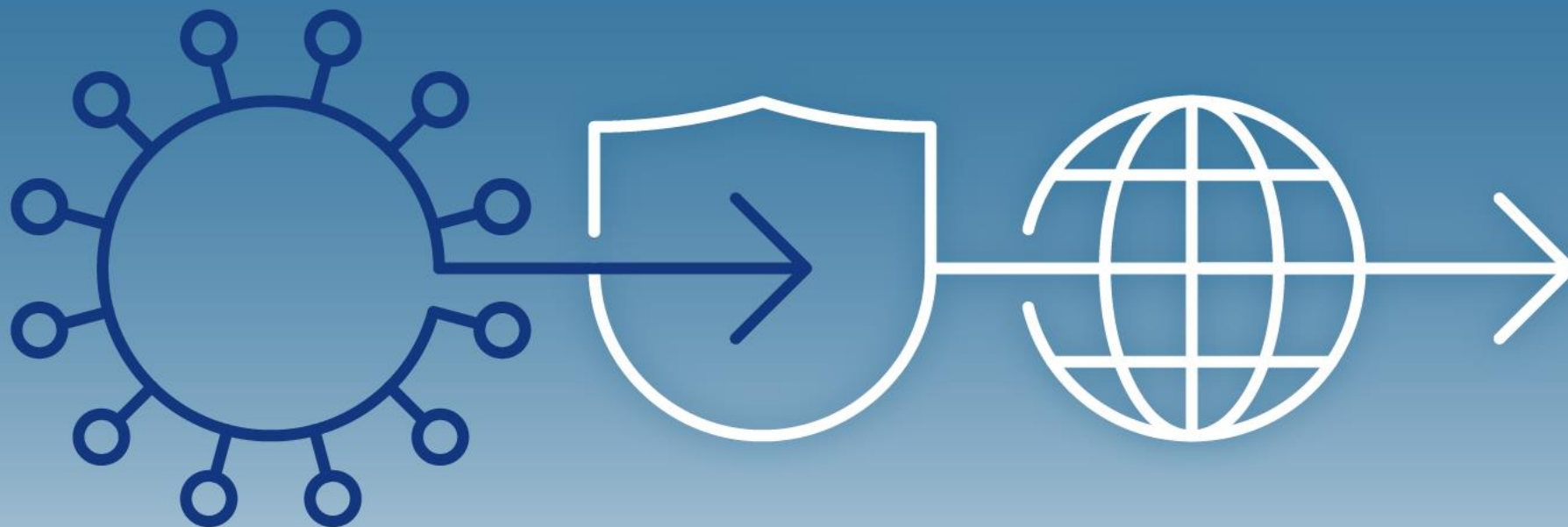


# Konferencja Naukowa Bezpieczeństwo w Internecie – Cyberpandemia

22-23 października 2020 r.



Sektorowa Rada  
ds. Kompetencji  
Telekomunikacja  
i Cyberbezpieczeństwo



UNIwersytet Kardynała  
Stefana Wyszyńskiego  
w Warszawie



POLSKIE TOWARZYSTWO INFORMATYCZNE



Naukowe Centrum  
Prawno-informatyczne

# Handel narkotykami w cyberprzestrzeni

dr Krzysztof Jan Jakubski

Morskie Centrum Cyberbezpieczeństwa – Wydział Dowodzenia i Operacji Morskich AMW Gdynia

Collegium Civitas Warszawa



Sektorowa Rada  
ds. Kompetencji  
Telekomunikacja  
i Cyberbezpieczeństwo



UNIWERSYTET KARDYNAŁA  
STEFANA WYSZYŃSKIEGO  
W WARSZAWIE



POLSKIE TOWARZYSTWO INFORMATYCZNE

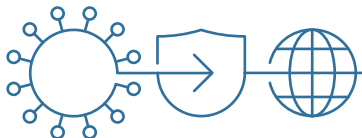


Naukowe Centrum  
Prawno-informatyczne



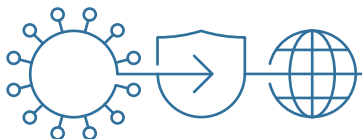
*Pociąg ludzi do zła ujawnia się zwłaszcza  
tam,  
gdzie pojawia się nowa technologia*  
[Stanisław Lem]

*Z technologiami jak z bronią atomową.  
Może zabijać i ratować*  
[Anna Streżyńska]



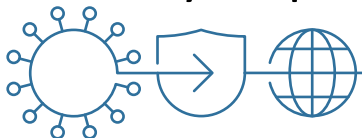
# Cyberprzestępczość – zjawisko stare czy nowe?

- Nadużycia popełniane przez użytkowników systemów informatycznych były, aż do końca lat 80. XX w., bagatelizowane, a dekadę wcześniej wręcz negowano szkodliwość i znaczenie tych czynów.
- Przestępczość komputerowa ewoluuje. Wirusy komputerowe, których celem było dokonywanie drobnych aktów komputerowego wandalizmu oraz przysporzenie rozgłosu ich twórcom zastąpił wyrafinowany malware, mający na celu paraliżowanie działania systemów określonych organizacji, instytucji i przedsiębiorstw oraz pozyskiwanie informacji chronionych. W głębokiej sieci przestępczość wszelkiego rodzaju kwitnie, a serwisy takie jak Silk Road i jego kolejne klony, czy polskie ToRepublic czy Hydra tworzyły wyśmienite warunki do rozwijania karier przestępczych.
- Dziś w cyberświecie znajdziemy praktycznie wszystkie odmiany przestępczości.



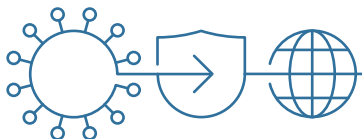
# Narkotyki w cyberprzestrzeni są od zawsze

- John Markoff w książce *What the Dormouse Said: How the Sixties Counterculture Shaped the Personal Computer Industry* napisał, że pierwszą na świecie transakcją online była transakcja narkotykowa, bowiem „w 1971 lub 1972 r. studenci Stanford korzystający z kont Arpanet w Laboratorium Sztucznej Inteligencji Uniwersytetu Stanford przeprowadzili transakcję handlową ze swoimi odpowiednikami w Massachusetts Institute of Technology. Przed Amazonem, przed eBayem, przełomowym aktem handlu elektronicznego była umowa narkotykowa. Studenci skorzystali z sieci, aby po cichu zorganizować sprzedaż nieokreślonej ilości marihuany”
- Ujawnione w 1989 r. przez astronoma z Lawrence Berkeley National Laboratory – Clifforda Stolla, powiązania niemieckiej grupy hackerskiej Chaos Computer Club z Hamburga z radzieckim KGB i wykradanie z amerykańskich sieci rządowych szeregu informacji, w tym m.in. dotyczących projektu promu kosmicznego, za które KGB płacił nie tylko pieniędzmi, ale także heroiną.



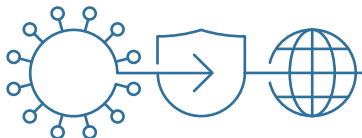
# Narkotyki w cyberprzestrzeni są od zawsze

- W przestrzeni publicznej od momentu powstania Internetu tworzone wiele witryn handlowych oferujących asortyment zakazany w legalnej przestrzeni. Były to zarówno strony typu warez, czyli oferujące pirackie oprogramowanie lub programy służące do przełamania technicznych zabezpieczeń głównie oprogramowania, gier komputerowych, rzadziej sprzętu komputerowego, ale też przykładowo strony zawierające fałszywe karty płatnicze, dokumenty tożsamości oraz strony oferujące narkotyki, prekursorzy czy paraleki.
- Rozwój Darknetu oraz zdecydowane działania organów ścigania spowodowały przeniesienie się do tego obszaru szeregu witryn i grup dyskusyjnych dotychczas działających w indeksowanych obszarach Sieci.
- Współczesne darkmarkety (cryptomarkets) zostały ukształtowane przez dwa zjawiska technologiczne. Pierwszym zjawiskiem było powstanie/upublicznienie sieci The Onion Router (2003), zapewniającej wysoki poziom anonimowości i jednocześnie niezmiernie funkcjonalnej, drugim – stworzenie pierwszego środka płatniczego gwarantującego względną anonimowość (pseudoanonimowość), czyli kryptowaluty bitcoin (2009).



# Handel w sieci The Onion Router

- Jedyne upublicznione polskie badania, opublikowane w 2019 r., a będące wynikiem obserwacji, prowadzonej od 6 do 27 sierpnia 2018 r. 17 sklepów, z których dziewięć to sklepy pojedynczych sprzedawców (tzw. vendor shops), a osiem to darkmarkety w pełnym tego słowa znaczeniu (realizujące model targowiska – wielu sprzedających, natomiast właściciel występuje jako tzw. zaufana trzecia strona) potwierdzają, iż najliczniejszą kategorią dóbr sprzedawanych w darkmarketach są środki psychoaktywne stanowiące blisko połowę wszystkich ofert (47,6%) w grupie ponad 226 tysięcy ofert. W większości są to produkty nielegalne (czarny rynek). Druga kategoria – około jednej czwartej wszystkich ofert (26,9%) – to towary legalne, choć w wielu przypadkach procedury ich dystrybucji są nielegalne (szary rynek). Trzecią pod względem liczebności grupą produktów i usług (15,2%) są programy i sprzęt komputerowy. Jest to kategoria mieszana, w której można odnaleźć produkty zaliczane do białego, szarego i czarnego rynku. Lokuje się tu programy służące do popełniania przestępstw finansowych, „pirackie” wersje programów i gier oraz sprzęt i oprogramowanie związane z bezpieczeństwem czy kryptowalutami. Pozostałe kategorie, z których żadna nie przekracza 3 proc., to towary i usługi przynależne w większości do szarego i czarnego rynku. [Mider D., *Czarny i czerwony rynek w sieci The Onion Router – analiza funkcjonowania darkmarketów*, Przegląd Bezpieczeństwa Wewnętrznego 2019, nr 21, s. 154-190]
- Podobne wyniki znajdziemy w publikacjach zagranicznych

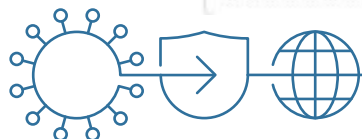


# Z czego wynika popularność darkmarketów w sieci TOR

Screenshot strony z darkmarketu Empire wg stanu z czerwca 2020

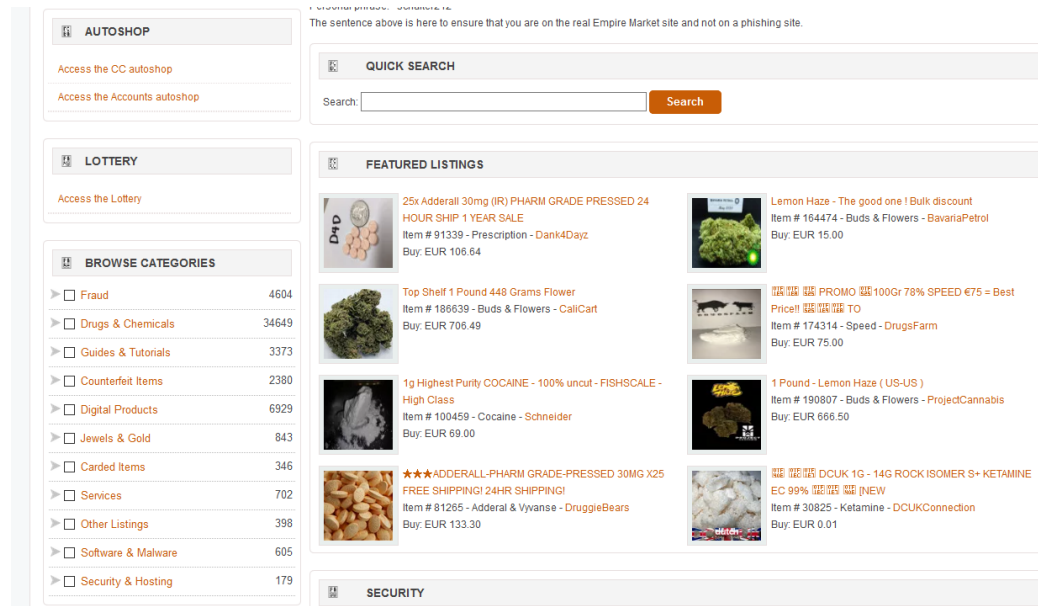
| BROWSE CATEGORIES                             |       |
|-----------------------------------------------|-------|
| ➤ <input type="checkbox"/> Fraud              | 4604  |
| ➤ <input type="checkbox"/> Drugs & Chemicals  | 34649 |
| ➤ <input type="checkbox"/> Guides & Tutorials | 3373  |
| ➤ <input type="checkbox"/> Counterfeit Items  | 2380  |
| ➤ <input type="checkbox"/> Digital Products   | 6929  |
| ➤ <input type="checkbox"/> Jewels & Gold      | 843   |
| ➤ <input type="checkbox"/> Carded Items       | 346   |
| ➤ <input type="checkbox"/> Services           | 702   |
| ➤ <input type="checkbox"/> Other Listings     | 398   |
| ➤ <input type="checkbox"/> Software & Malware | 605   |
| ➤ <input type="checkbox"/> Security & Hosting | 179   |

- Łatwość dostępu
  - Przeglądarka TOR (TOR Browser aktualnie w wersji 10.0.1) bazująca na zmodyfikowanej wersji Firefoxa
  - Intuicyjność
  - Istniejące wyspecjalizowane wyszukiwarki witryn w Darknecie (np.
    - Tor Serach – <http://http://kbhpodhnfxl3clb4.onion/>
    - Tor Find – <http://http://ndj6p3asftxboa7j.onion/>
    - TORCH – <http://xmh57jrznw6insl.onion/>
    - Grams – <http://grams7enufi7jmdl.onion/>
- Popularność (sporo opisów funkcjonowania w sieci indeksowanej (Surface Web))
- Względna anonimowość zarówno sprzedawcy jak i nabywcy
- W miarę solidne zabezpieczenia witryn

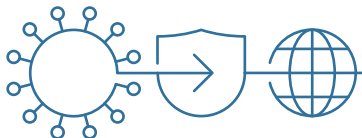


# Z czego wynika popularność darkmarketów

Screenshot kategorii z marketu Empire wg  
stanu z czerwca 2020

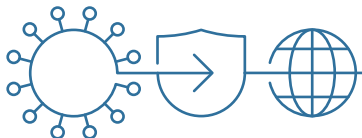


- Działania sprzedawcy
  - Rejestracja w darkmarkecie i wpłata opłaty wpisowej, powodujące założenie konta
  - Łatwość publikacji oferty (możliwość korzystania z wzorów grafiki itp.)
  - Bezpieczeństwo finansowe transakcji
  - Obowiązek stworzenia systemu „bezpiecznego” przekazywania towaru dla kupującego
- Działania kupującego
  - Rejestracja w darkmarkecie i wpłata opłaty wpisowej, powodujące założenie konta
  - Łatwość przeglądania oferty i kontaktu ze sprzedającym
  - Bezpieczeństwo finansowe transakcji
- Działania prowadzącego darkmarket
  - Zabezpieczenie serwerów, w tym dostępności i poufności
  - Kontrola poprawności transakcji i bezpieczeństwa użytkowników darkmarketu
  - Prowadzenie kantoru wymiany walut
  - Pobieranie prowizji od transakcji



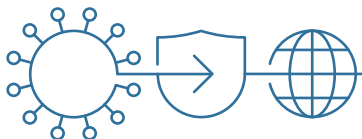
# Organy ścigania kontra darkmarkety (1)

- Operacja „*Onymous*”, listopad 2014
  - zaangażowano siły policyjne z 17 krajów, była koordynowana przez Europejskie Centrum ds. Cyberprzestępczości (EC3), Eurojust, FBI oraz U.S. Immigration and Customs Enforcement’s (ICE) i Homeland Security Investigation (HSI). Operacja zakończyła się aresztowaniem 17 osób, oraz przejęciem kilkuset adresów z domeny „.onion” i zajęciem bitcoinów wartości 1 miliona USD (wg cen w momencie realizacji), narkotyków, złota i srebra. Oprócz Silk Road 2.0 na liście ofiar organów ścigania znalazły się także takie markety jak **Pandora**, **Blue Sky**, **Topix**, **Flugsvamp**, **Cannabis Road** oraz **Black Market**. Wyłączone zostały także serwisy zajmujące się praniem brudnych pieniędzy: **Cash Machine**, **Cash Flow**, **Golden Nugget** i **Fast Cash**.
- Operacja „*Bayonet*”, lipiec 2017
  - prowadzona przez FBI i DEA i zrealizowana wspólnie z organami ścigania Kanady i Tajlandii doprowadziła do zatrzymania twórcy i administratora darkamarketu **AlphaBay**, kanadyjczyka Alexandre Cazes, prywatnie prezesa firmy programistycznej o nazwie EBX Technologies, mieszkającego w Tajlandii. Na AlphaBay było ponad 250 000 wpisów dotyczących nielegalnych narkotyków i toksycznych chemikaliów oraz ponad 100 000 wpisów dotyczących skradzionych i fałszywych dokumentów identyfikacyjnych i urzędzeń dostępu, podrobionych towarów, złośliwego oprogramowania i innych narzędzi do hakowania komputerów, broni palnej i oszukańczych usług. Ostrożnie oszacowano obrót na 1 miliard USD od czasu jego powstania w 2014 roku. Transakcje były opłacane w kryptowalutach



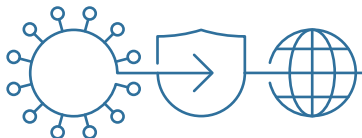
# Organy ścigania kontra darkmarkety (2)

- 20 czerwiec 2017
  - Likwidacja darkmarketu **Hansa**, który od 2016 r. był skutecznie rozpracowywany przez holenderską policję. Holenderska policja doprowadziła do aresztowania dwóch jej administratorów w Niemczech i zajęcia serwerów w Holandii, Niemczech i na Litwie. Europol i agencje partnerskie w tych krajach
- Operacja „*Darknet*”, maj 2018
  - włoska policja finansowa (Guardia di Finanza), w ramach swojego śledztwa, zidentyfikowała sprzedawcę, znanego w środowisku Dark Web jako „g00d00”. Podczas operacji funkcjonariusze organów ścigania przechwycili 2,2 kg narkotyków (kokaina, ketamina, MDMA), które były gotowe do wprowadzenia do obrotu na czarnym rynku, wraz z 163 gotowymi tabletkami ecstasy i 78 znaczkami nasączonymi LSD. Analiza komputerów osobistych, notebooków i smartfonów przejętych podczas operacji pozwoliła śledczym wyśledzić administratorów **Berlusconi Market**. W efekcie aresztowano administratora używającego pseudonimu „Władimir Putin” i moderatora o pseudonimie „Emmanuel Macron”, zamykając darkmarket, który oprócz narkotyków oferował do sprzedaży złośliwe oprogramowanie, narzędzia hakerskie, usługi hakerskie oraz skradzione dane kart płatniczych



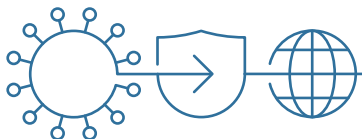
# Organy ścigania kontra darkmarkety (3)

- Operacja „*SaboTor*”, wiosna 2019
  - koordynowana przez utworzony w 2018 r w Departamencie Sprawiedliwości USA zespół Joint Criminal Opioid Darknet Enforcement (J-CODE) i Europol , której celem były działania dążące do zlikwidowania rynków leków i narkotyków online. W wyniku tych posunięć fińskie służby celne (Tulli) w ścisłej współpracy z francuską policją krajową (La Police Nationale Française) i Europolem zlikwidowały jeden z najstarszych (działający od 2013 r w sieci TOR) market **Silkkitie** (znany jako **Valhalla Marketplace**). Następnie niemiecka Federalna Policja Kryminalna (Bundeskriminalamt) wspierana przez holenderską policję narodową (Politie), Europol, Eurojust i różne agencje rządowe Stanów Zjednoczonych (DEA, FBI, IRS, HSI, US Postal Inspection Service i US Department of Justice) zamknęła **Wall Street Market**. Trzecim ważnym wydarzeniem w ramach tej operacji było zlikwidowanie w dniu 7 maja 2019 r., działającego od 2013 r., serwisu informacyjnego **DeepDotWeb**, poświęconego wydarzeniom w i wokół ciemnej sieci, zawierającego wywiady i recenzje na temat rynków Darknet oraz adresy ukrytych usług TOR, na których sprzedawcy sprzedawali nielegalne narkotyki, broń palną, złośliwe oprogramowanie i narzędzia hakerskie, skradzione informacje finansowe i karty płatnicze oraz inne nielegalne dobra. Dwóch administratorów strony internetowej zostało aresztowanych 6 maja 2019 roku we Francji i w Izraelu. Władze w USA oskarżyły ich o pranie brudnych pieniędzy i otrzymywanie prowizji, stanowiących część dochodów z każdego zakupu nielegalnych towarów dokonanych na ciemnym rynku internetowym połączonym z witryną DeepDotWeb . Jednocześnie witryna DeepDotWeb została przejęta przez organy ścigania i organy sądowe



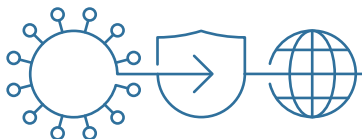
# Organy ścigania kontra darkmarkety (4)

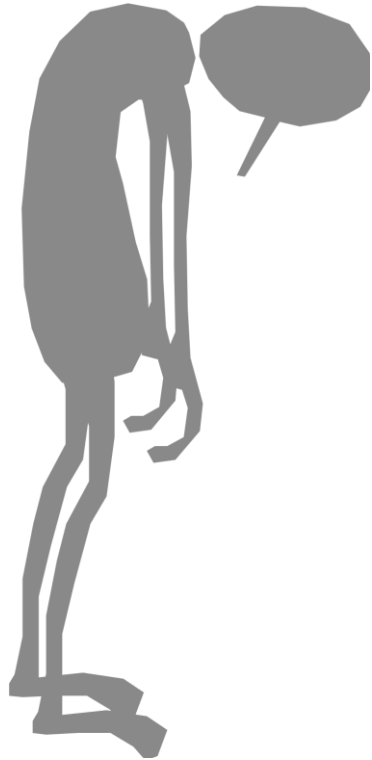
- Sierpień 2020
  - W sposób nagły administratorzy marketu „**Empire**” zakończyli jego działalność. Początkowo podejrzewano, że "Empire" nie działa, ponieważ padł ofiarą zmasowanego ataku DDoS, które coraz częściej są wymierzone w darknetowe rynki. Jest to skuteczny środek stosowany przez organy ścigania, aby wyeliminować nielegalną działalność. Wykorzystuje go również konkurencja, która w ten sposób chce pozbyć się rywala. Obecnie wszystko wskazuje na to, że to nie atak DDoS doprowadził do zamknięcia serwisu, tylko administratorzy serwisu dokonali tzw. exit scamu, czyli zniknęli bez śladu z całym zgromadzonym kapitałem. Nie wykluczone jednak, że przyczyna może być inna (podobna opinia krążyła po zamknięciu „Alpha Bay”), a po pewnym czasie przeczytamy komunikat o aresztowaniu administratorów. "Empire" powstał w 2018 roku, po tym jak upadły inne znane darkmarkety. Szybko wyrósł on na lidera w anglojęzycznym świecie Darknetu. W lipcu 2020 roku, jego obroty wyniosły około 6,5 miliona dolarów i przeprowadzono na nim ponad 50 tys. aukcji. Pozwalał na handel narkotykami, skradzionymi danymi z kart kredytowych, złośliwym oprogramowaniem, wykradzionymi bazami danych, fałszywymi paszportami i innymi dokumentami. Oferowano również m.in. usługi VPN czy różnego rodzaju poradniki dot. przeprowadzania cyberataków. Empire oferowało również automatyczny sposób płacenia kryptowalutami. Sprzedający mogli szybko tworzyć ogłoszenia o swoim produktach, a kupujący oceniali ich jakość, podobnie jak na dobrze znanych w Surface Web serwisach internetowych jak np. Allegro czy e-Bay.



# Organy ścigania kontra darkmarkety - wnioski

- Z całą pewnością ostatnie pięć lat działań organów ścigania zwalczających przestępczość w Darknecie spowoduje szereg zmian w ich funkcjonowaniu w najbliższym czasie.
- Już w grudniu 2019 roku zespół administratorów największego rosyjskiego darkmarketu **Hydra** - skoncentrowanego przede wszystkim na narkotykach, ale oferującego także towary związane z oszustwami: skradzione dane z kart kredytowych i SIM, portfele na pieniądze elektroniczne, skradzione konta i fałszywe pieniądze - ogłosił kilka nowych projektów, z których najważniejsze to **Eternos** (nowy anglojęzyczny darkmarket dla oszustów) i **AspaNET** (alternatywa dla TOR). Na te cele Hydra próbowała sprzedać 1470 000 tokenów (każdy wyceniony na 100 USD). Z założeń wynika, że Eternos będzie zawierał system dostarczania narkotyków oparty na skrytkach pozycjonowanych GPS-em oraz zaszyfrowane wiadomości i wbudowany mikser kryptowalut (usługa, która łączy różne strumienie potencjalnie możliwej do zidentyfikowania krypto waluty - właściciel bitcoina przesyła pieniądze do usługi mieszania, która miesza je z BTC innych użytkowników i przesyła mieszaną walutę na żądany adres, co oznacza, że ginie związek między pierwotną transakcją a tym adresem).
- Poza siecią TOR w Darknecie istnieją także inne sieci, które obecnie zyskują coraz więcej zwolenników – np. I2P (Invisible Internet Project) czy Freenet

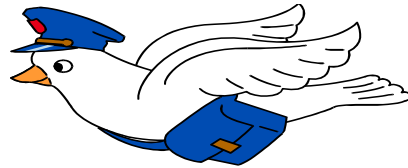




Oczekiwanie na niebezpieczeństwo jest gorsze  
niż moment, gdy ono na człowieka spada  
[Alfred Joseph Hitchcock]

**Dziękuję bardzo za uwagę**

*Kontakt do prelegenta:*



e-mail: [kojot@jakubski.pl](mailto:kojot@jakubski.pl)

