Górka, M., 2018, *Wybrane aspekty polityki cyberbezpieczeństwa Unii Europejskiej na przykładzie Europolu*, Przegląd Geopolityczny, 25, s. 86-103.

Marek GÓRKA
Politechnika Koszalińska

WYBRANE ASPEKTY POLITYKI CYBERBEZPIECZEŃSTWA UNII EUROPEJSKIEJ NA PRZYKŁADZIE EUROPOLU

Abstrakt:

Zwalczanie cyberprzestępczości nie może być prowadzone wyłącznie przez organy ścigania, bez ściślejszej współpracy międzynarodowej. Aby walczyć z cyberzagrożeniami, służby bezpieczeństwa muszą również współpracować ze środowiskiem akademickim i sektorem prywatnym. Zmiany w strukturze zarządzania na poziomie państwowym jak i ponadnarodowym wynikają z dominującej roli cyberprzestrzeni. Jej obrona w zmieniającym się świecie musi być rozumiana w wymiarze krajowym jak i międzynarodowym. Internet stanowi również środowisko, które otwiera nowe perspektywy dla polityki Unii Europejskiej.

Celem artykułu jest konceptualizacja ram zarządzania Internetem w celu lepszej kontroli nad bezpieczeństwem cybernetycznym przez instytucje Unii Europejskiej ze szczególnym uwzględnieniem Europolu. Ponieważ podmioty niepaństwowe i państwowe coraz częściej próbują w nielegalny sposób pozyskać dane, dokonują oszustw, a nawet destabilizują sytuację polityczną poprzez działania dezinformujące w cyberprzestrzeni, dlatego też Europol zaczyna odgrywać coraz większe znaczenie w zakresie polityki bezpieczeństwa.

Słowa kluczowe: Europol, Unia Europejska, polityka bezpieczeństwa, cyberbezpieczeństwo, cyberprzestępstwa.

Wprowadzenie

Cyberprzestrzeń interpretowana jest jako możliwość rozwoju w wymiarze politycznym, gospodarczym i kulturowym, ale równocześnie może być postrzegana jako źródło wielu niebezpieczeństw. Różnorodność współczesnych zagrożeń, w tym przestępstw związanych z zaawansowanymi technologiami jak: wyciek danych osobowych, działania dezinformacyjne, cyberataki na infrastrukturę krytyczną oraz wymuszenia seksualne, tworzą nowe i trudne wyzwania w zakresie polityki bezpieczeństwa zarówno dla poszczególnych

państw jak i większych ponadnarodowych organizacji politycznych. W konsekwencji ekspansja cybertechnologii wymusiła również na Unii Europejskiej odpowiednie działania w ramach polityki cyberbezpieczeństwa.

O znaczeniu cyberprzestrzeni dla bezpieczeństwa państwa oraz jej wpływu na bieg wydarzeń politycznych świadczą chociażby cyberataki wymierzone w amerykański system polityczny w 2016 roku. Innym ważnym wydarzeniem ilustrującym rolę zagrożeń cybernetycznych był cyberatak, wywołany przez wirus o nazwie „WannaCry", który w maju 2017 roku zablokował komputery m.in. w fabrykach, szpitalach, sklepach oraz szkołach i dotyczył ponad 200 tysięcy użytkowników w co najmniej 150 krajach[1]. Troska o stabilność polityczną i gospodarczą rodzi pytania o to, kto jest odpowiedzialny za zapewnienie bezpieczeństwa w cyberprzestrzeni, a także jak technologia wpływa na sferę polityki? Czy Unia Europejska będzie odgrywać znaczącą rolę w polityce bezpieczeństwa cybernetycznego? Pytania te dotyczą szerokiej i skomplikowanej materii, jednak warto podkreślić, że poszukiwanie odpowiedzi na tego typu dylematy, będzie wyznaczać dalszy kierunek w dyskusji w obszarze współczesnej polityki.

Celem artykułu jest przybliżenie charakteru cyberzagrożeń, które obecnie zaczynają dominować w przestrzeni publicznej, a tym samym stają się kluczowym elementem polityki bezpieczeństwa. Zjawisko to stanowi także punkt wyjścia dla dalszej analizy dotyczącej roli i zadań Europolu, jako instytucji unijnej odpowiedzialnej m.in. za działania z zakresie bezpieczeństwa cybernetycznego, a także za dostarczanie aktualnych informacji na temat cyberzagrożeń oraz prowadzenie i promowanie profilaktyki poprzez edukację i wymianę najlepszych praktyk. Praca stanowi także próbę syntetycznego ujęcia wybranych działań Unii Europejskiej na rzecz kontroli nad przestrzenią cybernetyczną poprzez zrozumienie relacji międzynarodowych względem podobieństw jak i rozbieżności w procesie współpracy między podmiotami politycznymi.

Cyberprzestępczość ma charakter międzynarodowy, a walka z tym procederem obejmuje wiele państw i instytucji publicznych. Jednak badania nad tym zjawiskiem napotykają wiele przeszkód związanych z pozyskaniem wiedzy z zakresu kontrwywiadu do której dostęp jest ograniczony. Nie bez znaczenia są także informacje na temat działań samych organów ścigania, które nie są w pełni udostępnianie, podobnie jak z wiedzą ze strony instytucji i organizacji, które padły ofiarą cyberataków. Niechęć przed upublicznieniem tego typu danych wynika - jak można przypuszczać - z obawy przed utratą dobrego wizerunku w oczach opinii publicznej. A zatem ważnym elementem w budowie polityki bezpieczeństwa jest transparentność instytucji publicznych oraz edukacja na

[1] Europol: *200K users, 150 nations hit by cyber attack and counting: World Cyber Attack*, „EFE News Service", 14 maja 2017 r.

rzecz cyberbezpieczeństwa, która często okazuje się ważnym narzędziem w działaniach prewencyjnych.

Wybrane kierunki ewolucji cyberzagrożeń

Rosnąca liczba zagrożeń sprawiła, że to ogólnoświatowe zjawisko stało się jednym z priorytetów polityki bezpieczeństwa[2]. Upowszechnienie technologii umożliwiło bardziej elastyczny dostęp do Internetu oraz zmodernizowało proces przenoszenia danych. Okazuje się więc, że w zapobieganiu cyberprzestępczości nie chodzi już tylko o ochronę komputerów, laptopów, smartfonów, ale o cyberprzestrzeń, w której zapisywane są kluczowe informacje. Państwa członkowskie UE, zdaniem ekspertów, już teraz zaliczają się do najbardziej „zakażonych" państw na świecie, jeśli chodzi o wirusy komputerowe i złośliwe oprogramowanie (Button, Stiernstedt, 2017, s. 245-257). Można przypuszczać, że im bardziej łączność internetowa będzie się rozprzestrzeniać, to tym bardziej obywatele UE oraz organizacje będą narażone na ataki cybernetyczne pochodzące również z wcześniej niepowiązanych z UE obszarów świata.

Poufne dane będące w posiadaniu instytucji odpowiedzialnych za funkcjonowanie infrastruktury krytycznej pozostają kluczowym towarem dla cyberprzestępców. W wielu przypadkach są one pozyskiwane w celu uzyskania natychmiastowych korzyści finansowych, ale coraz częściej są również nabywane w celu popełnienia bardziej złożonych oszustw, szyfrowania dla okupu lub innych form wymuszeń. Przestępczość zorganizowana staje się coraz bardziej powszechna i stanowi zagrożenie o zasięgu międzynarodowym. Nie bez znaczenia jest także zniesienie granic między państwami strefy Schengen, co stanowi także dodatkowe wyzwanie dla organów ścigania. Cyberprzestępcy bowiem mogą podejmować działania spoza granic Unii Europejskiej, aby dokonywać szkód w infrastrukturze krytycznej, których skutki mogą być odczuwalne przez dużą liczbę ofiar, przy minimalnych nakładach i ryzyku po stronie cybernapastników.

Najsłabszym ogniwem bezpieczeństwa cybernetycznego jest jednak czynnik ludzki. Wiele wyrafinowanych form ataków inżynierii społecznej skierowanych jest na pewien rodzaj oszustwa i manipulacji personelu, a bez odpowiedniego szkolenia w zakresie bezpieczeństwa może on ujawnić przestępcom poufne informacje. Przyczyną problemu cyberbezpieczeństwa są też złe praktyki przedsiębiorstw oraz kultura pracowników w zakresie bezpieczeństwa cyfrowego (Olszewski 2018).

Według sprawozdania opublikowanego w 2016 roku przez Europol zakres oraz koszty materialne cyberprzestępczości w porównaniu z poprzednimi

[2] Pytanie o cyberbezpieczeństwo dotyczy nie tylko równowagi między poczuciem bezpieczeństwa a wolnością, ale i na skoncentrowaniu się - szczególnie w kontekście cyberrewolucji - na relacji między zyskiem ekonomicznym, a bezpieczeństwem cybernetycznym (Górka, 2016, s. 49-79).

latami wykazują tendencję wzrostową. Co więcej w dokumencie zauważono, że liczba nielegalnych działań dokonywanych przy pomocy cybertechnologii zaczyna w niektórych państwach UE przewyższać liczbę tradycyjnych przestępstw[3]. Zjawisko cyberprzestępczości staje się więc coraz bardziej agresywne, a liczba zaawansowanych ataków cybernetycznych wymierzonych w międzynarodowe systemy wciąż rośnie. Europejskie Centrum ds. Cyberprzestępczości (EC3) uczestniczyło w samym 2016 roku w 131 operacjach cybernetycznych zakończonych sukcesem. Warto zauważyć, że takich akcji jeszcze dwa lata wcześniej, czyli w 2014 roku było 72. Zmiana ta wskazuje na rosnące zagrożenie, a także na możliwość zwiększenia efektywności i zdolności w walce z cyberprzestępczością po stronie sił policyjnych. Może to być także dowód na lepszą i skuteczniejszą współpracę między instytucjami pochodzącymi z rożnych państw. Realizacja partnerstwa między służbami na rzecz cyberbezpieczeństwa stwarza także nowe wyzwania (Sadowski 2017).

W raporcie odnotowane zostało również masowe stosowanie oprogramowania służącego do oszustw płatniczych. Cyberprzestępcy poszerzają zakres stosowania wirtualnych walut, takich jak „bitcoin" szczególnie w odniesieniu do okupu oraz innych form wymuszania płatności (Dallyn 2017). Zauważono także ścisły związek między osobami tworzącymi specjalistyczne cybernarzędzia a zorganizowanymi grupami przestępczymi i terrorystycznymi. Cyberprzestrzeń staje się coraz częściej obszarem do propagowania ekstremistycznych haseł. W raporcie dostrzeżono także, że cyberprzestępcy w większym stopniu kierują ataki na instytucje lub osoby o tzw. „wysokiej wartości", czyli na cele, które odpowiedzialne są za podejmowanie decyzji lub jej przekazywanie do innych miejsc w strukturze organizacji. Na cyberataki narażone są również podmioty, które ze względu na realizację swoich działań mają dostęp do kluczowych danych bądź też są odpowiedzialne za funkcjonowanie infrastruktury krytycznej.

Reasumując na podstawie sprawozdania Europolu można zidentyfikować wiele tendencji, które mogą wskazywać na przyszłe zagrożenia, ale i na obszary, w których będzie prowadzona polityka bezpieczeństwa cybernetycznego UE jak i samodzielne działania realizowane w tym zakresie przez państwa członkowskie.

Strategiczne wymiary Unii Europejskiej w zakresie cyberbezpieczeństwa

Unia Europejska podejmuje działania w celu zapewnienia bezpieczeństwa cybernetycznego. Głównym jej zadaniem jest zwiększenie zdolności państw członkowskich do wdrożenia międzynarodowej współpracy w dziedzinie bezpieczeństwa cybernetycznego oraz prowadzenia działań

[3] https://www.europol.europa.eu/newsroom/news/relentless-growth-of-cybercrime, 12.11.2017.

prewencyjnych wobec zjawisk cyberprzestępczości (Bebber 2017). Przykładem tego są liczne dokumenty, zwane także strategiami, które ustanawiają instytucje odpowiedzialne za zapewnienie bezpieczeństwa cybernetycznego, a także określają zakres ich kompetencji i zadań.

Ważnym krokiem na drodze do zapewnienia bezpieczeństwa cybernetycznego było przyjęcie w dniu 7 lutego 2013 roku dokumentu o nazwie „Strategia bezpieczeństwa cybernetycznego Unii Europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń" (Buse 2017). Celem strategii jest określenie zakresu działań, których zadaniem jest i będzie zapobieganie atakom cybernetycznym, a także zdefiniowanie odpowiednich kroków, które będą reakcją na skutki cyberincydentów.

W strategii określono pięć uniwersalnych priorytetów, które stanowią również podstawę do konstruowania cyberstrategii przez państwa członkowskie. Należą do nich takie zadania jak: osiągnięcie odporności cybernetycznej, ograniczenie cyberprzestępczości, opracowanie polityki i zdolności w zakresie obrony cybernetycznej, budowanie zdolności związanej ze wspólną polityką bezpieczeństwa i obrony, a także rozwój zasobów przemysłowych i technologicznych na rzecz bezpieczeństwa cybernetycznego. Ponadto 28 kwietnia 2015 roku w kontekście wydarzeń będących zagrożeniem dla państw członkowskich Unii Europejskiej oraz ich obywateli przyjęto nowe zapisy, które wprowadzały w zakres polityki cyberbezpieczeństwa trzy nowe cele, którymi są walka z terroryzmem, zwalczanie przestępczości zorganizowanej oraz reagowanie na zagrożenia bezpieczeństwa cybernetycznego (Kosiński 2015, s. 222).

W dokumentach sporządzonych przez instytucje europejskie i dotyczące cyberbezpieczeństwa wskazuje się na potrzebę dzielenia się informacjami za pośrednictwem Europolu oraz utrzymywania kontaktów z sektorem bezpieczeństwa krajów członkowskich jak i środowiskiem naukowym posiadającym wiedzę specjalistyczną w dziedzinie bezpieczeństwa cybernetycznego[4].

Zwalczanie cyberprzestępczości wymusza na instytucjach europejskich prowadzenie nowej strategii międzynarodowej oraz zainicjowanie ściślejszej współpracy między państwami w zakresie polityki bezpieczeństwa. Dla bezpieczeństwa państwa duże znaczenie mają sieci cywilne, które wykorzystywane są przez wiele instytucji publicznych przy współpracy i realizacji zadań publicznych z organizacjami prywatnymi. Te ostatnie jednak nie dysponują środkami prawnymi ani politycznymi umożliwiającymi bezpośrednie zajęcie się cyberzagrożeniami. Partnerstwo między instytucjami publicznymi a sektorem prywatnym ma zasadnicze znaczenie, nie tylko dla dzielenia się wiedzą wywiadowczą czy też dowodami operacyjnymi, ale także przy opracowywaniu

[4] https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016, 12.10.2017 r.

narzędzi technicznych jak i środków służących egzekwowaniu prawa. Ogrom wiedzy na temat cyberzagrożeń wymaga scentralizowanego gromadzenia danych wywiadowczych.

Instytucje unijne rozpoczęły również szereg tzw. inicjatyw miękkich, czyli działań o charakterze edukacyjnym i promocyjnym, które polegają na m.in. prowadzeniu Europejskiego Miesiąca Bezpieczeństwa Cybernetycznego. Dokonywane są także działania odnoszące się do współpracy w zakresie cyberprzestępczości i wzajemnej pomocy prawnej. Poprzez szkolenia i podnoszenie świadomości, jak również dostarczanie najlepszych praktyk w zakresie bezpieczeństwa instytucje unijne wspierają i budują strategię zwalczania cyberzagrożeń.

Rozwiązanie dzisiejszych problemów związanych z bezpieczeństwem cyfrowym wymaga wspólnego podejścia wielu instytucji państwowych jak i tych działających w sektorze prywatnym. W złożonym krajobrazie bezpieczeństwa takie partnerstwo stają się coraz ważniejsze, zwłaszcza ze względu na szybkość rozwoju technologii. Współpraca umożliwia m.in. wymianę wiedzy, danych statystycznych i informacji strategicznych dotyczących zagrożeń cybernetycznych między obiema stronami. Biorąc jednak pod uwagę wciąż nowe zagrożenia stanowiące również wyzwania dla polityki bezpieczeństwa Unii Europejskiej oraz odmienność w postrzeganiu cyberzagrożeń między państwami członkowskimi, można przypuścić, że ustanowienie spójnej międzynarodowej polityki w dziedzinie cyberprzestrzeni dla Unii Europejskiej będzie przez następne lata jednym z głównych celów polityki unijnej.

Europol

W ciągu niemal dwóch dekad swego funkcjonowania Europejski Urząd Policji (Europol) stał się głównym podmiotem w dziedzinie bezpieczeństwa wewnętrznego w Europie[5]. Instytucja ta stopniowo zwiększyła swoją zdolność do kształtowania zewnętrznego otoczenia Unii Europejskiej. Obecnie porządek światowy nie jest już zdominowany przez dwa mocarstwa, a interesy wielu podmiotów politycznych krzyżują się, co powoduje, że coraz trudniej jest przewidzieć dalszy scenariusz wydarzeń. Ponadto intensyfikacja oraz tempo zmian jakie zaszły w sferze polityki, gospodarki oraz technologii sprawiły, że rozróżnienie między bezpieczeństwem wewnętrznym i zewnętrznym traci na znaczeniu (Gruszczak 2001; Błaszczyk 2004).

Misją Europolu zgodnie z definicją zawartą w art. 2 Konwencji o Europolu jest poprawa skuteczności i efektywności współpracy z organami państw członkowskich w zapobieganiu i zwalczaniu zjawisk przestępczości międzynarodowej (Mounier 2009). Pierwotnie konwencja o Europolu

[5] Europol utworzony został na mocy Traktatu z Maastricht z 1992 roku. Jednak dopiero w lipcu 1999 roku, po tym jak wszystkie państwa członkowskie UE ratyfikowały konwencję, Europolowi udało się rozpocząć pełną działalność (Rozée, Kaunert, Léonard 2013).

przewidywała, że urząd ten będzie zajmować się wyłącznie sprawami handlu narkotykami. Jednak stopniowo również inne ważne dziedziny w zakresie bezpieczeństwa wewnętrznego dodano do zadań tej organizacji. Europol został zaprojektowany tak, aby wspierać siły policyjne państw członkowskich w walce z terroryzmem i przestępczością transnarodową. Podstawową działalnością Europolu jest gromadzenie, wymiana informacji oraz analiza danych dotyczących zagrożeń (Wagner 2006; Florek-Klęsk 2015). Europol podejmuje działania operacyjne dotyczące takich zagadnień jak m.in.: terroryzm, narkotyki, handel ludźmi, wykorzystywanie seksualne dzieci, nielegalna imigracja, fałszowanie pieniędzy, oszustwa związane z kartami płatniczymi, przestępczość w dziedzinie zaawansowanych technologii, przestępstwa związane z własnością intelektualną, czy też oszustwa związane z podatkiem VAT (Safjański 2009).

W 2009 roku postanowiono przekształcić Europol z organizacji międzyrządowej na agencję Unii Europejskiej. Jedną z konsekwencji tej decyzji jest to, że Europol finansowany jest obecnie z budżetu ogólnego Unii Europejskiej, co zwiększa kontrolę Parlamentu Europejskiego nad tą instytucją, ponieważ Parlament współuczestniczy w przyjmowaniu budżetu, w tym przy zatwierdzaniu planu zatrudnienia oraz przy procedurze udzielenia absolutorium. Stopniowe upodmiotowienie Europolu doprowadziło do tego, że agencja ta zaczęła odgrywać centralną rolę w ramach współpracy policyjnej Unii Europejskiej (Carrapiço, Trauner, 2013).

Funkcjonariusze Europolu nie mają uprawnień wykonawczych, tzn. nie mogą prowadzić działań w zakresie przeszukiwania czy też aresztowania podejrzanych osób, ale ich działania mają na celu zwiększenie skuteczności działań wykonawczych policji krajowej. Ponadto państwa członkowskie UE uzgodniły przyznanie Europolowi „uprawnień operacyjnych" (Wagner, op.cit.). Traktat Amsterdamski zobowiązuje Radę Europejską do przyjęcia środków umożliwiających Europolowi udział w dochodzeniach międzynarodowych oraz prawo do bezpośredniego zwrócenia się do władz państwa członkowskiego o zbadanie konkretnych przypadków. Funkcjonariusze Europolu mogą uczestniczyć we wspólnych zespołach dochodzeniowo-śledczych z funkcjonariuszami policji z państw członkowskich. Można przypuszczać, że Europol prawdopodobnie będzie posiadał znaczący wpływ na przebieg dochodzeń ze względu na jego nadrzędny dostęp do danych wywiadowczych.

Europol ma kluczowe znaczenie dla zaangażowania Unii Europejskiej w zwalczanie przestępczości. Dostrzec to można również w dokumentach, takich jak program haski i sztokholmski, dotyczących kwestii wymiaru sprawiedliwości i spraw wewnętrznych, które przyjęte zostały odpowiednio w 2004 i 2010 roku. W programie haskim uznano, że Europol odgrywa kluczową rolę w realizacji polityki bezpieczeństwa. W tym celu Europol otrzymał zadanie sporządzania raportów z corocznych ocen zagrożenia. Sprawozdania te obejmują m.in. zagrożenia terrorystyczne w UE jak i zjawiska przestępczości zorganizowanej.

W programie sztokholmskim z 2010 roku stwierdzono, że Europol powinien stać się węzłem wymiany informacji między organami ścigania państw członkowskich. Podkreślono również, że Europol powinien bardziej systematycznie uczestniczyć w operacjach transgranicznych. Program sztokholmski kładzie nacisk na zwiększenie roli Europolu w zwalczaniu cyberprzestępczości. Wskazuje także na obszary, które ze względu na zagrożenie wchodzą zakres szczególnego zainteresowania policji, tj.: przemoc seksualna, ataki terrorystyczne, ataki na sprzęt elektroniczny oraz sieć cybernetyczną jak i oszustwa finansowe. Ponadto zawarto wiele umów operacyjnych i strategicznych pomiędzy Europolem a państwami trzecimi, a także instytucjami spoza UE, takimi jak Interpol i FBI (Willa 2007).

Zaangażowanie Europolu w działania zwiększające poziom bezpieczeństwa z pewnością się nasili ze względu na użyteczność tej instytucji i dobrze ugruntowaną sieć łącznikową oraz możliwość wymiany informacji za pomocą systemu informatycznego SIENA. Europol działa poprzez ścisłą współpracę z organami ścigania państw Unii. Głównymi elementami tych stosunków są krajowe jednostki Europolu, które służą jako kontakt między organami tego kraju a Europolem. Każde państwo członkowskie wyznacza do tego organu oficerów łącznikowych.

Od momentu rozpoczęcia swej działalności w zakresie bezpieczeństwa (czyli od 1999 roku) Europol napotykał trudności, które ograniczały jego osiągnięcia, zwłaszcza w dziedzinie walki z terroryzmem. Po pierwsze, organy ścigania państw członkowskich niechętnie przekazywały informacje Europolowi lub też niechętnie korzystały z jego źródeł z powodu braku zaufania. Wynikało to z tego powodu, że wiele krajowych służb od dawna funkcjonowało w nieformalnych relacjach, które dotyczyły wzajemnej wymiany informacji i mając też większe zaufanie do tej formy współpracy. Ponadto tak funkcjonujące relacje między organami ścigania były postrzegane jako bardziej elastyczne oraz pragmatyczne niż działania za pośrednictwem Europolu (Rozée, Kaunert, Léonard 2013). Przeszkodą w budowaniu współpracy między służbami państw członkowskich a Europolem może być także ograniczony poziom wiedzy na temat funkcjonowania Europolu i jego zadań. Kultura policyjna stanowi również barierę we wzajemnych stosunkach, ponieważ organy ścigania mogą niechętnie przekazywać innym służbom informacje wywiadowcze, które były trudne do uzyskania.

Od samego początku istnienia Europolu jego rola w zwalczaniu cyberprzestępczości stale rosła. Stopniowo też w strukturze tej organizacji zaczęły tworzyć się badawcze zaplecza kryminalistyczne. Europol przygotowuje i przeprowadza także szkolenia dotyczące cyberprzestępczości przez wyspecjalizowanych funkcjonariuszy policji w państwach członkowskich UE

oraz w państwach kandydujących do UE[6]. Wysoka renoma Europolu - wśród służb policyjnych - jako organizacji skutecznie zwalczającej cyberprzestępczość zaczęła być budowana w wyniku wspólnie przeprowadzonych operacji, takich jak „Karnawał w Wenecji"[7] czy też operacja „Komfort"[8].

Można stwierdzić, że zwalczanie cyberprzestępczości jest dziedziną, w której Europol wykazał znaczne zdolności oferując swoje umiejętności i wiedzę organom ścigania w państwach członkowskich. Chociaż sama agencja nie ma uprawnień do aresztowania, to jednak zatrzymanie wielu osób wynika bezpośrednio z dochodzeń do których przyczynił się Europol.

Wzrost zarówno liczby podmiotów cyberprzestępczych, jak i możliwości angażowania się w wysoce dochodowe nielegalne działania są jedną z głównych przyczyn popularności cyberprzestępstw. Przykładem tego jest jeden z najważniejszych trojanów bankowych „Zeus", który był dostępny na forach hakerów i stanowił duże zagrożenie nie tylko dla systemu bankowego, ale i stabilności finansowej wielu państw. Szacuje się, że cyberprzestępcy na skutek

[6] Najczęściej spotykaną formą oszustw jest atak „phishingowy", czyli oszustwo polegające na wyłudzaniu poufnych informacji, takich jak nazwy użytkowników, hasła i dane z kart kredytowych przy pomocy technik inżynierii społecznej. Główną metodą ataków typu „phishing" jest używanie wiadomości e-mail. Cyberprzestępcy mogą wykorzystywać te ataki wymierzone przeciwko użytkownikom w celu uzyskania dostępu do danych lub dokonania zmian określonych parametrów w tym także finansowych. Innymi słowy, głównym celem ataku phishingowego jest ustanowienie fałszywej komunikacji, która jest zazwyczaj inicjowana za pomocą poczty elektronicznej zawierającej fałszywy adres URL pochodzący ze strony internetowej banku lub jednostki rządowej. Ataki phishingowe zostały po raz pierwszy szczegółowo opisane w 1987 roku, chociaż termin ten został po raz pierwszy użyty w 1996 roku (Jansson, Solms, 2013).

[7] Włoska policja oraz Europol odkryły grupę przestępczą, która instalowała złośliwe oprogramowanie na niezabezpieczonych serwerach internetowych przedsiębiorstw, co służyło dystrybucji materiałów pornograficznych z udziałem dzieci. Włoska policja przekazała dane dotyczące zainfekowanych stron internetowych, które zostały rozpowszechnione przez Europol do wszystkich organów ścigania UE, a także do państw i agencji, z którymi Europol współpracuje. Dalsze badania wykazały, że właściciele serwerów internetowych nie byli świadomi problemu i nie byli także zaangażowani w działalność przestępczą, a ich serwery zostały zainfekowane z powodu braku bezpieczeństwa Internetu. Grupa przestępcza odpowiedzialna za złośliwe oprogramowanie pochodziła z Europy Wschodniej. Włoska Policja współpracując z Europolem opracowała strategie śledzenia transferu pieniędzy odkrywając w ten sposób klientów nielegalnych treści. W wyniku tej operacji ponad 1 000 serwerów internetowych na całym świecie zostało „wyczyszczonych" z nielegalnych zasobów (https://www.europol.europa.eu, 12.11.2017 r.).

[8] Na początku 2010 roku holenderska policja otrzymała informacje z holenderskiego hostingu internetowego, że na jednym z serwerów ich klienta cyberprzestępcy umieścili materiały przedstawiające wykorzystywanie seksualne dzieci. Pliki dziennika tego serwera z wykrytymi nielegalnymi treściami przesłano do baz danych Europolu. Funkcjonariusze Europolu przeanalizowali dane i przekazali sprawozdania z analiz wszystkim zainteresowanym państwom. W trakcie analizy zidentyfikowano aż 3 931 celów na terenie UE oraz 6 041 osób spoza niej, mających związek z nielegalnymi treściami (https://www.europol.europa.eu, odczyt z dnia: 12.11.2017 r.)

tego oprogramowania ukradli dziesiątkom tysięcy osób poufne informacje dotyczące ich rachunków bankowych, które opiewały na ponad 2 miliony euro. W 2015 roku wspólny zespół dochodzeniowy złożony z śledczych z sześciu krajów, koordynowany przez Eurojust i Europol, aresztował ukraińską grupę przestępczą zajmującą się cyberprzestępczością, która opracowała i rozpowszechniała różne wersje tego oprogramowania (Leon 2014). Innym, równie groźnym trojanem bankowym, który zainfekował tysiące komputerów okazało się oprogramowanie o nazwie „Shylock". Program ten kradł poufne informacje dotyczące bankowości internetowej i dokonywał oszustw finansowych podczas transakcji[9]. Operacja, która miała na celu eliminację szkodliwego oprogramowania oraz aresztowanie osób odpowiedzialnych za zainfekowanie systemów komputerowych, była koordynowana przez Europol i obejmowała współpracę jednostek ds. cyberprzestępczości z różnych krajów i CERT-UE.

Po atakach terrorystycznych w Paryżu w 2016 roku niektórzy europejscy politycy wzywali publicznie do zwiększenia uprawnień agencji. Charles Michel, premier Belgii, zaproponował nawet, aby UE utworzyła „europejski odpowiednik CIA"[10]. Można przypuszczać, że pomysły i inicjatywy polityczne wywołane po części dramatycznymi wydarzeniami oraz zwiększającym się zagrożeniem spowodują przyspieszenie ewolucji w kierunku budowy ponadnarodowej służby o znacznie większych kompetencjach oraz możliwościach wywiadowczych i kontrwywiadowczych.

System informacyjny Europolu

System informacyjny Europolu jest narzędziem za pomocą którego agencja wspiera prowadzone dochodzenia w państwach członkowskich. Grupy dochodzeniowe otrzymują wsparcie zespołów analizujących pliki AWF (Analysis Work Files) w postaci danych wywiadowczych, analiz oraz pomocy ekspertów. Dochodzenia krajowe prowadzą do uzyskania informacji, które są dostarczane za pośrednictwem bezpiecznych kanałów komunikacji do jednostki analitycznej Europolu. Tworzy się zamknięty obieg danych w taki sposób, że prowadzone dochodzenia dostarczają sobie nawzajem nowych informacji. W ten sposób baza ta działa jako centralny punkt umożliwiający korzystanie z informacji w śledztwach krajowych uzyskanych z innych państw[11].

Ponadto państwa członkowskie za pośrednictwem swoich biur łącznikowych mogą także bezpośrednio wymieniać dane dotyczące podejrzanych osób za pośrednictwem systemu wymiany informacji (InfoEx). Również utworzona platforma na bazie Europejskiego Centrum ds. Walki z

[9] *Shylock malware has taken a hit from Europol*, „Progressive Digital Media Technology News", 11. 07. 2014.
[10] https://www.ft.com/content/0a070084-aa8c-11e6-9cb3-bb8207902122, 12.09.2017 r.
[11] *Europol Information Management*, źródło: moi.mk/.../Europol%20Products%20and%20Services-Booklet.pdf, 12.11.2017 r.

Cyberprzestępczością zawiera takie elementy jak: system (I-CROS) umożliwiający zgłaszanie przestępstw w Internecie. Posiada narzędzia poprzez, które agencje krajowe mogą składać sprawozdania oraz internetowe ekspertyzy kryminalistyczne dzięki platformie (I-FOREX) zawierającej informacje wykorzystywane głównie do szkolenia i wymiany informacji między policją z poszczególnych państw.

System informacyjny Europolu gromadzi dane w sprawie zarówno podejrzanych jak i osób skazanych, do których policja państwa członkowskiego ma dostęp poprzez krajowe biura łącznikowe. Dodatkowo zbierane są informacje na temat ewentualnych świadków oraz osób związanych lub utrzymujących możliwy kontakt z przestępcami. Celem pozyskanych treści jest badanie struktur przestępczości zorganizowanej. Wyniki tych analiz są następnie przedstawiane państwom członkowskim, które z kolei mogą wszczynać dochodzenia. Dane Europolu pochodzą z państw członkowskich za pośrednictwem krajowych biur łącznikowych. Funkcjonariusze Europolu wprowadzają dane, które uzyskali również z trzeciego źródła, czyli od państwa nienależącego do UE lub od organizacji międzynarodowych (Wagner, op.cit.). Taka wymiana danych odbywa się w ramach odpowiednich umów o współpracy, a ich postanowienia były negocjowane przez m.in. Europol.

Jak wskazano wcześniej jednym z głównych zadań Europolu jest gromadzenie i analiza danych wywiadowczych dostarczanych przez państwa członkowskie lub pozostałe państwa, organizacje międzynarodowe bądź dostępne źródła informacji. Agencja używa do wymiany informacji, bezpiecznych instrumentów, takich jak SIENA, co pozwala jej na zachowanie poufnej wymiany danych między zainteresowanymi państwami. Narzędzie to zapewnia również wysoką zdolność do współdziałania z innymi systemami na poziomie europejskim oraz państwami współpracującymi z UE. Na przykład tylko w 2012 roku dzięki współpracy w ramach systemu SIENA wszczęto postępowanie w 15,949 przypadków. Bardzo wymowna jest także skala komunikatów operacyjnych, która w liczbie 414,334 informacji, była prowadzona między służbami (Ambrozie, 2014).

Oprócz danych na temat osób podejrzanych i skazanych, system obejmuje również dane osób, które miały powiązania z określonym przestępstwem (takich jak świadkowie i ofiary). Z uwagi na wrażliwość tego typu danych, baza ta nie jest otwarta dla wszystkich funkcjonariuszy. Jedynie śledczy z państw członkowskich uczestniczący w systemie przetwarzania informacji o określonych obszarach przestępczości mogą mieć do nich dostęp.

Europejskie Centrum ds. Walki z Cyberprzestępczością

W 2013 roku Europol utworzył Europejskie Centrum ds. Walki z Cyberprzestępczością (EC3), które działa na rzecz ochrony obywateli europejskich i państw członkowskich UE. Na poziomie operacyjnym EC3 koncentruje się na nielegalnych działaniach internetowych prowadzonych przez

zorganizowane grupy przestępcze takie jak: ataki na e-bankowość oraz inne internetowe transakcje finansowe, wykorzystywanie seksualne nieletnich, cyberataki skierowane na systemy infrastruktury krytycznej w UE. Instytucja oferuje także wsparcie dla krajowych organów ścigania w ich wysiłkach na rzecz zwalczania cyberprzestępczości (Safjański 2016; Buse 2017).

Jednym z przykładów skuteczności EC3 jest operacja „Onymous" z listopada 2014 roku, która przeprowadzona została w oparciu o współpracę z ponad 15 służbami z krajów członkowskich. Celem tej akcji było ograniczenie działań w tzw. „darknecie", czyli w przestrzeni, która jest trudno dostępna i znana tylko nielicznym użytkownikom. Ponadto miejsce to opiera się na anonimowości użytkowników, a przeprowadzane transakcje najczęściej dotyczą nielegalnych towarów i usług jak: narkotyki, broń palna, skradzione dane wraz z kartami kredytowymi, fałszywe paszporty, a także narzędzia komputerowe wraz z radami, wskazówkami lub specyficznymi usługami ze strony hakerów. Na skutek tej operacji zidentyfikowano 400 internetowych adresów użytkowników oraz zarekwirowano podobną liczbę serwerów komputerowych[12].

Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)

Wraz z rozwojem polityki cyberbezpieczeństwa w Unii Europejskiej utworzona została w 2004 roku Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA), która stanowi centrum wiedzy specjalistycznej w zakresie bezpieczeństwa cybernetycznego. Jej głównym zadaniem jest pomaganie państwom członkowskim w zapobieganiu problemom związanym z bezpieczeństwem informacji. Agencja ściśle współpracuje z państwami członkowskimi i sektorem prywatnym w celu zapewnienia doradztwa i rozwiązań. Jej działania obejmują ogólnoeuropejskie ćwiczenia w zakresie bezpieczeństwa cybernetycznego, opracowanie krajowych strategii bezpieczeństwa cybernetycznego oraz współpracę z zespołami na poziomie państw narodowych reagującymi na zagrożenia i incydenty bezpieczeństwa w cyberprzestrzeni tzw. CSIRT (ang. Computer Security Incident Response Team). ENISA zajmuje się także wspieraniem potencjału technologicznego i intelektualnego, który wzmacniałby politykę bezpieczeństwa w kwestii ochrony danych osobowych oraz identyfikowaniem możliwych zagrożeń cybernetycznych (Buse, op.cit.). Agencja ta opracowuje i publikuje również sprawozdania dotyczące kwestii bezpieczeństwa cybernetycznego. W najnowszym raporcie z 2016 roku autorzy zauważyli groźną tendencję do zwiększonego występowania przypadków złośliwego oprogramowania, cyberataków oraz odmowy świadczenia usług w wyniku paraliżu systemów operacyjnych. Podkreślono również znaczenie czynników poza

[12] https://www.justice.gov/opa/speech/attorney-general-loretta-e-lynch-addresses-european-cybercrime-center-europol, odczyt: 06.10.2017 r.

technologicznych, które mają ogromny wpływ na manipulacje, uszkodzenia czy też na takie zjawiska jak kradzieże i wycieki poufnych danych.

Współpraca w zakresie cyberbezpieczeństwa

Dużym wyzwaniem jest współpraca operacyjna między rządami europejskimi, a strukturami UE. Europol, Eurojust (Europejska Jednostka Współpracy Sądowej) oraz ENISA pełnią rolę instytucji współpracujących z organami krajowymi. Istotną rolę odgrywa również Centrum ds. Cyberprzestępczości Europolu (EC3), które stało się ośrodkiem koordynacji międzynarodowego wsparcia dla wspólnych działań organów ścigania związanych z cyberprzestrzenią. EC3 pomaga państwom członkowskim, a także służbom o charakterze międzynarodowym w zwalczaniu cyberprzestępczości poprzez wykorzystanie infrastruktury i sieci Europolu, która służy m.in. do wymiany informacji wywiadowczych (Gruszczak 2009; Korajda 2016).

Dzielenie się wiedzą i współpraca w zakresie incydentów pozostają dobrowolne, a zatem do państw członkowskich należy dążenie do bliższej współpracy. Pomimo wielu wyzwań, dostrzec można znaczący postęp i poprawę w zakresie współpracy międzynarodowej w ciągu ostatnich kilku lat. Na poziomie polityki bezpieczeństwa, pojawiło się wiele inicjatyw na rzecz poprawy i harmonizacji przepisów, takich jak Network and Security (NIS) dyrektywy przyjętej przez Parlament Europejski w marcu 2015 roku[13]. Ponadto inicjatywy do podjęcia współpracy od dawna widoczne są w kontaktach z licznymi partnerami politycznymi, w tym Chinami, Indią, Koreą Południową i Japonią[14]. Warto wspomnieć, że prowadzony dialog UE ze Stanami Zjednoczonymi pomógł obu podmiotom skoordynować wspólne podejście do polityki bezpieczeństwa cybernetycznego w większości kluczowych obszarów dla gospodarki państwa. Można odnotować również zauważalną zbieżność kierunków polityki USA i UE. Przykładem tego jest ustawa uchwalona w 2015 roku przez Kongres Stanów Zjednoczonych, a także rozporządzenie prezydenta Obamy z 2015 roku. Oba dokumenty dotyczą przede wszystkim zwiększenia szybkości, regularności i centralizacji w procesie wymiany informacji między sektorem publicznym a prywatnym[15].

Europol, za pośrednictwem EC3, uczestniczył w licznych operacjach z organami ścigania Stanów Zjednoczonych w celu zlikwidowania cyberprzestępczości. Współpracował z partnerami sektora prywatnego takimi

[13] *EUROPOL's Master Keystroke: The architecture of cyber superiority in a crime-free EU,* źródło: http://chicagopolicyreview.org/2015/01/21/europols-master-keystroke-the-architecture-of-cyber-superiority-in-a-crime-free-eu, 11.11.2017 r.

[14] http://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2015)564374, 12.11.2017 r.

[15] R. Tehan, *Cybersecurity Legislation, Hearings, and Executive Branch Documents*, źródło: https://fas.org/sgp/crs/misc/R43317.pdf, 09.10.2017 r.

jak Microsoft i Symantec, aby w zlikwidować jeden z najbardziej szkodliwych botnetów (Ilves, Evans 2016).

W 2015 roku w ramach operacji „Bugbite" będącej efektem współpracy FBI i Europolu udało się usunąć w „darknecie" jedno z najbardziej rozbudowanych forum cyberprzestępczości[16]. Komunikacja między cyberprzestępcami odbywa się najczęściej w tego typu zakonspirowanych sieciach internetowych. A zatem fora, na których cyberprzestępcy dzielą się informacjami znajdują się w tzw. „darknecie", który zawiera wiele treści na temat m.in. nielegalnych materiałów czy też narzędzi do ataków cybernetycznych (Moore, Rid 2016).

Badacze wskazują na prawdopodobieństwo zwiększonego wykorzystania wspólnych zespołów dochodzeniowo-śledczych, ponieważ mogą one mieć pozytywny efekt w walce z przestępczością międzynarodową (Occhipinti 2015). Współpraca EC3 z przedstawicielami policji z państw członkowskich UE polega m.in. na dostarczaniu wsparcia analitycznego, prawnego oraz technicznego. Instytucja ta współpracuje także z 19 państwami nienależącymi do UE, jak np.: Rosja, Ukraina, Kolumbia, Turcja i Stany Zjednoczone. EC3 współpracuje także z Centrum Doskonalenia Obrony przed Cyberatakami NATO w Tallinie (Bossong, Wagner 2017).

Bardzo dobrym przykładem wysiłków EC3, w celu zaspokojenia potrzeb państw członkowskich w efektywnej współpracy globalnej w walce z cyberprzestępczością jest powołanie Wspólnej Grupy Zadaniowej ds. Walki z Cyberprzestępczością (Joint Cybercrime Action Taskforce J-CAT). Jest to międzynarodowy zespół zadaniowy i operacyjny, do którego należą organy ścigania z krajów UE jak i spoza UE, pod przewodnictwem brytyjskiej Narodowej Agencji ds. Przestępczości (NCA)[17]. Został on uruchomiony w celu walki z przestępczością w Internecie poprzez łączenie zasobów pochodzących od państw członkowskich UE oraz od kluczowych partnerów z całego świata.

Organy ścigania nie mogą walczyć z cyberprzestępczością w izolacji. Dlatego EC3 nie tylko stawia duży nacisk na rozwój relacji z organami ścigania i spoza Europy, ale także dociera do sektora prywatnego, środowisk akademickich i organizacji partnerskich, takich jak ENISA, CEPOL, Eurojust i Interpol[18].

[16] https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta-2016, odczyt z dnia: 07.10.2017 r.

[17] https://www.cbronline.com/cybersecurity/solutions/uk-to-lead-europols-new-international-cybercrime-taskforce-020914-4359118, 07.10.2017 r.

[18] Europol podejmuje ścisłą współpracę z Interpolem polegająca na przeprowadzaniu wspólnych operacji wymierzonych w działalność osób, których działania w cybersieci, mogą stanowić zagrożenie dla m.in. sprawnego funkcjonowania infrastruktury krytycznej jak systemy energetyczne czy telekomunikacyjne (Safjański, 2015).

Zakończenie

Po 20 latach od ataków cybernetycznych na Estonię w 2007 roku można stwierdzić, że przestrzeń publiczna wraz z infrastrukturą państwa jest narażona na znacznie większe zagrożenie niż do tej pory. Unia Europejska stoi również w obliczu tego samego rodzaju cyberprzestępstw, z którymi niemal na co dzień zmagają się instytucje w sektorze prywatnym, począwszy od losowych po przemyślane i ukierunkowane cyberataki. Mimo środków zapobiegawczych cyberprzestępcy na całym świecie nadal uzyskują dostęp do tych sieci, w tym do sieci będących elementem infrastruktury krytycznej.

Rewolucja cyfrowa zmieniła podstawowe środowisko, w którym działają rządy, co wymaga zwiększenia poziomu transgranicznej współzależności i łączności. Państwa europejskie odpowiedziały na potrzebę współpracy poprzez nowe inicjatywy na poziomie państwowym oraz ponadnarodowym. Istnieją jednak pewne trudności w zwalczaniu cyberprzestępczości w obszarze polityki europejskiej. Jednym z takich głównych problemów jest brak możliwości współpracy prawno-sądowej z państwami spoza Unii Europejskiej. Dlatego wciąż dużym wyzwaniem w zakresie polityki cyberbezpieczeństwa jest harmonizacja norm i zapisów prawnych dotyczących takich działań jak identyfikacja sprawców i przekazywanie danych na ich temat oraz prowadzenie działań śledczych mających doprowadzić sprawców przed wymiar sprawiedliwości.

W ostatniej dekadzie UE uznała, że bezpieczeństwo cybernetyczne jest kluczowym wyzwaniem dla polityki bezpieczeństwa, wyrazem tego jest przyjmowanie coraz bardziej ambitnych strategii, tworzenie nowych organizacji oraz wprowadzanie przepisów mających na celu przeciwdziałanie cyberzagrożeniom. Dotychczasowe regulacje oraz działania poszczególnych instytucji unijnych odpowiedzialnych za bezpieczeństwo tworzą skuteczny unijny system ochrony obywateli, przedsiębiorstw i instytucji publicznych w Europie. Pamiętać jednak należy, że na skutek udanych i widocznych działań organów ścigania takich jak operacja „Onymous" cyberprzestępcy mogą zintensyfikować wysiłki poprzez skuteczniejszy proces anonimizacji i szyfrowania swoich działań.

UE podejmuje działania w celu zwiększenia odporność na ataki cybernetyczne. A zatem odgrywa ona istotną rolę w kształtowaniu europejskiego krajobrazu bezpieczeństwa cybernetycznego, głównie poprzez prawodawstwo oraz podległe jej instytucje, które w założeniu mają zapobiegać oraz szybko i skutecznie reagować na zaistniałe już cyberprzestępstwa. W tym zakresie główną instytucją jest Europol, będący jednocześnie centralnym punktem współpracy policyjnej w Europie. Jego zadania odnoszące się do cyberbezpieczeństwa można podzielić na trzy główne obszary: pierwszym z nich są oszustwa online dokonywane przez zorganizowane grupy przestępcze; drugim przestępczość wymierzona w konkretne grupy społeczne (na przykład wykorzystywanie

seksualne dzieci w Internecie) i trzecim to cyberataki skierowane na krytyczne systemy infrastruktury i informacji w Unii Europejskiej.

Europol ma na celu nawiązywanie i utrzymywanie współpracy ze środowiskiem akademickim oraz przemysłem, dzięki czemu organy ścigania mają możliwość prowadzenia analizy oraz wzajemnej wymiany wiedzy i doświadczeń z obszaru cyberbezpieczeństwa. Cyberprzestrzeń jest także narzędziem wspomagającym funkcjonowanie Europolu, który za pomocą nowych technologii powoli staje się wiodącą instytucją, która zbiera informacje na temat przestępczości. W odniesieniu do tak realizowanego celu strategicznego, Europol może stać się głównym ośrodkiem wsparcia dla działań europejskich organów ścigania.

W strategicznym interesie UE leży zapewnienie, by narzędzia bezpieczeństwa cybernetycznego rozwijały się w sposób umożliwiający rozwój gospodarki cyfrowej, chroniąc jednocześnie państwo i jego obywateli.

Literatura

Ambrozie, O., 2014, *European Institutions involved in the fight against serious forms of crime*, International Scientific Conference Strategies XXI, vol. 2, s. 64-69.

Bebber, R., 2017, *Cyber power and cyber effectiveness: An analytic framework*, Comparative Strategy, vol. 36/5, s. 426-436.

Błaszczyk, M., 2004, *Europejski Urząd Policji - EUROPOL: geneza, podstawy prawne, struktura wewnętrzna i zakres działania,* Problemy Integracji Europejskiej, T. 1., s. 81-90.

Bossong, R., Wagner, B., 2017, *A typology of cybersecurity and public-private partnerships in the context of the EU*, Crime, Law and Social Change, vol. 67/3, s. 265-288.

Buse, M., 2017, *European Union cyber security in a globalized world*, International Scientific Conference Strategies XXI, vol.1, s. 159-164.

Button, M., Stiernstedt, P., 2017, *The evolution of security industry regulation in the European Union*, International Journal of Comparative and Applied Criminal Justice, vol. 42/4, s. 245-257.

Carrapiço, H., Trauner, F., 2013, *Europol and its Influence on EU Policy-making on Organized Crime: Analyzing Governance Dynamics and Opportunities*, Perspectives on European Politics and Society, vol. 14/3, s. 357-371.

Dallyn, S., 2017, *Cryptocurrencies as market singularities: the strange case of Bitcoin*, Journal of Cultural Economy, vol. 10/5, s. 462-473.

Florek-Klęsk, D., 2015, *Europol jako instytucja ochrony bezpieczeństwa państwa*, [w:] *Służby i formacje w ochronie bezpieczeństwa państwa*, red. I. Oleksiewicz, Rzeszów, s. 17-27.

Górka, M., 2016, *Wolność czy bezpieczeństwo? Przyczynek do rozważań na przykładzie ustawy o działaniach antyterrorystycznych z dnia 10 czerwca 2016 roku*, e-Politikon, nr 19, s. 49-79.

Gruszczak, A., 2001, *Europol : wyzwania i zadania na progu XXI wieku*, Przegląd Policyjny, nr 3, s. 125-140.

Gruszczak, A., 2009, *Europejski Urząd Policji (Europol): okoliczności i geneza powstania*, Politeja, nr 2, s. 213-234.

Ilves, L. K., Evans, T. J., 2016, *European Union and NATO Global Cybersecurity Challenges: A Way Forward*, Journal of the Center for Complex Operations, vol. 6/2, s. 126-141.

Jansson, K., Solms, R., 2013, *Phishing for phishing awareness*, Behaviour & Information Technology, vol. 32/6, s. 584-593.

Korajda, A., 2016, *Europejski Urząd Policji - Europol*, Policja: Kwartalnik Kadry Kierowniczej Policji, vol. 17/2, s. 17-25.

Kosiński, J., 2015, *Paradygmaty cyberprzestępczości,* Difin, Warszawa.

Leon, M., 2014, *Bankers' guide to Malware*, Bank Technology News, vol. 27/3.

Moore, D., Rid, T., 2016, *Cryptopolitik and the Darknet*, Global Politics and Strategy, vol. 58/1, s. 7-38.

Mounier, G., 2009, *Europol: A New Player in the EU External Policy Field?,* Perspectives on European Politics and Society, vol. 10/4, s. 582-602.

Occhipinti, J. D.,2015, *Still Moving Toward a European FBI? Re-Examining the Politics of EU Police Cooperation*, Intelligence and National Security, vol. 30/2-3, s. 234-258.

Olszewski, B., 2018, *Ataki cyber-fizyczne a system bezpieczeństwa narodowego*, [w:] T. Dąbrowski (red.), *Cyberbezpieczeństwo wyzwaniem XXI wieku*, Uniwersytet Wrocławski, Łódź-Wrocław, s. 67-84.

Rozée, S., Kaunert, Ch., Léonard, S., 2013, *Is Europol a Comprehensive Policing Actor?,* Perspectives on European Politics and Society, vol. 14/3, s. 372-387.

Sadowski, J., 2017, *Cybernetyczny wymiar współczesnych zagrożeń*, Studia nad Bezpieczeństwem, nr 2, s. 57-75.

Safjanski, T., 2015, *Prospects for the Development of the International Criminal Police Organisation Interpol*, Internal Security, vol. 7/2, s. 267-277.

Safjański, T., 2009, *Europejskie Biuro Policji Europol: geneza, główne aspekty działania, perspektywy rozwoju*, Oficyna Wolters Kluwer Polska, Warszawa.

Safjański, T., 2016, *Taktyczno-kryminalistyczne aspekty działania Europejskiego Centrum ds. Walki z Cyberprzestępczością*, Przegląd Policyjny, R. 26, nr 2, s. 114-126.

Świątkowska, J., 2017, *Walka z cyberzagrożeniami jako wyzwanie stojące przed globalnym bezpieczeństwem*, Przegląd Geopolityczny, 20, s. 162-177.

Wagner, W., 2006, *Guarding the guards. The European Convention and the communitization of police co-operation*, Journal of European Public Policy, vol. 13/8, s. 1230-1246.

Wilczyński, P. L., 2017, *Problematyka bezpieczeństwa we współczesnym dyskursie eksperckim w Polsce,* Przegląd Geopolityczny, 21, s. 48-66.

Wilczyński, P. L., Adamczyk, N., 2018, *Siły zbrojne Unii Europejskiej*, Przegląd Geopolityczny, 23, s. 100-122.

Willa, R., 2007, *Europol - forum wymiany informacji czy europejskie FBI?*, Athenaeum, vol. 18, s. 86-100.

Selected aspects of European Union cyber security policy on the example of Europol

Combating cybercrime can not be carried out solely by law enforcement authorities, without closer international cooperation. To fight cyber threats, security services also need to work together with academia and the private sector. Changes in the governance structure at the state and supranational level result from the dominant role of cyberspace. Its defence in a changing world must be understood both nationally and internationally. The Internet is also an environment that opens up new perspectives for the European Union's policy.

The aim of this article is to conceptualize the framework of Internet governance in order to improve the control over cyber security by European Union institutions, with particular focus on Europol. Since non-State actors and state entities are increasingly trying to illegally obtain data, engage in fraud and even destabilise the political situation through disinformation activities in cyberspace, Europol is therefore beginning to play an increasingly important role in the field of security policy.

Key words: Europol, European Union, security policy, cybersecurity, cybercrime.