

## CYBERBAT NA PRZESTĘPCÓW. STRUKTURY UNIJNE PROPONUJĄ ZMIANY

„Ponieważ nasze życie i działalność przeniosły się do internetu bardziej niż kiedykolwiek, ślady przestępstw są również cyfrowe” – wskazuje Komisja Europejska, dodając, że ponad 80% dzisiejszych przestępstw zawiera element cyfrowy. Wagę problemu potęguje również skala zjawiska, dlatego też podjęto decyzję o wydaniu propozycji w sprawie zwiększenia możliwości służb w zwalczaniu tego typu zagrożeń.

Komisja Europejska w opublikowanym 14 kwietnia br. dokumencie „Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the EU Strategy to tackle Organised Crime 2021-2025” podkreśla pilną potrzebę zwiększenia potencjału i zdolności organów ścigania oraz prokuratury w ramach wzmocnienia dążeń do pozyskiwania specjalistycznej wiedzy w zakresie dochodzeń cyfrowych. Unijny organ wskazuje, że organy ścigania i wymiar sprawiedliwości muszą nadążać za szybko rozwijającymi się technologiami wykorzystywanymi przez przestępców.

W opublikowanym stanowisku, Komisja Europejska poświęciła osobny rozdział na wytyczne odnośnie dostosowania organów ścigania i sądownictwa do ery cyfrowej. W tej części KE wskazuje na problematykę pozyskiwania przez te podmioty dostępu do zasobów informacyjnych. Jak podkreślono, skala problemu zorganizowanej przestępczości prowadzonej przy pomocy sieci oraz szybkość, z jaką rozwija się technologia stanowią duże wyzwanie dla jej zwalczania. Sporym problemem jest również przeniesienie niektórych dowodów przestępczej działalności do sieci, a także możliwość ukrywania się za szyfrowaniem.

Kolejnym wyzwaniem, zdaniem Komisji, jest niedostosowanie do funkcjonowania w świecie cyfrowym niektórych instrumentów i środków przeznaczonych do gromadzenia materiału dowodowego – co powoduje spowalnianie, a także utrudnianie dochodzenia – głównie z uwagi na fakt, że niektóre dane mogą już nie być dostępne u operatorów. Komisja podkreśliła, że dochodzenia w sprawie przestępczości zorganizowanej zwykle wymagają dostępu do danych pochodzących z łączności elektronicznej: „dane te są potrzebne, aby stworzyć powiązanie między przestępstwem, sprawcą i ich ofiarami, a także wysledzić sieci przestępcze”. Jak wykazano w dokumencie, „biorąc pod uwagę skalę i strukturę zorganizowanej przestępczości, powiązania są trudne do prześledzenia przez organy ścigania bez dostępu do metadanych dotyczących prowadzonej komunikacji”.

*Metadane komunikacyjne mają szczególne znaczenie w dochodzeniach i ściganiu cyberprzestępczości.*

Communication from the commission to the European Parliament, the Council, the European

Dokument wskazuje na tezę zawartą w dokumencie, że utrudniony dostęp do tego typu danych powoduje, że ograniczone są możliwości identyfikacji osób stojących na czele przestępczych organizacji, które de facto „pociągają za sznurki w tle”, a zatrzymania odnoszą się do osób bezpośrednio przyłapanych na miejscu popełniania przestępstwa. Dlatego też w ramach przyjętego stanowiska, Komisja Europejska wskazuje, że konieczne jest wprowadzenie obowiązku przechowywania danych przez dłuższy czas: „Metadane komunikacyjne mają szczególne znaczenie w dochodzeniach i ściganiu cyberprzestępczości; często są podstawowym środkiem wykrywania przestępstwa i stanowią kluczowe dowody”. Jednocześnie podkreślono fakt skomplikowania rozwiązywania spraw związanych z działalnością przestępczości zorganizowanej, w szczególności w kontekście handlu narkotykami, ludźmi czy prania brudnych pieniędzy – czas potrzebny na rozwiązywanie tego typu spraw oraz fakt, że podejrzani są widoczni dopiero w toku prowadzenia dochodzenia, wskazuje jak istotne jest zwiększenie czasu przeznaczanego na przetrzymywanie danych.

Unijny organ zwraca również uwagę na potrzebę zaangażowania Europolu oraz EU Innovation Hub for Security w celu kompleksowego zidentyfikowania luk technologicznych oraz potrzeb na rzecz zwiększenia możliwości działania organów ścigania w tym zakresie. Analiza potrzeb powinna zakończyć się określeniem priorytetów badań i rozwoju, które z kolei zostaną zatwierdzone przez państwa członkowskie. Komisja wyraża także pogląd, że Europol powinien stać się punktem kompleksowej obsługi, zapewniającym dostęp do narzędzi i usług, takich jak analiza złośliwego oprogramowania dla krajowych organów ścigania.

Dlaczego jest to ważne? Jak tłumaczy portal Infosecurity24.pl omawiając w sposób kompleksowy całość dokumentu, biorąc jedynie dziewięć kluczowych przestrzeni dochodu zorganizowanej przestępczości w UE, to jej zyski można szacować na poziomie 139 mld euro, czyli wartości zbliżonej do 1 proc. unijnego PKB. Stąd też, tak istotnym staje się wymóg silniejszego wspierania poszczególnych państw członkowskich w zmaganiach ze zorganizowaną przestępczością i w tym miejscu UE nie może rozmywać swojej odpowiedzialności. Szczególnie, że PZ jest dziś coraz częściej porównywana do transnarodowych korporacji, mając swoje filie, sieci kontaktowe oraz przede wszystkim działając w oparciu o osoby wywodzące się z wielu krajów.

**Czytaj też:** [EUROPOL i EMPACT silniejsze w walce z przestępczością zorganizowaną](#)

Jak wskazuje Jacek Raubo na łamach InfoSecurity24.pl, w przypadku samej UE szacuje się, że 65 proc. grup przestępczych jest złożona z członków z różnych państw. Dlatego kluczowym aspektem, z perspektywy unijnej, staje się usprawnienie przesyłu informacji pomiędzy państwami członkowskimi oraz służbami policyjnymi itd. Zwraca się uwagę na nowe możliwości EUROPL-u, chociażby w przypadku korzystania z systemu alertów w ramach SIS (Schengen Information System), obecnie jednej z najbardziej używanych baz danych w kontekście bezpieczeństwa przestrzeni schengenowskiej.



# Reporterskie śledztwo o współczesnych metodach prowadzenia wojny informacyjnej

Sklep.Defence **24**