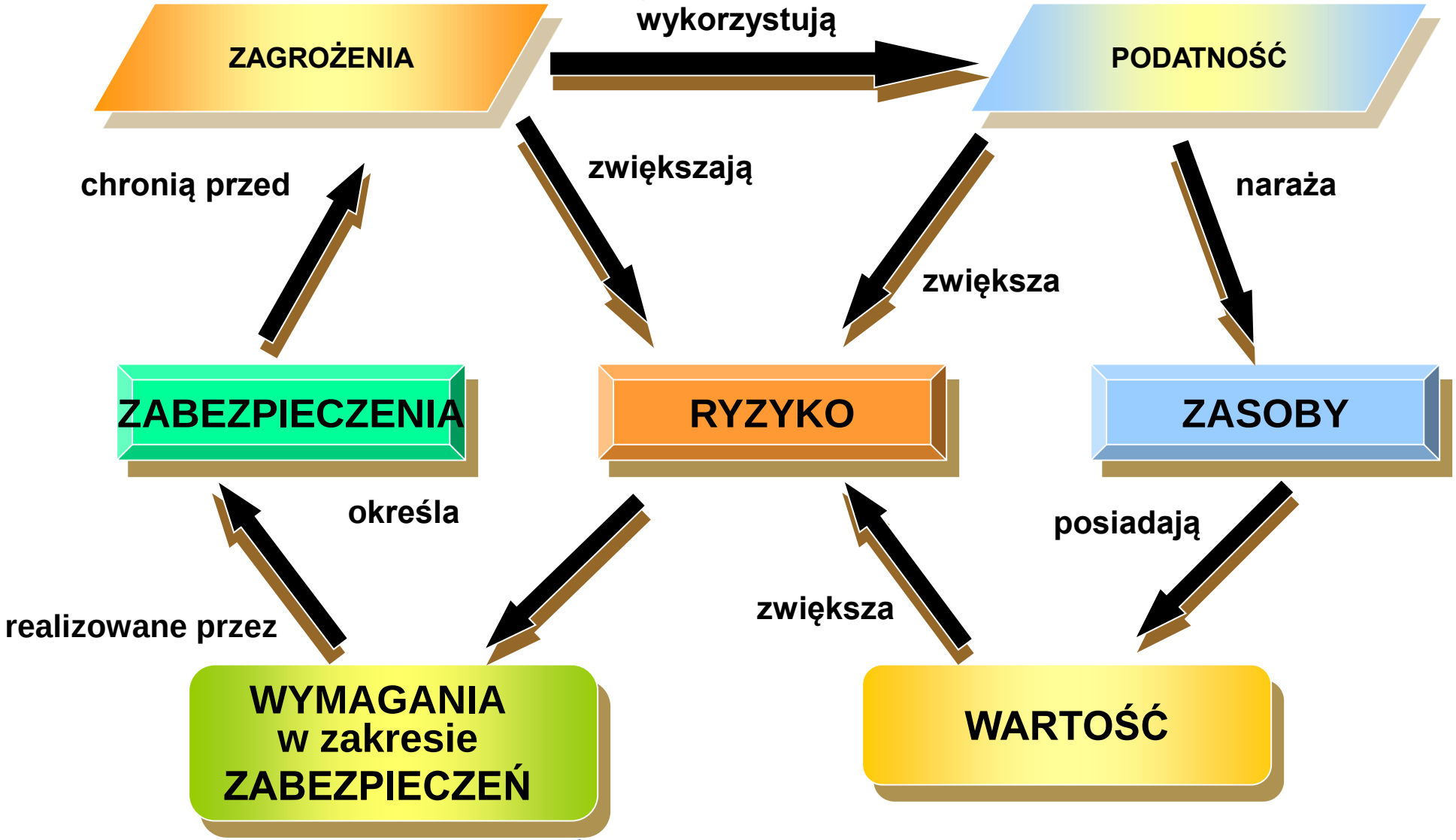
- Prowadzi to ustawicznie do powstawania sytuacji konfliktowych, w których zapewnienie poufności informacji zderza się z narastającą presją na zwiększanie otwartości systemów informatycznych stymulowanej potrzebami społeczeństwa informacyjnego.

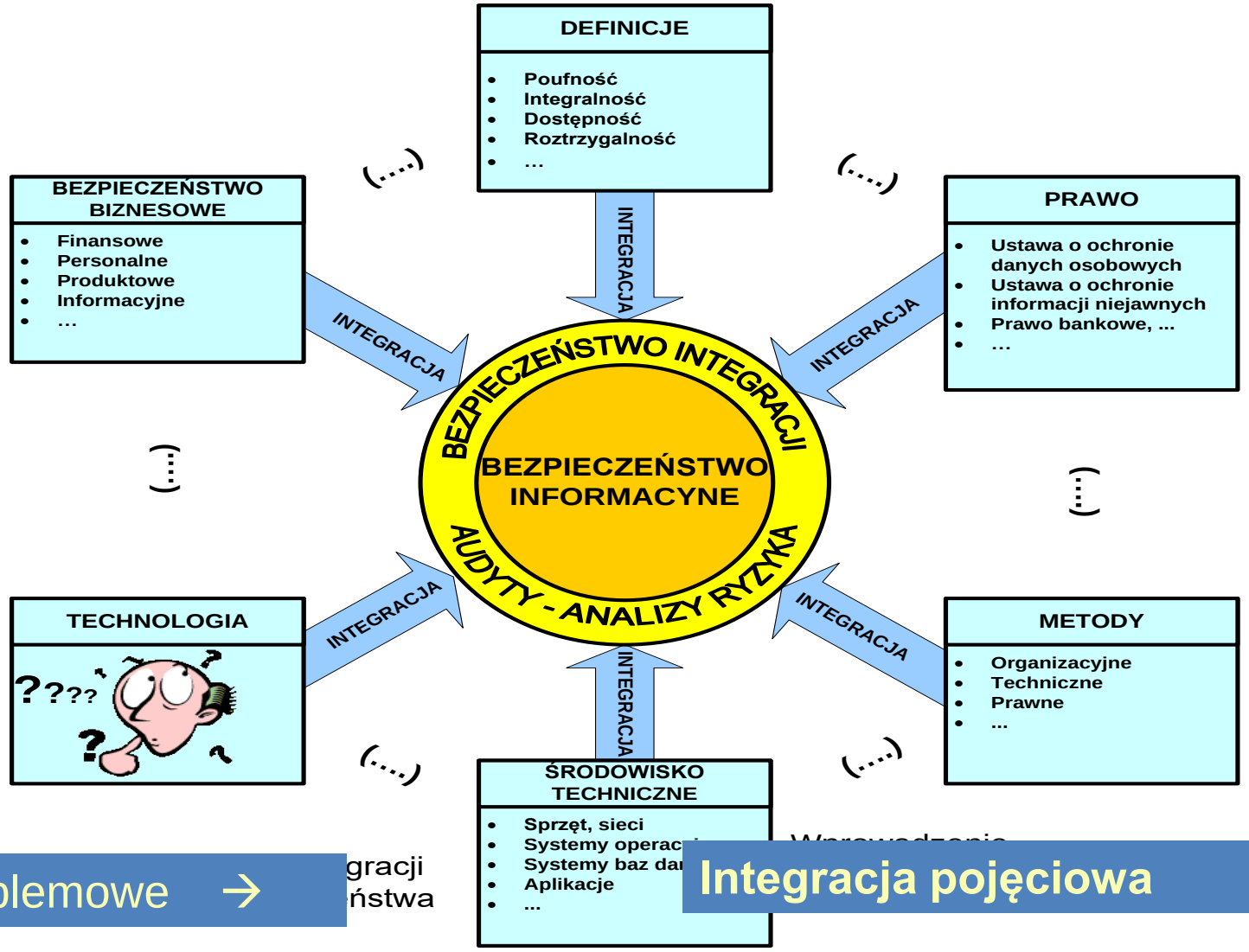
Wniosek: leksykon musi także uwzględnić pojęcia opisujące wyżej opisaną sytuację uczestników społeczeństwa informacyjnego

Na kolejnych dwóch slajdach przedstawiono (nr 8 i 9):

- slajd 8 - zestaw najważniejszych pojęć i zależności między nimi obowiązujących przed wprowadzeniem pojęcia cyberbezpieczeństwo. Wokół nich można zbudować zbiór pojęć istotnych z punktu widzenia informatyków. Ponadto mogą one stanowić dogodny punkt wyjścia do określenia kryteriów kwalifikacji pojęć do leksykonu, wspólnych dla informatyków i prawników.
- slajd 9 - przedstawia schematycznie złożoność zapewniania (cyber)bezpieczeństwa, które wymaga zastosowania narzędzi i środków z różnej natury dziedzin. Każda z dziedzin ma obecnie ukształtowane i zakorzenione w „mowie i piśmie" specyficzne słownictwo.

Wniosek: do momentu upowszechnienia się internetu słownictwo z dziedziny bezpieczeństwa było „ trzymane w ryzach"; obecnie wymknęło się ono spod kontroli, masowo upowszechnia słownictwo „żargonowe", anglicyzmy (zbędne lub co najmniej „niefortunne, bo nie poddające się regułom języka polskiego anglicyzmy, drastycznie zmalała lub zniknęła rola uczelni w kreowaniu nowych pojęć .


ZAGROŻENIA
wykorzystują
PODATNOŚĆ
chronią przed
zwiększają
zwiększa
naraża
ZABEZPIECZENIA
RYZYKO
ZASOBY
określa
posiadają
realizowane przez
zwiększa
WYMAGANIA
w zakresie
ZABEZPIECZEŃ
WARTOŚĆ



Obszary problemowe →

Integracja pojęciowa

Zakończenie: kilka propozycji

Proponuję:

- **określić kryteria kwalifikacji do leksykonu, rodzaje klasyfikacje pojęć, poziomy klasyfikacji, język opisu (bardziej prawny czy techniczny; dla kogo i po co leksykon?**
- **upowszechnić definicję informacji wykorzystującą pojęcie entropii, bo to chęć zmniejszenia entropii jest „motorem" zarówno legalnego, jak i najbardziej nas w tym przypadku interesującego nielegalnego, dostępu do zasobów informacyjnych,**
- **badanie problemu (cyber)bezpieczeństwa w większym stopniu skupić na bezpieczeństwu procesów informacyjnych (podejście dynamiczne) a nie bezpieczeństwu samych informacji (podejście statyczne), bowiem oddaje dynamikę zasilania w informacje niezbędne do realizacji procesów informacyjnych (decyzyjnych, badawczych, poznawczych, śledczych, dowódczych, edukacyjnych, diagnostycznych, itd.),**
- **nadać większe znaczenie pojęciu „bezpieczeństwo informacyjne w miejsce bezpieczeństwo informacji, krytycznie przeanalizować polskie regulacje prawne ze standardami lub normami komercyjnymi w celu ich uspójnienia lub odrzucenia dominacji regulacji komercyjnych nad prawnymi (audyty są często wykonywane na bazie standardów komercyjnych nie mających umocowania w polskim prawie),**
- **dogłębnie przeanalizować i być może na nowo określić relacje między (cyber)bezpieczeństwem i integralnością,**
- **uwzględnić dziedzinę dezinformacji,**
- **uwzględnić kwestie bezpieczeństwa i odpowiedzialności w kontekście sztucznej inteligencji.**