Tom 17/2025, ss. 159-178
ISSN 0860-5637
e-ISSN 2657-7704
DOI: 10.19251/rtnp/2025.17(8)
www.rtnp.mazowiecka.edu.pl

Izabela Markiewicz
Uniwersytet Warszawski
i.markiewic2@student.uw.edu.pl
https://orcid.org/0009-0006-4697-2296

Wpływ służb specjalnych na kształtowanie cyberbezpieczeństwa. Perspektywa europejska

The Impact of Intelligence Services on Shaping Cybersecurity: A European Perspective

Streszczenie
Celem artykułu jest ocena roli służb specjalnych w kształtowaniu polityk i strategii cyberbezpieczeństwa w Europie w latach 2000–2025, ze szczególnym uwzględnieniem modeli Wielkiej Brytanii, Norwegii i Szwajcarii oraz studium przypadku roli GCHQ i National Cyber Force w tworzeniu *National Cyber Strategy 2022. Zastosowano jakościową* metodę badań: krytyczny przegląd literatury, dokumentów strategicznych i aktów prawnych, analizę porównawczą rozwiązań instytucjonalnych oraz studium przypadku. Wnioski wskazują, że skuteczność służb rośnie wraz z ich formalną integracją z krajowymi strukturami cyberbezpieczeństwa (CSIRT/NCSC), skodyfikowanymi procedurami wymiany informacji i zdolnościami ofensywnymi osadzonymi w przejrzystych ramach prawnych. Jednocześnie utrzymuje się napięcie między potrzebą bezpieczeństwa a ochroną

praw podstawowych. Artykuł rekomenduje wzmacnianie nadzoru demokratycznego, interoperacyjnych procedur reagowania oraz dalszą harmonizację standardów w UE (NIS2, certyfikacja).

Słowa kluczowe: cyberbezpieczeństwo; służby specjalne; GCHQ; National Cyber Force; NIS2; ENISA; ransomware; APT; Europa.

Abstract
This article assesses how intelligence services have shaped cybersecurity policies and strategies across Europe (2000–2025), focusing on the UK, Norway, and Switzerland, and featuring a case study of GCHQ and the National Cyber Force (NCF) in drafting the UK *National Cyber Strategy 2022*. The study applies qualitative methods: a critical review of the relevant literature, strategies and the legal acts, a comparative analysis of institutional models, and a case study approach. Findings show the effectiveness increases when intelligence services are formally integrated with national cybersecurity structures (CSIRTs/NCSC), operate under codified information sharing procedures, and maintain calibrated offensive capabilities within clear legal and ethical frameworks. Tensions persist between security needs and civil liberties, especially with regard to bulk surveillance powers and cyber operation attribution. The article recommends strengthening democratic oversight, interoperable incident response procedures, and further EUlevel harmonisation (NIS2, certification).

Keywords: cybersecurity; intelligence services; GCHQ; National Cyber Force; NIS2; ENISA; ransomware; APT; Europe.

1. Wstęp

Postępująca cyfryzacja państw i gospodarki uczyniła cyberprzestrzeń jednym z głównych pól rywalizacji geopolitycznej. Od prostych robaków początków lat 2000 po złożone kampanie APT, ransomware i operacje wpływu – skala oraz konsekwencje incydentów wymusiły redefinicję roli służb specjalnych w polityce bezpieczeństwa państw europejskich [ENISA 2022; Europol 2021]. Szczególnym katalizatorem zmian stały się ataki z 2007 r. na Estonię oraz z 2017 r. (*WannaCry*, *NotPetya*), a w najnowszym okresie – wojna rosyjsko-ukraińska i towarzyszące jej działania w cyberprzestrzeni [Cloudflare 2025; ENISA 2024]. W świetle powyższego, artykuł stawia sobie za problem badawczy pytanie: jak

i w jakim zakresie służby specjalne kształtują krajowe i europejskie ramy cyberbezpieczeństwa?

Głównym celem badania jest ocena wpływu służb specjalnych na strategie i systemy cyberbezpieczeństwa państw europejskich w latach 2000–2025. Analiza koncentruje się na wybranych modelach europejskich, ze szczególnym uwzględnieniem Wielkiej Brytanii, Norwegii i Szwajcarii, a także na roli brytyjskich agencji GCHQ (Government Communications Headquarters) oraz NCF (National Cyber Force) w kształtowaniu brytyjskiej *National Cyber Strategy 2022* [Great Britain – GCHQ 2022; Great Britain – NCF 2023].

Dla osiągnięcia tego celu sformułowano następujące pytania badawcze:

1. Jakie modele integracji służb specjalnych z krajowym systemem cyberbezpieczeństwa wykształciły wybrane państwa europejskie?
2. Jak GCHQ/NCF wpłynęły na brytyjską politykę cyberbezpieczeństwa?
3. Jakie są konsekwencje dla równowagi między wymogami bezpieczeństwa a prawami obywatelskimi w kontekście wzmocnionej roli wywiadu?

Badanie ma charakter jakościowy. Wykorzystano przegląd literatury i dokumentów (strategie, ustawy UE i krajowe), porównanie modeli instytucjonalno-prawnych oraz studium przypadku (GCHQ/NCF). Zakres czasowy obejmuje lata 2000–2025 w kontekście europejskim, przy czym ograniczeniem metodologicznym jest siłą rzeczy brak dostępu do niejawnych danych operacyjnych.

2. Teoretyczne i historyczne podstawy roli służb specjalnych w cyberprzestrzeni

Rozważania na temat roli służb specjalnych w cyberprzestrzeni warto poprzedzić wprowadzeniem teoretycznym wyjaśniającym główne pojęcia występujące w pracy:

Służby specjalne: pojęcie, które można rozumieć wąsko: jako służby cywilne i wojskowe organizujące i prowadzące działania wywiadowcze i kontrwywiadowcze [Słownik terminów, 2002, s. 118]. W literaturze definicję przytacza Jerzy Gryz, według którego służby specjalne to usytuowane w strukturze aparatu państwowego samodzielne organizacyjnie lub wchodzące w skład innej jednostki państwowej instytucje uprawnione do prowadzenia działań o charakterze tajnym, z wykorzystaniem metod operacyjnych naruszających prawa i wolności osobiste [Gryz, 2012, s. 77]. Z kolei Sławomir Zalewski definiuje służby specjalne jako zorganizowane zazwyczaj przez państwo struktury, ukierunkowane na niejawne pozyskiwanie informacji, istotnych z punktu widzenia bezpieczeństwa organizatora tej działalności (państwa) bądź przeciwdziałanie ich zdobywaniu przez podobne struktury, identyfikowane jako obce [Zalewski, 2005, s. 34].

Wywiad/kontrwywiad: zgodnie ze słownikiem PWN: wywiad to działalność i instytucja pozyskująca tajne informacje; kontrwywiad – działania zmierzające do zwalczania obcego wywiadu oraz ochrony tajemnic [PWN b.r.].

Cyberbezpieczeństwo: zgodnie z definicją ENISA i prawem UE to działania niezbędne do ochrony sieci i systemów oraz użytkowników przed cyberzagrożeniami [ENISA 2025; Regulation (EU) 2019/881]. \

3. Ewolucja zagrożeń cyfrowych w Europie (2000–2025)

3.1 Wczesne lata 2000 – pierwsze masowe incydenty i reakcje

Okres początku lat 2000 charakteryzował się masowymi incydentami – dominowały szybko rozprzestrzeniające się wirusy i robaki komputerowe, takie jak robak ILOVEYOU z maja 2000 roku, które powodowały globalne straty finansowe i zakłócenia w sieciach [Haertle, 2012] oraz pierwsze działania „hacktywistyczne". Przełomem były ataki DDoS na Estonię (2007) – uznawanego za pierwszy w historii masowy cyberatak na skalę państwa. Atak

na kilkanaście dni sparaliżował funkcjonowanie kluczowych usług online. Serwery estońskich instytucji rządowych, banków i mediów zostały przeciążone, co zmusiło do czasowego wyłączenia witryn internetowych, a nawet zakłóciło działanie numeru alarmowego [Ottis, 2008]. Cyberatak na Estonię stał się sygnałem alarmowym dla Europy, uświadamiając realność cyberwojny i podatność infrastruktury teleinformatycznej państw na celowe działania destabilizacyjne. Kontynuacją tego trendu była kampania w czasie konfliktu w Gruzji (2008), która również unaoczniła podatność usług publicznych i krytycznej infrastruktury [ENISA, 2022]. Reakcją na rosnące zagrożenia w cyberprzestrzeni były pierwsze inicjatywy instytucjonalne na poziomie europejskim. Już w 2004 r., a więc przed incydentem estońskim, Unia Europejska utworzyła Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA), której zadaniem stało się wzmocnienie ogólnego poziomu bezpieczeństwa teleinformatycznego w Europie. ENISA zajęła się doradztwem, szkoleniami i analizą zagrożeń, wspierając państwa członkowskie w budowaniu strategii ochrony przed cyberatakami.

3.2 Lata 2010–2020 – nowe typologie zagrożeń

Druga dekada XXI wieku przyniosła istotną ewolucję zagrożeń cyfrowych – od pojedynczych ataków hakerskich do zaawansowanych kampanii cybernetycznych prowadzonych przez grupy przestępcze sponsorowane przez państwa. W latach 2010–2015 nastąpił gwałtowny wzrost ataków typu APT (Advanced Persistent Threat), czyli długotrwałych, skomplikowanych operacji cyberszpiegowskich. Ich celem stały się rządy, instytucje UE oraz europejski sektor przemysłowy. Równolegle rozwinęło się zjawisko *hacktywizmu* - grupa Anonymous i inne kolektywy hakerskie dokonywały głośnych włamań w ramach ideologicznych protestów (np. ujawnienie danych organizacji rządowych czy korporacji [De Marignan, 2017]). W 2010 r. portal WikiLeaks opublikował setki tysięcy poufnych depesz dyplomatycznych USA, co uwidoczniło moc oddziaływania wycieku informacji w erze cyfrowej. Incydent ten, choć nie był klasycznym „atakiem", lecz przeciekiem, wpłynął

na podejście państw do ochrony informacji i kontroli dostępu. Od około 2013 r. na znaczeniu zaczęło zyskiwać złośliwe oprogramowanie wymuszające okup – ransomware. Początkowo wymierzone w pojedynczych użytkowników, a z czasem w całe przedsiębiorstwa i instytucje. W maju 2017 doszło do jednego z najgłośniejszych ataków ransomware – WannaCry, który zainfekował setki tysięcy komputerów w około 150 krajach, szyfrując dane i żądając okupu. W Europie szczególnie dotkliwie odczuła to Wielka Brytania – atak sparaliżował działanie systemu opieki zdrowotnej NHS, zmuszając szpitale do odwoływania zabiegów [Alraddadi i Sarvotham, 2018]. Europol określił skalę WannaCry jako bezprecedensową. W czerwcu 2017 nastąpił kolejny potężny atak ransomware NotPetya, początkowo wymierzony w Ukrainę, lecz wskutek globalnego łańcucha dostaw uderzył też w wiele europejskich firm.

Rok 2017 stał się punktem zwrotnym, seria głośnych cyberataków zwróciła uwagę opinii publicznej i decydentów na kwestie cyberbezpieczeństwa w niespotykanym dotąd stopniu [Mortera -Martinez, 2018]. Celem ataków stawały się już nie tylko systemy informatyczne firm, ale krytyczna infrastruktura państw oraz procesy demokratyczne. Znaczącym zjawiskiem stały się próby ingerencji w procesy polityczne za pomocą cyberataków i kampanii dezinformacji. Głośnym echem odbiły się ataki podczas kampanii wyborczych – np. w 2016 r. wyciekły e-maile sztabu wyborczego Hillary Clinton (co, według służb USA, było częścią operacji rosyjskiego wywiadu), zaś w 2017 r. podobny los spotkał sztab Emmanuela Macrona we Francji [Chrisafis, 2025]. Tuż przed drugą turą wyborów prezydenckich we Francji ujawniono w internecie skradzione dokumenty i korespondencję ruchu En Marche, co uznano za próbę destabilizacji demokracji na wzór wcześniejszej operacji w USA. Choć francuscy wyborcy okazali odporność na tę manipulację informacyjną (incydent nazwany *Macron Leaks* nie wpłynął znacząco na wynik wyborów), stało się jasne, że cyberprzestrzeń stała się areną walki informacyjnej prowadzonej przez wrogie podmioty. Państwa europejskie zaczęły wówczas rozwijać mechanizmy przeciwdziałania kampaniom dezinformacyjnym oraz doskonalić systemy ochrony infrastruktury wyborczej.

W odpowiedzi na intensyfikację zagrożeń w latach 2010–2020, Unia Europejska zacieśniła współpracę i zainicjowała nowe ramy prawne w dziedzinie cyberbezpieczeństwa. W 2013 r. przyjęto pierwszą unijną Strategię cyberbezpieczeństwa UE (European Union, 2013), a w 2016 r. uchwalono Dyrektywę NIS (Network and Information Security Directive) – pierwszy akt prawny zobowiązujący państwa UE do zapewnienia minimalnych standardów bezpieczeństwa sieci i informacji oraz do ustanowienia krajowych CSIRT-ów (zespołów reagowania na incydenty komputerowe). Z kolei w 2019 r. UE wzmocniła mandat ENISA, przyjmując tzw. Akt o cyberbezpieczeństwie (Cybersecurity Act) – na mocy Rozporządzenia ENISA zyskała status stałej agencji UE o rozszerzonych kompetencjach, m.in. w zakresie certyfikacji bezpieczeństwa produktów ICT [Regulation (EU) 2019/881, 2019].

3.3 Lata 2020–2025 – nowe wyzwania: pandemia i cyberwojna

Najnowsze lata przyniosły dalsze zmiany w krajobrazie zagrożeń cyberprzestrzeni w Europie, głównie za sprawą globalnej pandemii oraz zaostrzenia konfrontacji geopolitycznych. Pandemia COVID-19 spowodowała nagłe przeniesienie wielu aspektów życia do sfery online. Na skutek czego odnotowano gwałtowny wzrost ataków phishingowych i kampanii malware. Europol raportował, że w okresie pandemii przestępcy eksploatowali lęk i dezinformację związaną z koronawirusem – phishing z motywem COVID-19 oraz oszustwa internetowe (fałszywe sklepy ze środkami medycznymi, wyłudzanie danych logowania do kont bankowych) stały się powszechne [Europol, 2021]. Rozproszenie infrastruktury IT (praca z domu) zwiększyło też podatność na ataki – firmy często musiały rozluźnić polityki bezpieczeństwa, by umożliwić zdalny dostęp, co tworzyło nowe luki [Europol, 2021]. Jednak najpoważniejszym katalizatorem zmian w cyberzagrożeniach ostatnich lat stała się wojna rosyjsko-ukraińska rozpoczęta w lutym 2022 roku. Po raz pierwszy w historii Europy pełnoskalowemu konfliktowi zbrojnemu towarzyszyły zakrojone na szeroką skalę operacje w cyberprzestrzeni. Już w pierwszym dniu inwazji na

Ukrainę doszło do cyberataku na sieć satelitarną Viasat, który zakłócił łączność również w innych krajach Europy [Rzeczpospolita Cyfrowa, 2022]. W kolejnych miesiącach prorosyjskie grupy (takie jak *Killnet*) przeprowadziły szereg ataków DDoS wymierzonych w strony rządowe i infrastrukturę informatyczną państw wspierających Ukrainę – ofiarami krótkotrwałych paraliżów padły instytucje we Włoszech, Polsce, krajach bałtyckich. ENISA w swoim najnowszym raporcie zauważa, że obecny kontekst geopolityczny stał się czynnikiem zmieniającym reguły gry w cyberprzestrzeni – wojna na Ukrainie doprowadziła do wzrostu znaczenia cyberwojny i zjawiska zorganizowanego haktywizmu po obu stronach konfliktu [ENISA, 2022].

Na szczeblu unijnym ostatnie lata przyniosły ważne reformy wzmacniające odporność Europy na zagrożenia cyfrowe. W grudniu 2020 r. Komisja Europejska ogłosiła nową Strategię UE w zakresie cyberbezpieczeństwa, przewidującą m.in. utworzenie sieci centrów operacji bezpieczeństwa (SOC) i zwiększenie inwestycji w technologie ochronne. W 2022 r. przyjęto natomiast Dyrektywę NIS 2, rozszerzającą zakres obowiązków w zakresie cyberbezpieczeństwa na większą liczbę sektorów i zaostrzającą wymagania względem podmiotów krytycznych.

Podsumowując, w latach 2000–2025 nastąpiła wyraźna ewolucja zagrożeń cyfrowych w Europie – od prostych wirusów i incydentalnych włamań po wyrafinowane ataki o charakterze globalnym, stanowiące element rywalizacji geopolitycznej. Państwa europejskie i instytucje unijne stopniowo rozwijały środki zaradcze – od powołania agencji takich jak ENISA czy EC3, przez przyjmowanie regulacji (dyrektywy NIS/NIS2, Cybersecurity Act), aż po implementację środków dyplomatycznych (sankcje) i budowę wspólnych zdolności obronnych. Mimo tych wysiłków, poziom zagrożenia cyberbezpieczeństwa dla Europy pozostaje wysoki, a skuteczna ochrona wymaga ciągłej adaptacji do dynamicznie zmieniających się metod działania agresorów. Można jednak zauważyć rosnącą dojrzałość struktur bezpieczeństwa cybernetycznego w Europie – zwiększoną świadomość zagrożeń, lepszą koordynację między państwami oraz inwestycje w rozwój

technologiczny, co łącznie wpływa na stopniowe umacnianie cyberodporności Unii Europejskiej.

4. Wpływ służb specjalnych na krajowe strategię cyberbezpieczeństwa państw europejskich

Współczesne zagrożenia cybernetyczne charakteryzują się coraz większą złożonością i międzynarodowym zasięgiem, co wymaga od państw europejskich opracowania kompleksowych strategii cyberbezpieczeństwa. Służby specjalne odgrywają kluczową rolę w procesie kształtowania narodowych polityk cyberbezpieczeństwa, łącząc funkcje wywiadowcze, obronne i ofensywne w cyberprzestrzeni. Analiza modeli legislacyjnych oraz przypadków z wybranych państw europejskich pozwala na zidentyfikowanie odmiennych praktyk i tendencji w zakresie integracji służb specjalnych z systemami cyberbezpieczeństwa narodowego.

4.1 Model brytyjski – zintegrowane podejście do cyber power

Wielka Brytania opracowała jeden z najbardziej zaawansowanych modeli integracji służb specjalnych z narodową strategią cyberbezpieczeństwa. Realizując wizję „leading responsible and democratic cyber power" w *National Cyber Strategy 2022*, opartą m.in. na wzmocnieniu odporności, przewodzeniu w technologiach oraz wykrywaniu i zakłócaniu działań przeciwników [Great Britain – GCHQ, 2022]. Kluczową innowacją jest National Cyber Force – partnerstwo obrony i wywiadu prowadzące operacje w i poprzez cyberprzestrzeń [Great Britain – NCF 2023]. Operacje nadzorowane są politycznie, a ramy prawne tworzą m.in. Investigatory Powers Act 2016 (mechanizm „podwójnej blokady" decyzji) oraz Product Security and Telecommunications Infrastructure Act 2022 (obowiązki bezpieczeństwa dla IoT) [Investigatory Powers Act 2016; PSTI Act 2022].

4.2 Model norweski – wieloinstytucjonalne zarządzanie cyberbezpieczeństwem

NSM (National Security Authority), utworzona w 2003 roku jako następca Forsvarets sikkerhetsstab, pełni funkcję centralnej agencji odpowiedzialnej za bezpieczeństwo narodowe oraz kwestie bezpieczeństwa ICT, w tym krajowy zespół reagowania na incydenty komputerowe (NorCERT). Agencja współpracuje ściśle z Norwegian Intelligence Service (NIS) w zakresie analizy zagrożeń na poziomie narodowym. Kluczowym elementem współpracy jest Joint Cyber Coordination Centre (FCKS), które obejmuje przedstawicieli czterech agencji: NSM (Norweski Urząd ds. Bezpieczeństwa Narodowego), Państwowa Służba Śledcza (National Criminal Investigation Service, Kripos, Norweska Służba Bezpieczeństwa Policji (Politiets sikkerhetstjeneste, PST) oraz wcześniej wspomnianą Służbę Wywiadowczą (Norwegian Intelligence Service), mając za zadanie poprawę krajowej zdolności do wykrywania i przeciwstawiania się poważnym cyberatakom.

National Cyber Security Strategy for Norway opiera się na pięciu celach strategicznych: bezpieczna cyfryzacja przedsiębiorstw, solidna infrastruktura cyfrowa dla funkcji krytycznych, rozwój kompetencji cyberbezpieczeństwa, poprawa zdolności wykrywania i reagowania na cyberataki oraz wzmocnienie zdolności policji w zwalczaniu cyberprzestępczości [Norway, 2019], Norweski Security Act z 2019 roku rozszerzył zakres zastosowania przepisów bezpieczeństwa ze względu na rosnące współzależności między granicami cywilno-wojskowymi oraz publiczno-prywatnymi, nakładając wymogi zabezpieczenia wszystkich systemów informacyjnych zawierających informacje wymagające ochrony, nie tylko tych używanych do przetwarzania informacji niejawnych. Nowe regulacje znacznie wzmocniły rolę norweskich służb specjalnych w cyberprzestrzeni. Otrzymały one rozszerzone kompetencje kontrolne, a współpraca między NSM, PST została zinstytucjonalizowana, zwiększono nacisk na wykrywanie operacji wywiadowczych w cyberprzestrzeni oraz wzmocniono narodową

kontrolę nad krytycznymi usługami ICT jako elementem suwerenności cyfrowej.

4.3 Model szwajcarski – federalne podejście do cyberobrony

Szwajcaria, zachowując neutralność polityczną, opracowała własny model cyberbezpieczeństwa. Swiss Federal Council przyjął w 2018 roku National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018-2022 [Switzerland, Federal Department of Finance, 2018], którą implementuje National Cybersecurity Centre (NCSC). Strategia opiera się na czterech celach strategicznych: Building capabilities and knowledge […], Building processes, structures and foundations […], Focus on the protection of critical infrastructures […], Strengthening cooperation with third parties. [Switzerland, Federal Department of Finance, 2018]

W odpowiedzi na zmieniające się zagrożenia, Szwajcaria przyjęła Security Strategy 2025 [The Swiss Federal Counci, 2025], która priorytetyzuje cyberobronność oraz współpracę z NATO i krajami sąsiednimi. Strategia ma na celu zmniejszenie podatności na ataki hybrydowe, operacje wpływu, dezinformację i sabotaż przy jednoczesnym zachowaniu zobowiązań neutralności.

5. Analiza porównawcza

Porównanie trzech modeli ujawnia różne podejścia do integracji służb specjalnych z systemami cyberbezpieczeństwa. Model brytyjski charakteryzuje się najwyższym stopniem centralizacji i integracji wszystkich zdolności cybernetycznych pod jednolitym dowództwem, gdzie National Cyber Force (NCF) współpracuje bezpośrednio z GCHQ, MI5 i MI6 w ramach skoordynowanej struktury operacyjnej. Model norweski opiera się na współpracy międzyinstytucjonalnej z wyraźnym podziałem kompetencji między agencjami, gdzie Norwegian National Security Authority (NSM) koordynuje działania z Police Security Service (PST) i Norwegian Intelligence Service (NIS) przy zachowaniu wyraźnego

rozgraniczenia ról. Model szwajcarski uwzględnia specyfikę federalną państwa oraz wymogi neutralności politycznej, gdzie National Cyber Security Centre (NCSC) działa w zdecentralizowanej strukturze respektującej autonomię kantonów. Wszystkie trzy modele podkreślają znaczenie współpracy publiczno-prywatnej oraz międzynarodowej kooperacji w dziedzinie cyberbezpieczeństwa, jednak różnią się fundamentalnie w sposobach implementacji tych założeń. Różnice dotyczą stopnia centralizacji struktur, zakresu uprawnień służb specjalnych oraz podejścia do operacji ofensywnych w cyberprzestrzeni. Model brytyjski reprezentuje najbardziej agresywne podejście do cyberbezpieczeństwa z otwartymi zdolnościami ofensywnymi, podczas gdy model norweski koncentruje się na obronie infrastruktury krytycznej, a szwajcarski balansuje między neutralnością polityczną a szeroką współpracą wywiadowczą. Brytyjski Investigatory Powers Act z 2016 roku zapewnia służbom najszersze uprawnienia „bulk powers" umożliwiające masowe gromadzenie danych, podczas gdy norweski Security Act z 2019 roku kładzie nacisk na współpracę międzysektorową i zarządzanie ryzykiem. Szwajcarski Federal Information Security Act z 2024 roku wprowadza obowiązki raportowania przy zachowaniu federalnej struktury odpowiedzialności, co odzwierciedla unikalne podejście każdego z państw do równoważenia potrzeb bezpieczeństwa z ochroną praw obywatelskich i specyfiką ustrojową. Kluczowe różnice uwidaczniają się również w podejściu do operacji ofensywnych, gdzie Wielka Brytania otwarcie rozwija zdolności poprzez NCF, Norwegia ogranicza się głównie do działań defensywnych i wywiadowczych, a Szwajcaria oficjalnie zachowuje neutralność przy jednoczesnym utrzymywaniu szerokich kontaktów wywiadowczych z agencjami partnerskimi. Owe różnice w podejściach odzwierciedlają nie tylko odmienne tradycje polityczne i prawne, ale również różne postrzeganie zagrożeń cybernetycznych i roli państwa w ich neutralizacji, co prowadzi do powstania trzech odrębnych, ale komplementarnych przykładowych modeli zarządzania cyberbezpieczeństwem w Europie.

6. Studium przypadku: GCHQ i National Cyber Force (UK)

Government Communications Headquarters (GCHQ) odegrało kluczową rolę w opracowaniu i implementacji National Cyber Strategy 2022, wykorzystując swoje doświadczenie jako agencja wywiadowcza i cyberbezpieczeństwa specjalizująca się w signals intelligence (SIGINT). Utworzone w 1946 roku GCHQ pomyślnie dostosowało swoje zdolności do wymogów współczesnej cyberprzestrzeni. Proces opracowania strategii charakteryzował się ścisłą współpracą między GCHQ a National Cyber Security Centre (NCSC), które zostało utworzone w 2016 roku jako integralny element GCHQ. NCSC pełni funkcję centralnego punktu doradztwa i wsparcia w zakresie cyberbezpieczeństwa, w tym zarządzania incydentami cybernetycznymi. Utworzenie NCSC stanowiło pierwszą tego typu inicjatywę na świecie, łączącą rząd, agencje wywiadowcze i sektor prywatny w jednej organizacji.

GCHQ wniosło do procesu strategicznego swoją wiedzę w zakresie analizy zagrożeń, zdolności technicznych oraz współpracy międzynarodowej w ramach sojuszu Five Eyes Intelligence Oversight and Review Council (*FIORC is composed of the following non-political intelligence oversight, review, and security entities of Australia, Canada, New Zealand, the United Kingdom, and the United States*) [United States Office of the Director of National Intelligence, b.d.] Agencja wykorzystała swoje doświadczenie w wykrywaniu, atrybucji i przeciwdziałaniu złośliwej aktywności cybernetycznej, co znalazło odzwierciedlenie w piątym filarze strategii dotyczącym wykrywania, zakłócania i odstraszania przeciwników.

6.1 Integracja zdolności obronnych i ofensywnych

Jednym z najważniejszych wkładów GCHQ w National Cyber Strategy było zdefiniowanie roli National Cyber Force jako podmiotu odpowiedzialnego za operacje ofensywne w cyberprzestrzeni. NCF została utworzona w 2020 roku jako partnerstwo między obronnością a wywiadem, łączące elementy GCHQ,

Ministerstwa Obrony, Secret Intelligence Service oraz Defence Science and Technology Laboratory. GCHQ opracowało zasady etyczne i prawne regulujące działania ofensywne NCF, które zostały przedstawione w dokumencie „Responsible Cyber Power in Practice" [National Cyber Force, The National Cyber Force, 2023] Dokument ten po raz pierwszy publicznie ujawnił zasady rządzące brytyjskimi operacjami ofensywnymi w cyberprzestrzeni, określając je jako „accountable", „precise" i „calibrated". Zasady opracowane przez GCHQ obejmują minimalizację szkód ubocznych, proporcjonalność działań oraz zgodność z prawem międzynarodowym.

6.2 Współpraca międzynarodowa i wpływ na politykę europejską

GCHQ odegrało znaczącą rolę w kształtowaniu międzynarodowego wymiaru National Cyber Strategy 2022 poprzez swoją pozycję w sojuszu Five Eyes oraz współpracę z partnerami europejskimi. Strategia przewiduje utworzenie formalnych dialogów cybernetycznych z Unią Europejską oraz współpracę z organizacjami światowymi:

> *And we will continue to work with effective multilateral organisations and partnerships including the United Nations, Five Eyes, NATO, G7, European Union, Commonwealth, OECD, Global Forum on Cyber Expertise (GFCE), ASEAN Forum, African Union and the World Bank [Great Britain, Government Communications Headquarters, 2022]*

Agencja wspierała rozwój zdolności cybernetycznych NATO, w tym wzmocnioną integrację cywilno-wojskową w cyberobronie oraz uruchomienie mechanizmu koordynacji zdolności reagowania na incydenty. GCHQ wniosło również wkład w rozwój europejskich standardów certyfikacji bezpieczeństwa ICT oraz promowanie zastosowań komunikacji kwantowej.

6.3 Działania ofensywne w cyberprzestrzeni – doktryna i praktyka

National Cyber Force, działając pod kierownictwem GCHQ, opracowało kompleksową doktrynę operacji ofensywnych w cyberprzestrzeni. Zgodnie z opublikowanymi zasadami, operacje NCF mają charakter ukryty z intencją, aby przeciwnicy często nie zdawali sobie sprawy, że doświadczane przez nich efekty są wynikiem operacji cybernetycznej.

GCHQ zdefiniowało trzy główne zalety operacji ofensywnych: podważanie zdolności przeciwnika, precyzyjna i ukierunkowana interwencje, tworzenie efektów kognitywnych.

> *They can sometimes provide the only practical means of disrupting an adversary's ability to exploit the internet and digital technology. They can be precisely targeted with specific effect and can avoid the challenges of using other, potentially physically destructive, interventions. They can create a range of cognitive effects – such as undermining an adversary's confidence in the data they are receiving or in the ability of their information systems to function effectively [...] [United Kingdom, HM Governmen, 2023]*

NCF prowadzi operacje obejmujące pełen zakres priorytetów bezpieczeństwa narodowego Wielkiej Brytanii, od zwalczania poważnej przestępczości, międzynarodowego terroryzmu i złośliwej aktywności państw, po przygotowania do wojny. W przeciwieństwie do na przykład modelu amerykańskiego, brytyjskie podejście integruje zdolności ofensywne wszystkich agencji w jednej organizacji, co w amerykańskich kategoriach odpowiadałoby połączeniu ofensywnych zdolności cybernetycznych Cyber Command, National Security Agency, Central Intelligence Agency i Federal Bureau of Investigation.

7. Podsumowanie

Porównanie modeli Wielkie Brytani, Norwegii oraz Szwajcarii sugeruje, że spójność dowodzenia (UK) ułatwia szybkie reagowanie i prowadzenie operacji ofensywnych, lecz wymaga silnych gwarancji nadzoru (np. *doublelock* IPA 2016). Modele zdecentralizowane (Norwegia, Szwajcaria) zwiększają odporność sieciową i integrację sektora prywatnego, ale mogą spowalniać decyzje w kryzysie transgranicznym [Investigatory Powers Act 2016; Norway MoJ 2019; Swiss Federal Council 2025]. W perspektywie UE NIS2 wzmacnia minimalne standardy i obowiązki raportowe [Directive 2022/2555; European Commission 2020], lecz praktyczna interoperacyjność i atrybucja nadal wymagają pogłębionej koordynacji.

8. Zakończenie

W świetle przeprowadzonych analiz służby specjalne jawią się jako kluczowy węzeł europejskiego ekosystemu cyberbezpieczeństwa, łączący kompetencje rozpoznawcze, kontrwywiadowcze, defensywne i ofensywne z rosnącym potencjałem regulacyjnym i dyplomatycznym. Wspólna ścieżka rozwoju unijnych ram prawnych – od pierwszej Strategii cyberbezpieczeństwa UE, przez dyrektywy NIS i NIS 2, aż po wzmocnienie mandatu ENISA – udowadnia, że harmonizacja standardów pozostaje niezbędnym warunkiem budowania odporności w cyberprzestrzeni. Jednocześnie studium przypadków Wielkiej Brytanii, Norwegii i Szwajcarii pokazuje, iż różnice konstytucyjne, kulturowe i geopolityczne kształtują odmienne modele udziału służb specjalnych w ochronie domeny cyfrowej. Najbardziej scentralizowany model brytyjski, zwieńczony powołaniem National Cyber Force, potwierdza tezę, że koncentracja zdolności w jednej strukturze sprzyja szybkości i spójności reakcji na incydenty, ale równocześnie generuje największe wyzwania z punktu widzenia kontroli demokratycznej. Norwegia – korzystająca z rozproszonego systemu

koordynowanego przez National Security Authority – ilustruje, że efektywna obrona może wynikać także z modelu sieciowego, opartego na ścisłej współpracy służb z policją i sektorem prywatnym. Szwajcarska koncepcja z kolei podkreśla, iż nawet w warunkach neutralności możliwe jest utrzymanie aktywnej polityki wywiadowczej i partnerskiej, niezbędnej do minimalizowania rosnących zagrożeń transgranicznych.

Bibliografia

Akt o cyberbezpieczeństwie – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013. Dz.U. L 151, 07.06.2019.

Alraddadi, W., i H. Sarvotham. „Session III Report 3". https://peopleece.vse.gmu.edu/coursewebpages/ECE/ECE646/F20/project/F18_presentations/Session_III/Session_III_Report_3.pdf [dostęp: 13 czerwca 2025 r.].

Chrisafis, Angelique. 2025. „France says Russian hackers behind attack on Macron's 2017 presidential campaign". *The Guardian*. https://www.theguardian.com/world/2025/apr/29/france-says-russian-hackers-behind-attack-on-macrons-2017-presidential-campaign [dostęp: 13 czerwca 2025 r.].

Cybersecurity Act – Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013.

Cybersecurity Intelligence. „National Cyber Force (NCF) – UK". *Cybersecurity Intelligence*. https://www.cybersecurityintelligence.com/national-cyber-force-ncf-uk-11483.html [dostęp: 13 czerwca 2025 r.].

De Marignan, Florence. 2017. „Cyberattack: major cyber-attacks over the past 10 years". *Phys.org*. https://phys.org/news/2017-05-cyberattack-major-cyber-years.html#:~:text=A%20similar%20election%20attack%20targeted,movement%20were%20dumped%20online [dostęp: 13 czerwca 2025 r.].

European Union Agency for Cybersecurity (ENISA). 2022. *ENISA Threat Landscape 2022*. https://www.enisa.europa.eu/sites/default/files/

publications/ENISA%20Threat%20Landscape%202022.pdf [dostęp: 13 czerwca 2025 r.].

European Union Agency for Cybersecurity (ENISA). „Who we are". *European Union Agency for Cybersecurity*. https://www.enisa.europa.eu/about-enisa/who-we-we-are [dostęp: 13 czerwca 2025 r.].

European Union, Spójny komunikat do parlamentu europejskiego, rady, europejskiego komitetu ekonomiczno-społecznego i komitetu regionów. 2013. *Strategia bezpieczeństwa cybernetycznego unii europejskiej: otwarta, bezpieczna i chroniona cyberprzestrzeń*. https://eur-lex.europa.eu/legal-content/PL/ALL/?uri=celex:52013JC0001 [dostęp: 13 czerwca 2025 r.].

Europol. 2021. *Internet Organised Crime Threat Assessment (IOCTA) 2021*. Luxembourg: Publications Office of the European Union. https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf [dostęp: 13 czerwca 2025 r.].

Great Britain, Government Communications Headquarters. 2022. *National Cyber Strategy 2022: Making the UK a Global Cyber Power*. London: HMSO. https://assets.publishing.service.gov.uk/media/62b55f128fa8f53579842425/National_Cyber_Strategy_2022_-_GOV.UK.pdf [dostęp: 13 czerwca 2025 r.].

Great Britain, Investigatory Powers Act 2016, (c. 25). 2022. The Stationery Office. https://www.legislation.gov.uk/ukpga/2016/25/contents [dostęp: 13 czerwca 2025 r.].

Great Britain, Parliament. 2022. *Telecommunications Infrastructure Act 2022*. London: The Stationery Office. https://www.legislation.gov.uk/ukpga/2022/46/contents [dostęp: 13 czerwca 2025 r.].

Gryz, Jacek. 2012. „Teoretyczne aspekty funkcjonowania służb specjalnych RP". *Realia i co dalej* nr 1: 77.

Haertle, Adam. „Wiadomości z myszką ILoveYou". *ZaufanaTrzeciaStrona*. https://zaufanatrzeciastrona.pl/post/wiadomosci-z-myszka-iloveyou/ [dostęp: 13 czerwca 2025 r.].

K. Kraj. „Kontrwywiad". *Słownik Społeczny Bezpieczeństwo Publiczne Tom IX: Bezpieczeństwo publiczne*. Instytut Kultury, Ignatianum. https://slownikispoleczne.ignatianum.edu.pl/index.php/ss/catalog/book/307#:~:text=DE-FINICJA%20POJ%C4%98CIA%3A%20Kontrwywiad%20jest%20cz%C4%99%C5%9Bci%C4%85,pa%C5%84stwa%20oraz%20wybrane%20jednostki%20prywatne [dostęp: 13 czerwca 2025 r.].

Mortera-Martinez, Camino. Lipiec 2018. *Game over? Europe's cyber problem*. London: Centre for European Reform. https://www.cer.eu/sites/default/files/cover_pbrief_game_over2_9.7.18.pdf [dostęp: 13 czerwca 2025 r.].

National Cyber Force, The National Cyber Force. 2023. *Responsible Cyber Power in Practice*. Government Communications Headquarters. https://assets.publishing.service.gov.uk/media/642a8886fbe620000c17dabe/Responsible_Cyber_Power_in_Practice.pdf [dostęp: 13 czerwca 2025 r.].

Norway, Ministry of Justice and Public Security. 2019. *National Cyber Security Strategy for Norway.* Oslo: Norwegian Ministries. https://www.regjeringen.no/contentassets/c57a0733652f47688294934ffd93fc53/national-cyber-security-strategy-for-norway.pdf [dostęp: 13 czerwca 2025 r.].

Ottis, Rain. 2008. *Analysis of the 2007 Cyber Attacks against Estonia from the Information Warfare Perspective*. Tallinn: Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf [dostęp: 13 czerwca 2025 r.].

Rosja zaatakowała łączność satelitarną godzinę przed inwazją na Ukrainę. 2022. *Rzeczpospolita Cyfrowa*. https://cyfrowa.rp.pl/bezpieczenstwo/art36270381-rosja-zaatakowala-lacznosc-satelitarna-godzine-przed-inwazja-na-ukraine [dostęp: 13 czerwca 2025 r.].

Shakarian, Paulo. 2011. „The Criticality of Captains' Education: Now and in the Future". *Military Review* 91, nr 6: 63–68. https://www.armyupress.army.mil/Portals/7/militaryreview/Archives/English/MilitaryReview_20111231_art013.pdf [dostęp: 13 czerwca 2025 r.].

Słownik terminów z zakresu bezpieczeństwa narodowego. 2002. *Myśl Wojskowa* nr 6: 118.

Switzerland, Federal Department of Finance. 2018. *National Strategy for the Protection of Switzerland against Cyber Risks (NCS) 2018–2022*. Federal Department of Finance.

The Swiss Federal Council. *Digital Switzerland Strategy 2025*. https://digital.swiss/userdata/uploads/strategie-dch-en.pdf [dostęp: 13 czerwca 2025 r.].

United Kingdom, National Cyber Force. 2023. *Responsible Cyber Power in Practice*. HM Government. https://www.gov.uk/government/publications/responsible-cyber-power-in-practice/responsible-cyber-power-inpractice-html [dostęp: 13 czerwca 2025 r.].

United States, Office of the Director of National Intelligence. „Five Eyes Intelligence Oversight and Review Council". *Office of the Director of National Intelligence*. https://www.dni.gov/index.php/ncsc-how-we-work/217-about/organization/icig-pages/2660-icig-fiorc [dostęp: 13 czerwca 2025 r.].

Zalewski, s. 2005. *Służby specjalne w państwie demokratycznym*. Warszawa.