Młodzi
w Centrum LAB
Uniwersytet SWPS

Czy istnieje nauka o bezpieczeństwie komputerowym?

Co z tego wynika: dla Polski, Europy i teorii socjologicznej

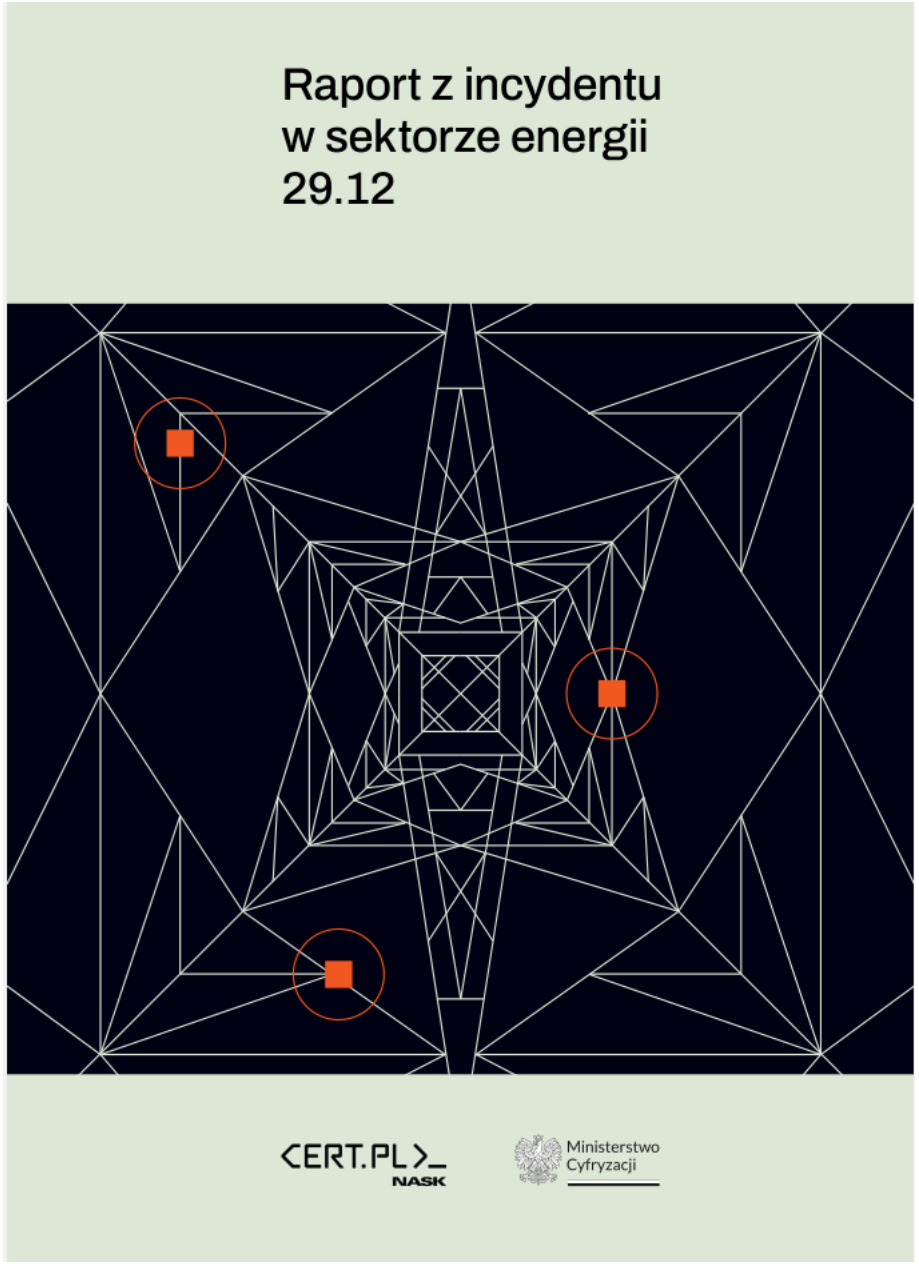
dr Marcin Zaród
mzarod@swps.edu.pl

O tym nie dyskutuję

- Bezpieczeństwo komputerowe to temat budzący emocje i kontrowersje.
- Będę pokazywał sposoby działania instytucji publicznych USA.
- Będę krytyczny wobec instytucji RP i UE.
- Dla jasności:
  - Federacja Rosyjska zaatakowała Ukrainę w 2014 roku.
  - Federacja Rosyjska stanowi w tej chwili największe zagrożenie zewnętrzne dla Rzeczypospolitej Polskiej.
  - Miejsce Polski jest w NATO i UE.

Plan

- Potrzeba
  - Atak na OZE, grudzień 2025. MITRE ATT@CK jako systematyka
- Nauka
  - Perspektywa socjologiczna: Praca i wytwór pracy
  - Trzy argumenty empiryczne
- Konsekwencje
  - Polska, Europa, socjologia



29 grudnia 2025

- Ataki:
  - Zespół PV+wiatraki
  - Duża elektrociepłownia
  - Przedsiębiorstwo produkcyjne
- Istotne:
  - ataki mające na celu wymazanie oprogramowania na sterownikach lokalnych („Wiper”)
  - brak zagrożenia w skali centralnej
  - wycieki danych
- Przebieg: z perspektywy instytucji:
  - Kontakt z dystrybutorem sterowników
  - Dobra współpraca z władzami lokalnymi
- Przyczyna: Błędy w instalacji

Przykład I: Systematyki

- MITRE ATT@CK ENTERPRISE:
  - Baza danych taktyk i technik ataków
  - Kurator: MITRE (za chwilę)
  - W ramach systematyki

MITRE ATT&CK Enterprise

Nazwa techniki	ID	Opis
UZYSKANIE POCZĄTKOWEGO DOSTĘPU		
External Remote Services	T1133	Wykorzystanie urządzeń brzegowych Fortinet do uzyskania dostępu do infrastruktury
Valid Accounts: Local Accounts	T1078.003	Logowanie na urządzenie Fortinet w przedsiębiorstwie sektora produkcyjnego
URUCHOMIENIE		
Scheduled Task/Job: Scheduled Task	T1053.005	Dystrybucja wipera w domenie z wykorzystaniem Scheduled Task
System Services: Service Execution	T1569.002	Wykonywanie poleceń za pomocą narzędzia PsExec
PERSYSTENCJA		
External Remote Services	T1133	Wykorzystanie Fortigate VPN do łączenia się z zaatakowanymi podmiotami
Valid Accounts: Local Accounts	T1078.003	Wykorzystanie lokalnych kont Fortigate VPN do łączenia się z zaatakowanymi podmiotami
Scheduled Task/Job	T1053	Utworzenie skryptów na urządzeniu Fortigate w celu kradzieży poświadczeń administratora oraz modyfikacji konfiguracji
ESKALACJA UPRAWNIEŃ		
Access Token Manipulation	T1134	Kradzież poświadczeń z usługi LSSAS Eskalacja uprawnień za pomocą tokenu procesu
Valid Accounts: Local Accounts	T1078.003	Wykorzystywanie konta posiadającego uprawnienia administratora na urządzeniu brzegowym
UNIKANIE WYKRYCIA		
Domain or Tenant Policy Modification: Group Policy Modification	T1484.001	Dystrybucja wipera w domenie poprzez modyfikację polityki GPO „Default Domain Policy"

Przykład zastosowania MITRE ATT@CK ENTERPRISE: Źródło: ibidem

Systematyki

- CVE: standard identyfikacji luk bezpieczeństwa komputerowego
  - Każda luka ma swój numer
  - Standard międzynarodowy (raczej zaufany w obszarze anglojęzycznym)
  - Analogia: ICD-11 dla chorób
  - Cel: pozwala ujednoznacznić

- Zgadywanie danych uwierzytelniających [T1110.001] lub ataki typu Brute force [T1110.003];
- Spearphishing ukierunkowany na uzyskanie danych uwierzytelniających [T1566];
- Spearphishing ukierunkowany na dostarczenie złośliwego oprogramowania [T1566];
- Podatność NTLM w oprogramowaniu Outlook (CVE-2023-23397);
- Podatności w oprogramowaniu Roundcube (CVE-2020-12641, CVE-2020-35730, CVE-2021-44026);
- Eksploitacja podłączonej do sieci Internet infrastruktury, w tym korporacyjnych usług VPN [T1133] poprzez znane publicznie podatności typu SQL Injection [T1190];
- Eksploitacja podatności w oprogramowaniu WinRar (CVE-2023-38831).

Przykład zastosowania CVE w komunikacji. SKW (2025). Działania rosyjskiej służby GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne.

https://www.gov.pl/web/baza-wiedzy/ostrzezenie-przed-dzialaniami-gru-w-cyberprzestrzeni-raport-sluzb-ujawnia-kampanie-wymierzona-w-firmy-logistyczne-i-technologiczne

Systematyki jako wspólny język

- Systematyki takie jak CVE i MITRE ATT@CK wytworzyły wspólny meta-język do definiowania i rozumienia cyberbezpieczeństwa:
  - Między zespołami bezpieczeństwa w firmach a zespołami w ramach instytucji publicznych
  - Między różnymi krajami
  - Między sektorem legalnym a nielegalnym
  - Między atakującymi (red team) a broniącymi (blue team)
  - Między różnymi skalami myślenia o infrastrukturze (architektura nowych produktów, utrzymanie, łączenie firm, poddostawcy usług)

Od wspólnego języka do nauki

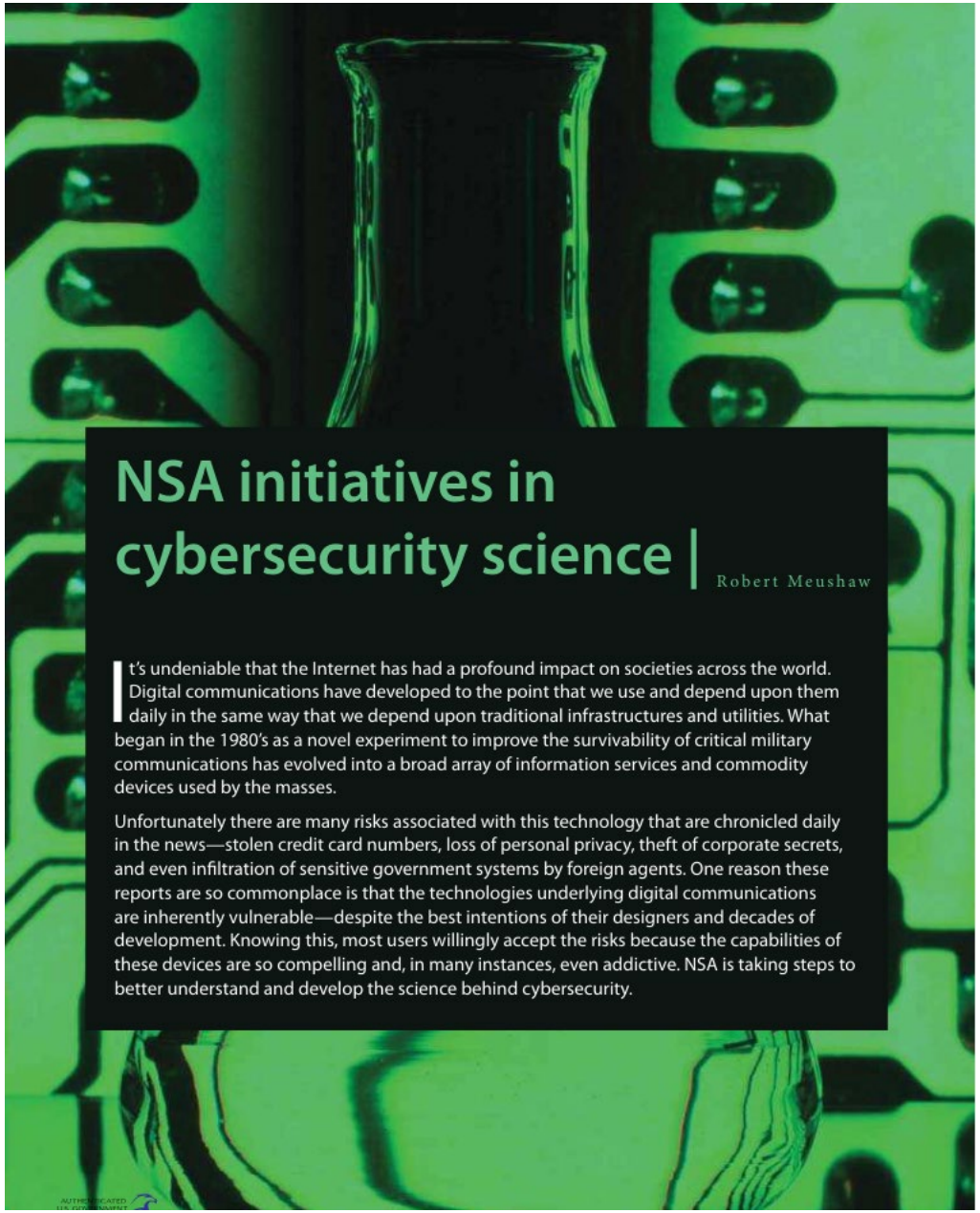
- Wspólna systematyka nie czyni jeszcze nauki („nauka to nie zbieranie znaczków”):
- Dlatego istotne było, że w oparciu o systematyki zaczęły powstawać:
  - Modele predykcyjne i automatyczne, jeszcze przed AI
  - Modele aktuarialne (wyceny ryzyk – np. ransomware)
  - Automatyczne wyszukiwanie luk i podatności analogicznych
  - Modele atrybucji ataku
  - Modele interwencji w trakcie incydentów
  - Pytania o uogólnienia węższej podklasy podatności na szerszą etc. -> analogicznie do twierdzeń matematycznych, modeli biologicznych etc.
  - Dyskuje i publikacje o nowych podejściach badawczych, nowych klasach abstrakcji itd.

Teza

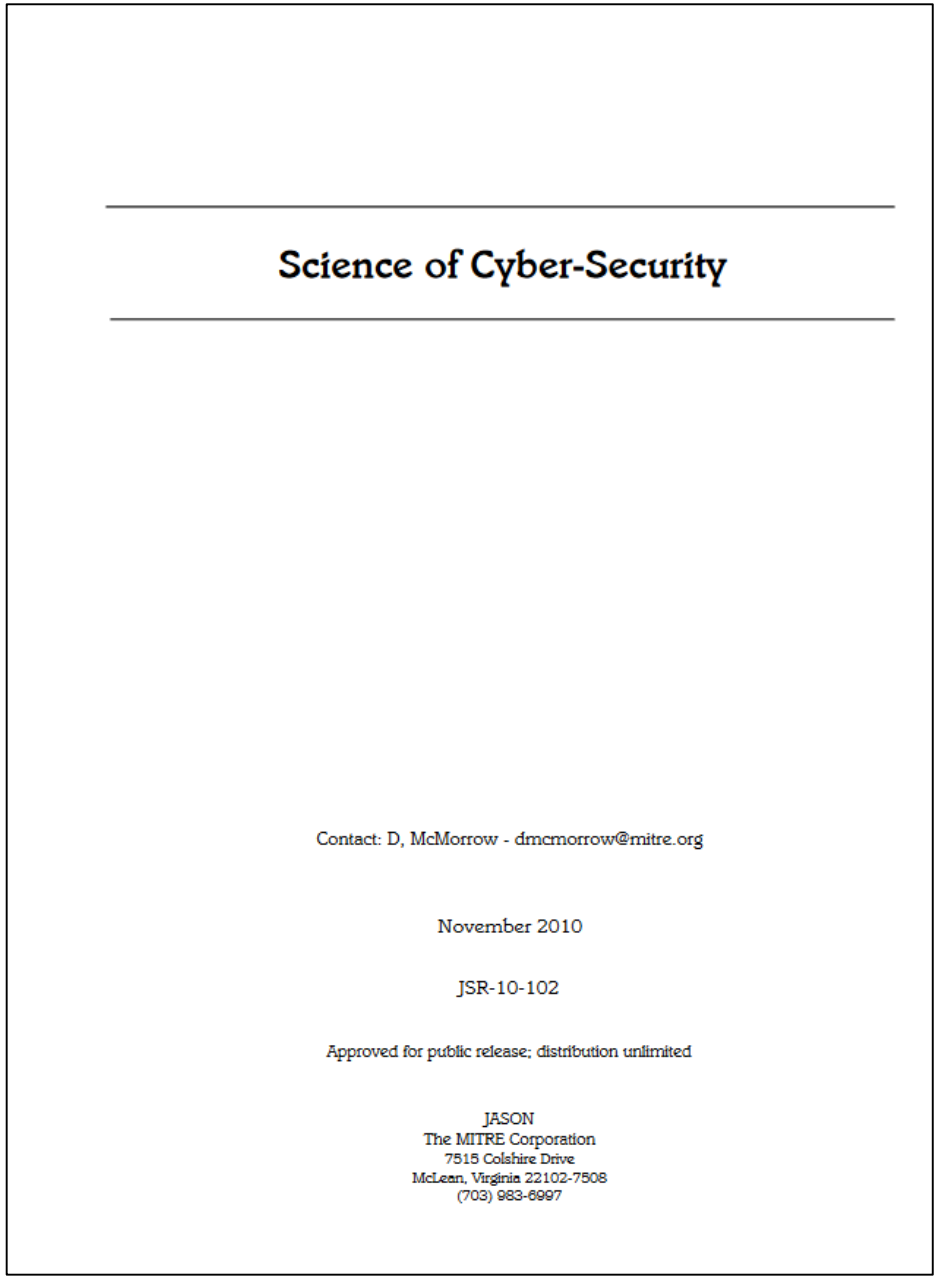
- W latach 2015-2025 bezpieczeństwo komputerowe przekształciło się w naukę
- Przekształcenie dokonało się równolegle poprzez procesy związane z pracą i tworzeniem standaryzacji w bezpieczeństwie komputerowym
  - W ramach anglojęzycznej sfery kapitalizmu cyfrowego
  - Przemiany nie miały charakteru spontanicznego
  - Przemiany nie były wyłącznie odpowiedziami np. na rozwój krytptowalut czy zapotrzebowanie na profesje związane z prywatnością post-RODO (Birnhack & Mundlak, 2025)
- Nie popełnijmy błędu:
  - Proces przekształcania się w naukę nie był neutralny politycznie
  - Proces przekształcania się nie zaszedł spontanicznie
  - Nie zaczął się dopiero w 2015

Co zmienia rozpoznanie bezp. komputerowego jako nauki?

- Mamy modele socjologiczne wypalenia zawodowego w nauce
  - Nowe dane porównawcze i źródła hipotez do modeli wypalenia zawodowego w cyberbezpieczeństwie!
  - Oczywiście to nie jest podobieństwo 1:1 (tak samo jak w ramach nauk są różnice a „unity of science is a useful theoretical fiction”)
- Mamy modele karier zawodowych, transferów zawodowych itd.
- Mamy modele laboratoriów
- Mamy pytania o wiedzę milczącą (tacit knowledge), czyli „to co bardzo trudno udokumentować” w oficjalnych systematykach. „niepisane sztuczki”, „ręce bogini labu” itd.
- Mamy jakieś koncepcje tego jak instytucje naukowe mają odpowiadać przed społeczeństwem i smutne lekcje historyczne z tego co się dzieje, gdy to jest zaniedbywane
- Mamy też pozytywne wzorce tego jak profesje naukowe pełnią rolę „czwartej władzy” w społeczeństwie
  - I dokładnie to samo już dzieje z cyberbezpieczeństwem! Nagle mamy do tego ramę prawną i socjologiczną!



Meushaw & Landwehr, 2012
(cryptic: NSA)



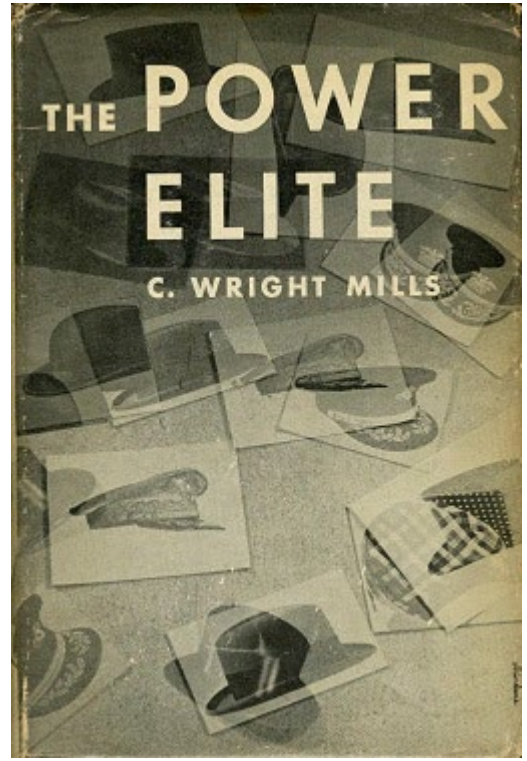
JASON 2010

Virginia czyli Bruksela à rebours

- Efekt Brukseli: rozprzestrzenie się sfery wpływów UE poza granice państw członkowskich dzięki regulacjom takim jak GDPR / RODO
  - (Bradford, 2012; Birnhack & Mundlak, 2025; Ylönen, 2025)
  - Logika: Jeśli chcesz robić interesy z UE / w ramach UE: dopasuj swoje standardy prywatności.
  - Efekt: Kanada, Szwajcaria, Argentyna i in. dopasowały swoje regulacje dot. prywatności danych do standardów UE

Virginia czyli Bruksela à rebours

- Instytucje, które są kuratorami systematyk w bezp. komputerowym to amerykańskie: MITRE (brak rozwinięcia), NIST (National Institute of Standards)
- MITRE pozostaje poza kontrolą parlamentarną (Not-For-Profit-Organization): otrzymuje fundusze federalne, realizuje zlecenia z wojska, ale nie jest instytucją federalną



Virginia czyli Bruksela à rebours

- Teza: Proces upowszechniania się systematyk takich jak CVE i MITRE ATT@CK określam jako „Virginia effect”.
  - Rozciąganie władzy USA poza zasięg geograficzny poprzez sprawowanie kontroli nad metrologiami cyberbezpieczeństwa
  - Wraz z upływem czasu standardy przyjmowane dobrowolnie petryfikują w formie infrastruktur
  - Virginia: siedziba MITRE i wywiadu komputerowego NSA

Zaród, M. (2025). *The Sociology of Cybersecurity: An Ethnography of a Science and the Profession* (1. wyd.). Routledge. https://doi.org/10.4324/4

Przykład II: Capture the Flag (CTF)

- Międzynarodowa sieć zawodów w łamanie zabezpieczeń komputerowych
- Zawody organizowane przez firmy, uczelnie, instytucje publiczne i grupy fanowskie
- Podstawowa logika: grupy rywalizują ze sobą rozwiązując problemy z bezp. komputerowego
  - Problemy są „sztuczne” (stworzone na potrzeby danych zawodów)
  - Ale narzędzia, mechanizmy i problemy „odkrywane” w każdym zadaniu są rzeczywiste
  - Analogia: zawody NATO w biathlonie w grudniu w Finlandii

CTF

- USA: Użycie CTF do uczenia systemów automatycznego hakowania na użytek wojska (najlepsi zawodnicy z całego świata byli zapraszani do gry przeciwko systemom komputerowym)
- USA, Polska: Drużyny akademickie, użycie jako edukacja pozaformalna
- Polska: użycie zadań CTF do rekrutacji do wojsk komputerowych
- Federacja Rosyjska (bez potwierdzenia): pomysł stworzenia systemu rozgrywek CTF na podobieństwo systemu kształcenia szachistów i ciężarowców w ZSRR (sponsoring jednego z oligarchów IT)
- Niemcy: finały na konferencji anarchistyczno-haktywistycznej (Chaos Communication Congress)

CTF: Polska, 2022-2025

- Przykład: ludzie z polskiej ekipy CTF zostali wynajęci do badania podejrzanego systemu w lokomotywach produkowanych przez firmę Newag (lokomotywy 31WE, 35WE, 36WEa, 37WE, 39WE, 45WE, 222M)

Za: https://dragonsector.pl/ (dla ścisłości: trzech badaczy bezpieczeństwa było nazwanych „Dragon Sector” raczej jako uproszczenie medialne. Zdaję sobie sprawę z tego, że drużyna CTF jest odrębnym bytem od ekipy realizującej badanie. Istotne z punktu widzenia socjologicznego są dwie rzeczy: 1) CTFy były rozpoznane jako źródło wiedzy eksperckiej, też w systemie sądowym, 2) Ikonografia CTFowa została atrybuowana przez media do opisu zespołu badawczego. Podaję logo ze względu na 2, choć zaznaczam,

CTF

- Co tu się dzieje?
  - Osoby z drużyny bardzo specyficznego e-sportu -> rozpoznawalność globalna w branży -> badanie cyberbezpieczeństwa -> briefing w Kancelarii Prezesa Rady Ministrów?
- Brak działań KPRM -> upublicznienie wniosków z badania na kongresie hakerskim (odpowiedzialność publiczna?) -> działania prokuratury i urzędów regulacyjnych
- Stawka: transport regionalny w kilku województwach w Polsce, zakres badań realizowanych w ramach serwisu pojazdów szynowych?

Materiały z badań własnych

Author:	What makes a good CTF task?
Participant A:	A CTF task is good when it brings something new. It is not repeating something that has been done many times. A good task should not be simply tedious or complicated in a way that requires many hours to parse. A good task is a playable one.
Participant B:	It is very easy to construct a hard CTF problem doing some huge and messed up binary file. Everybody will be reading millions of lines of code for 48 hours and will be none the wiser.
Participant C:	A good problem should be slightly beyond your current limits. It should also be slightly beyond expectations.
Participant D:	Bad problems require a lot of blind guessing or pure intuition. A good task leaves breadcrumbs and clues and characteristics akin to real-life slightly unsafe systems.

Fragment 3.2 Answers to a question "What makes a good CTF task?" Participants emphasised new knowledge, subversion of expectations and cerebral challenge. Randomness and tediousness are criticised. Observe also how participants emphasise the "good kind of broken system" from the bad one. This is akin to the expressions of epistemic aesthetics' recognition of mathematical proofs.

Zaród, M. (2025). *The Sociology of Cybersecurity: An Ethnography of a Science and the Profession* (1. wyd.). Routledge. https://doi.org/10.4324/

Wnioski z przykładu II

- CTFy: system międzynarodowy i międzyinstytucjonalny, który jest jednym z mechanizmów wyznaczania prestiżu w ramach profesji
- Zwycięzcy ważnych zawodów -> oferty pracy w ważnych zespołach
- Oprócz tego: mechanizm uzgadniania znaczeń, testowania narzędzi i uwspólniania rozumienia podatności niezależny i istniejący obok systematyk „formalnych”
- Oprócz tego: forma rekreacji umysłowej związanej z profesją, forma realizacji potrzeb poznawczych i rywalizacji bez konieczności utowarowiania
- CTFy są rozgrywane od 1996, ale od 2014 lawinowo wzrosła ich popularność, upowszechnienie oraz

Przykład III: Spectre i Meltdown

- W 2017 opublikowano serię artykułów, twitów i innych form komunikacji pokazujących, że mechanizm alokacji pamięci we współczesnych procesorach może być użyty do ataku
  - W ogromnym uproszczeniu: procesory dokonują uproszczeń w alokacji pamięci co do kolejnych poleceń, co pozwala im szybciej kolejkować polecenia.
  - Niestety w bardzo szczególnych warunkach, dla pewnych kombinacji zawartość jednych poleceń w kolejce może „przeciekać” do innych

https://meltdownattack.com/ (interp: MZ)

Przykład III: Spectre i Meltdown jako seria równoczesnych odkryć

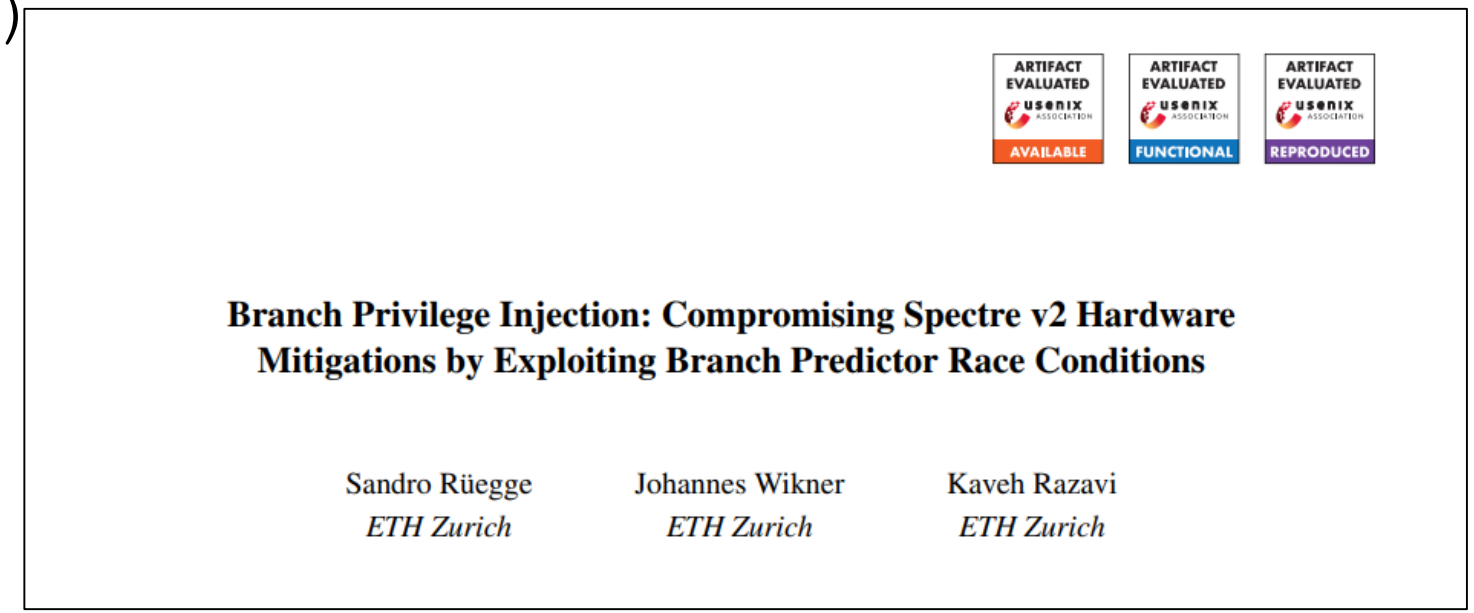
- Spectre:CVE-2017-5753 i CVE-2017-5715
  - Jann Horn (Google Project Zero),
  - Werner Haas, Thomas Prescher (Cyberus Technology),
  - Daniel Gruss, Moritz Lipp, Stefan Mangard, Michael Schwarz (Graz University of Technology)
- Meltdown: CVE-2017-5754
  - Jann Horn (Google Project Zero) and
  - Paul Kocher colab. Daniel Genkin (University of Pennsylvania and University of Maryland), Mike Hamburg (Rambus), Moritz Lipp (Graz University of Technology), Yuval Yarom (University of Adelaide and Data61)

Wnioski z przykładu III

- Po pierwsze (argument filozoficzny):
  - odkrycie luki Meltdown (prawdziwa dla specyficznej klasy instrukcji) doprowadziło do uogólnienia w postaci luki Spectre (ogólny mechanizm)
- Po drugie (argumenty socjologiczne):
  - To była seria odkryć.
    - Najpierw pokazane modele teoretyczne ataku w artykułach aż z 2003-2005. Wg. innych wersji nawet wcześniej
    - Potem wąska klasa ataku dla Meltdown (wyciek aplikacja na aplikację)
    - Potem uogólnienie (z systemu operacyjnego na aplikację)
    - Potem zrozumienie szerokiego mechanizmu (problemy operacji na całej szerokiej rodzinie procesorów, praktycznie całość procesorów we współczesnych komputerach osobistych)
    - Kolejne konsekwencje i sposoby dalszego rozwinięcia, aż do wersji v6 luki (2023)
  - Absolutnie różne instytucje: Google, lab akademicki, małe

Wnioski z przykładu III

- Historia luk Spectre i Meltdown pokazuje, że bezpieczeństwo komputerowe wykształciło cały kolektyw myślowy (Fleck) lub program badawczy (Lakatos)



https://sekurak.pl/nowe-luki-w-procesorach-intel-powrot-do-problemow-spectre-i-meltdown-w-nowej-odslonie/

Socjologia pracy naukowej w bezp. komputerowym

Struktury społeczne pracy naukowej

- Program badawczy / Kolektyw myślowy
- Heurystyki pozytywne („na tym polega dobre badanie w cyberbezpieczeństwie”) i Heurystyki negatywne („to nie jest warte badania”)
- CTF: Uspołeczniona forma uczenia się jak rozróżniać „zwykłe błędy” od ważnych i przełomowych anomalii
- Wymiar społeczny etyki („responsible disclosure”): jakie elementy można badać i co można publikować żeby mieścić się w granicach debaty

Produkty pracy społecznej w nauce

- Bezpieczeństwo komputerowe wytwarza osobną klasę produktów
  - W książce nazywam „stabilized instability”
- Produkt pracy w bezp. komputerowym może być komodyfikowany
  - W formie bug-bounty
  - W formie podatności (rynek „zero days”) i amunicji do cyberbroni: patrz afera Pegasusa
  - W formie oceny ryzyka infrastruktury komputerowej
  - Jako nowy impuls rynkowy (Schumpeter) tworzący podklasę infrastruktur i ich problemów

Moje argumenty

1. W latach 2015-2025 upowszechniły się narzędzia i systematyki
   - Narzędzia (Ghidra) i systematyki (CVE) doprowadziły do
     - powstania modeli predykcyjnych, systemów uczących się i tworzących hipotezy
     - powstania wiedzy teoretycznej związanej z przewidywaniem, atrybucją, zapobieganiem itd.
   - Wokół standardów, systematyk i narzędzi wytworzone zostały struktury społeczne pracy naukowej oraz mechanizmy utowarowiania
2. Obiegi formalne powiązane z systematykami i instytucjami rozwinęły się na równi z obiegami nieformalnymi: CTF jako przykład.
   - Formy CTF istniały przed 1996 (są pojedyncze głosy w zinach i historiach grup hakerskich etc.), ale nie na taką skalę
   - Po 2015: rozwój w skali świata, standaryzacja systemu oceniania i kategorii zadań
3. Meltdown -> Spectre: badania luk w bezpieczeństwie: programy wieloletnie, heterogeniczność (bezp. firmowe, akademia, konsulting)

Co z tego wynika dla Polski?

- Pegasus (2018), Dragon-Impuls (2022-2025):
  - Broń komputerowa i inżynieria odwrotna jako aktorzy poza zrozumieniem w sferze publicznej
  - Niestety, również poza zrozumieniem w debacie nauk społecznych
- Otwarte pytania
  - CERT jako służba cywilna?
  - Na ile potrzebujemy instytucji takich jak Citizen Lab (śledztwo ws. Pegasusa) jako instytucji społeczeństwa obywatelskiego?
  - W jaki sposób klasyfikować badania, takie jak badania pociągów Impuls-Newag?
  - Niedofinansowane instytucje publiczne (ochrona zdrowia, edukacja, polityka społeczna) a lobbing?
- Osobny i otwarty problem: jak zorganizować monitoring infrastruktury subkrytycznej w skali regionalnej (takiej jak farmy OZE): gdzie trudno zestandaryzować procedury certyfikacji oraz prognozować scenariusze zagrożeń

Otwarty pomysł

- Infrastruktura subkrytyczna: taka, której zagrożenie niekoniecznie spowoduje wydarzenie medialne w skali kraju, reakcję rządu oraz odpowiedź międzynarodową
  - Za to będzie drenujące i wyczerpujące dla władz regionalnych
  - Poziom krytyczny: nie tylko jako skutek technologiczny, ale jako kryterium odpowiedzi i zainteresowania

Co z tego wynika dla Europy lub Unii Europejskiej?

- Interoperacyjność systemów informatycznych wytwarza nowe profile zagrożeń(zesp. Rocco Bellanova)
  - Hipoteza: interoperacyjność wytwarza p podatności nie tylko na styku państw członkowskich UE, krajowych systemów informatycznych i powiązanych z tym suwerenności, ale również w perspektywach regionalnych
  - Patrz studium przypadku ze strony: https://cert.pl/posts/2024/05/rekomendacje-ot/

Co z tego wynika dla UE?

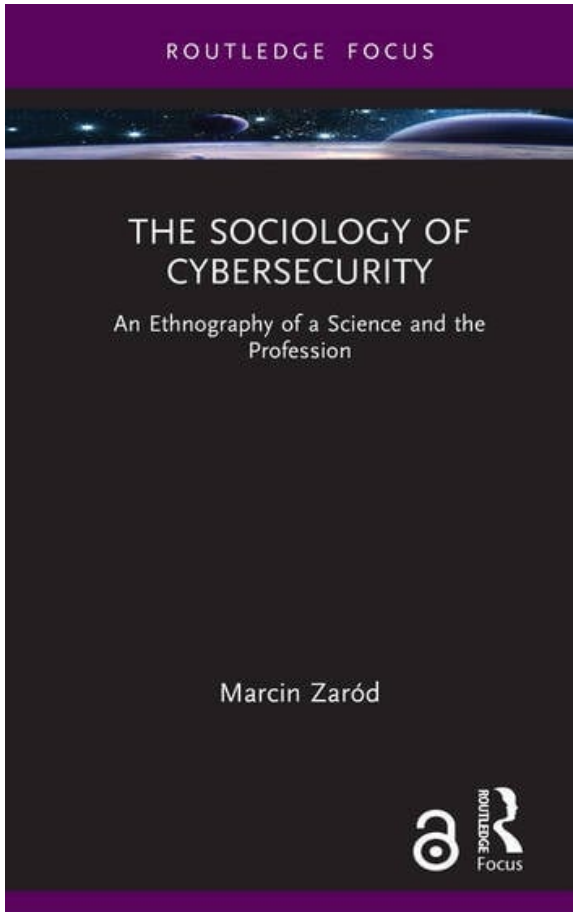
- Suwerenność cyfrowa musi dotyczyć nie tylko platform, regulacji i instytucji powiązanych z bezp. komputerowym
  - Suwerenność cyfrowa i procedury współpracy w skali kontynentu muszą dotyczyć również systematyk
  - Nowa odsłona suwerenności metrologicznej (W. Kula, A.W. Nowak).
    - Tym razem problem: bo mierzone i definiowane są obiekty z materialnością cyfrową (bity nadal wymagają socjomaterialności, to nadal są porty, obliczenia, procesory, ludzie, decyzje, instytucje).

Co z tego wynika dla teorii socjologicznej?

- Nowe spojrzenia na stare problemy badawcze:
  - Jaka wizja przyszłości i ekonomii stoi za projektem Google Zero (projekt: likwidacja wszystkich luk w bezpieczeństwie komputerowym)
  - Jakie rodzaje ryzyk są otwierane w momencie gdy luki w bezpieczeństwie są zamykane?
- Nowe problemy:
  - W jaki sposób rozumienie pracy naukowej w bezpieczeństwie wpływa na rozumienie przemian pracy w społeczeństwach w ogóle?
- Bezpieczeństwo komputerowe jako mechanizm walki i konsolidacji w technofeudalizmie?

Źródła

- Birnhack, M. D., & Mundlak, G. (2025). The Brussels effect(s) and the rise of a privacy profession. *International Data Privacy Law*, ipaf005. https://doi.org/10.1093/idpl/ipaf005
- CERT Polska. (2026). *Raport z incydentu w sektorze energii 29.12.2025*.
- Farrand, B., & Carrapico, H. (2018). Blurring Public and Private: Cybersecurity in the Age of Regulatory Capitalism. W O. Bures & H. Carrapico (Red.), *Security Privatization: How Non-security-related Private Businesses Shape Security Governance* (s. 197–217). Springer International Publishing. https://doi.org/10.1007/978-3-319-63010-6_9
- JASON. (2010). *Science of cyber-security*. JASON Office MITRE, McLean, VA.
- Kowalczyk, M., q3k, & Stepniewicz, J. (2025, grudzień 27). *We've not been trained for this: Life after the Newag DRM disclosure*. 38C3, Hamburg. https://media.ccc.de/v/38c3-we-ve-not-been-trained-for-this-life-after-the-newag-drm-disclosure
- Meushaw, R., & Landwehr, C. E. (2012). NSA initiatives in cybersecurity science. *The Next Wave, Vol. 19, No. 4, 2012, The Next Wave*, *19*(4). https://www.govinfo.gov/app/details/GPO-TNW-19-4-2012/GPO-TNW-19-4-2012-4
- Q3K. (2024). *"Software installed by hackers"- how the Polish Press Agency lies about the Newag scandal*. https://q3k.org/2024-06-11-pap-newag-en.html
- Redford, q3k, & MrTick. (2023). *Breaking „DRM" in Polish trains*. 37C3, Hamburg. https://media.ccc.de/v/37c3-12142-breaking_drm_in_polish_trains
- SKW. (2025). *Działania rosyjskiej służby GRU wymierzone w zachodnie podmioty logistyczne oraz przedsiębiorstwa technologiczne*. Służba Kontrwywiadu Wojskowego. https://go.recordedfuture.com/hubfs/reports/CTA-RU-2024-0530.pdf
- Spring, J. M., & Illari, P. (2019). Building General Knowledge of Mechanisms in Information Security. *Philosophy & Technology*, *32*(4), 627–659. https://doi.org/10.1007/s13347-018-0329-z
- Strom, B. E., Applebaum, A., Miller, D. P., Nickles, K. P., Pennington, A. G., & Thomas, C. B. (2018). *MITRE ATT&CK: Design and Philosophy* (10AOH08A-JC). MITRE. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
- Ylönen, M. (2025). Reconceptualising the Brussels Effect. *JCMS: Journal of Common Market Studies*. https://doi.org/10.1111/jcms.13731
- Zaród, M. (2025). *The Sociology of Cybersecurity: An Ethnography of a Science and the Profession* (1. wyd.). Routledge. https://doi.org/10.4324/9781003396871
- Zaród, M. (2018). *Aktorzy-sieci w kolektywach hakerskich*. https://depotuw.ceon.pl/handle/item/2909



Zapraszam do lektury i do kontaktu

https://www.routledge.com/The-Sociology-of-Cybersecurity-An-Ethnography-of-a-Science-and-the-Profession/Zarod/p/book/97

- mzarod@swps.edu.pl