Bank i Kredyt 53(4), 2022, 357-374

BANK I KREDYT
BANK & CREDIT

Cyberbezpieczeństwo systemu płatniczego w nadzorze systemowym Narodowego Banku Polskiego

Katarzyna Dmowska*

Nadesłany: 9 lutego 2021 r. Zaakceptowany: 16 maja 2022 r.

Streszczenie

Problem cyberodporności i ściśle z nią związane zapewnianie cyberbezpieczeństwa zajmują coraz ważniejsze miejsce w działaniach europejskich i krajowych organów sprawujących nadzór systemowy (*oversight*) nad infrastrukturą systemu płatniczego. Celem opracowania jest zestawienie obserwowanego stanu cyberodporności polskiego systemu płatniczego ze stanem normatywnie postulowanym i jego rewizja na podstawie analizy narzędzi mających zastosowanie w polskim nadzorze systemowym sprawowanym przez Prezesa Narodowego Banku Polskiego.

Tezę, że Narodowy Bank Polski ma odpowiednie narzędzia nadzorcze służące zapewnieniu wystarczającego poziomu cyberodporności nadzorowanych elementów systemu płatniczego, potwierdza analiza obowiązujących regulacji systemu płatniczego. Odzwierciedleniem prawidłowego stanu regulacyjnego jest przede wszystkim rzeczywiste funkcjonowanie systemów, schematów i usług składających się na system płatniczy. Prawidłowość rozwiązań z zakresu cyberbezpieczeństwa w nadzorowanej poprzez *oversight* infrastrukturze systemu płatniczego w szerszej perspektywie znajduje także potwierdzenie w niezakłóconym organizowaniu rozliczeń pieniężnych oraz obserwowanej stabilności krajowego systemu finansowego jako całości, co stanowi realizację ustawowych zadań banku centralnego.

Słowa kluczowe: nadzór systemowy, *oversight*, cyberbezpieczeństwo, system płatniczy, CROE

JEL: K24, E42, E58

* Współpracownik Katedry Prawa Informatycznego Uniwersytetu Kardynała Stefana Wyszyńskiego w Warszawie; e-mail: kddmowska@gmail.com, ORCID: 0000-0002-4636-856X.

1. Wstęp

Niniejsze opracowanie zawiera w głównej mierze zestawienie i analizę uregulowań w zakresie cyberbezpieczeństwa w nadzorze systemowym (*oversight*) sprawowanym nad polskim systemem płatniczym przez Prezesa Narodowego Banku Polskiego (NBP). Działania te mają na celu weryfikację prawidłowości rozwiązań przyjętych w tej materii. Jak wskazuje dotychczasowe działanie polskiego systemu płatniczego, można ocenić, że pozwalają one zapewnić wysoki stan cyberodporności jego infrastruktury. Artykuł opiera się na analizie obowiązujących aktów prawnych, międzynarodowych regulacji i standardów cyberbezpieczeństwa oraz literatury przedmiotu. Analizę poprzedzono syntetyczną charakterystyką struktury nadzoru nad systemem finansowym w Polsce.

2. Nadzór nad polskim systemem finansowym

Bank centralny jest jednym z podmiotów odpowiedzialnych m.in. za sprawowanie nadzoru makroostrożnościowego, koncentrującego się na zapewnieniu stabilności całego systemu finansowego lub jego istotnej części. Nadzór ten bezpośrednio leży w gestii Komitetu Stabilności Finansowej (KSF), będącego organem współtworzonym i obsługiwanym przez NBP oraz urząd obsługujący Ministra Finansów (Prezes NBP jest przewodniczącym KSF w zakresie zadań Komitetu dotyczących nadzoru makroostrożnościowego). Nadzór mikroostrożnościowy nad sektorem bankowym (koncentrujący się na ocenie stabilności pojedynczego podmiotu) został natomiast wyodrębniony z banku centralnego i przejęty przez Komisję Nadzoru Finansowego (KNF). Jest to zgodne z obowiązującym w Polsce tzw. modelem nadzoru zintegrowanego. Działania nadzorcze KNF są nadzorem typu ostrożnościowego (ang. *supervision*), definiowanym jako nadzór obejmujący ogólny, ciągły przegląd działań poszczególnych instytucji i całej branży w celu zapewnienia ich zgodności z prawem. Sprawowanie nadzoru ostrożnościowego związane jest również z przeprowadzaniem szczegółowych kontroli w nadzorowanych instytucjach oraz z ich krytyczną oceną.

Polski nadzór systemowy (*oversight*) sprawowany przez Prezesa NBP – będącego organem Narodowego Banku Polskiego – wynika pośrednio z art. 3 ust. 2 pkt 1 i 6a Ustawy z dnia 29 sierpnia 1997 r. o Narodowym Banku Polskim (Dz. U. z 2020 r. poz. 2027), czyli z zadań NBP, do których należy m.in. organizowanie rozliczeń pieniężnych i działanie na rzecz stabilności krajowego systemu finansowego. Bezpośrednią podstawą jego sprawowania jest art. 3 ust. 2 pkt 8 ustawy o NBP, w którym wskazano, że do zadań NBP należy wykonywanie innych zadań określonych ustawami. Przedmiotem *oversight* jest system płatniczy, czyli „system składający się z określonej grupy instytucji, ustalonych instrumentów i procedur wykorzystywanych do zapewnienia obiegu pieniądza na danym obszarze geograficznym, którym zazwyczaj jest jeden kraj" (NBP 2003, s. 5). W najnowszym opracowaniu NBP w tej materii system płatniczy definiowany jest także jako: „zbiór instrumentów, procedur oraz systemów, umożliwiających cyrkulację pieniądza lub instrumentów finansowych w ramach danego kraju lub obszaru walutowego" (NBP 2020b, s. 16). Co ważne, nadzór systemowy NBP skoncentrowany jest na funkcjonowaniu nadzorowanych przez Prezesa NBP elementów tworzących infrastrukturę polskiego systemu płatniczego: syste-

mów płatności[1], schematów płatniczych[2], systemów rozliczeń i systemów rozrachunku papierów wartościowych[3] oraz na usłudze *acquiring*[4], która jest świadczona przez krajowe instytucje płatnicze. *Oversight* nie skupia się na podmiotach prowadzących te systemy. Celem sprawowania nadzoru systemowego – obok wspomnianego wspierania bezpieczeństwa i sprawności poprzez monitorowanie i ocenę pod kątem przyjętych wymogów oraz inicjowanie koniecznych zmian – jest także zapewnienie zgodności zasad funkcjonowania nadzorowanych elementów infrastruktury systemu płatniczego z przepisami prawa (por. Szpringer 2014, s. 92–93, 138; NBP 2019a, s. 6). W tabeli 1 zawarto krótkie zestawienie odzwierciedlające różnice między nadzorem ostrożnościowym a systemowym.

Tabela 1
Zestawienie różnic między nadzorem ostrożnościowym i systemowym

	Nadzór ostrożnościowy (*supervision*)	**Nadzór systemowy (*oversight*)**
Podmiot sprawujący	bank centralny albo inny państwowy organ nadzoru	bank centralny
Przedmiot	poszczególne instytucje (podmioty tworzące infrastrukturę systemu finansowego oraz elementy nadzorowanej infrastruktury)	elementy infrastruktury systemu płatniczego
Główny cel	zapewnienie prawidłowości funkcjonowania nadzorowanych podmiotów	zapewnienie sprawnego i bezpiecznego funkcjonowania systemu płatniczego
Główna forma działania	szczegółowa weryfikacja spełniania wymogów ostrożnościowych	przeprowadzanie ocen sposobu organizacji i funkcjonowania elementów systemu płatniczego
Podstawa sprawowania	szczegółowe regulacje prawne	regulacje prawne albo przy wykorzystaniu autorytetu banku centralnego

Źródło: opracowanie własne na podstawie materiałów udostępnionych przez Departament Systemu Płatniczego Narodowego Banku Polskiego.

[1] System płatności to podlegające prawu polskiemu prawne powiązania pomiędzy co najmniej trzema instytucjami, w ramach których obowiązują wspólne dla uczestników tego systemu zasady przeprowadzania rozliczeń lub realizacji ich zleceń rozrachunku. Pełną definicję i rodzaje instytucji zawiera Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (Dz. U. z 2019 r. poz. 212).

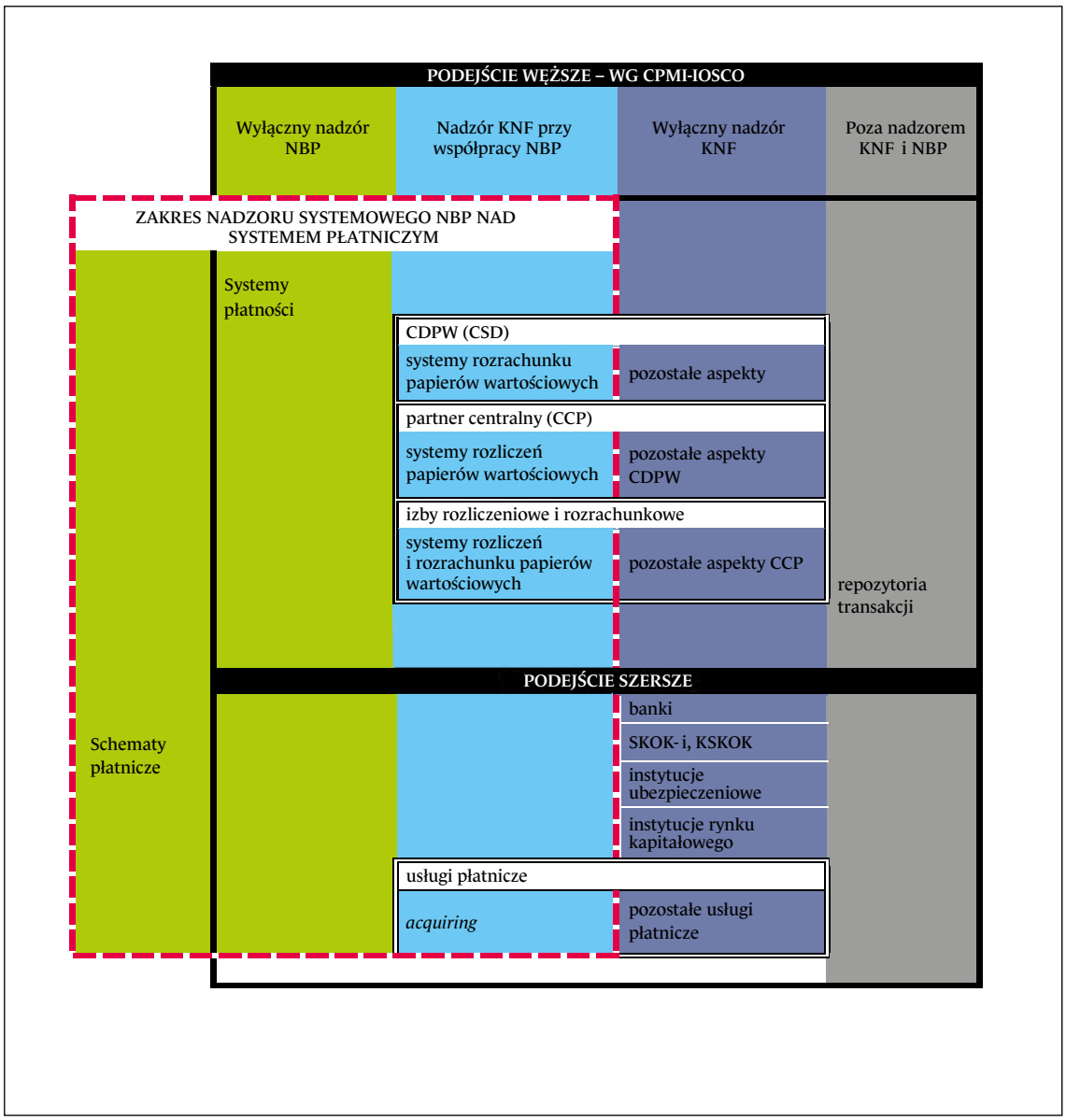
[2] „Schemat płatniczy to zbiór zasad przeprowadzania transakcji płatniczych, wydawania i akceptowania przez dostawców usług płatniczych instrumentów płatniczych i przetwarzania transakcji płatniczych, wykonywanych przy użyciu instrumentów płatniczych oraz system kart płatniczych". (NBP 2018a, s. 8).

[3] „Rozliczenie transakcji w obrocie instrumentami finansowymi jest to zespół czynności dokonywanych po zawarciu transakcji, w ramach którego ustala się wysokość zobowiązań stron transakcji oraz sprawdza dostępność instrumentów finansowych i środków pieniężnych potrzebnych do wypełnienia tych zobowiązań. (…) Rozrachunek (…) jest końcowym etapem procesu wykonywania transakcji. Polega on na przeniesieniu praw z instrumentów finansowych poprzez obciążenie konta strony sprzedającej instrumenty finansowe (zbywcy) oraz uznaniu konta strony kupującej te instrumenty (nabywcy) (…)". (NBP 2018a, s. 10).

[4] „Usługa acquiringu polega na akceptowaniu i przetwarzaniu transakcji płatniczych, wykonywanych przy użyciu instrumentu płatniczego płatnika, w celu dokonania transferu środków pieniężnych do odbiorcy. W szczególności usługa ta polega na obsłudze autoryzacji oraz przesyłaniu zleceń płatniczych do wydawcy karty płatniczej lub systemów płatności". (NBP 2018a, s. 13).

Wobec skomplikowanej i rozbudowanej struktury systemu płatniczego (*vide:* schemat 1), a przede wszystkim jego dynamicznie zmieniającej się formy i wykorzystywania nowych technologii w tworzących go infrastrukturach naturalne jest, że zakresy kompetencyjne nadzorców, tj. NBP i KNF, w niektórych obszarach będą nachodzić na siebie i wymagać współdziałania, również w trybie roboczym, bieżącym (Szpringer 2014, s. 167–168).

Schemat 1
Infrastruktura rynku finansowego a zakres nadzoru systemowego NBP nad systemem płatniczym



Źródło: na podstawie opracowania Departamentu Systemu Płatniczego Narodowego Banku Polskiego.

3. Cyberbezpieczeństwo w nadzorze systemowym

W zależności od jurysdykcji nadzór nad systemem płatniczym i obowiązki krajowego banku centralnego w tym zakresie mogą być jednoznacznie określone w aktach prawa powszechnie obowiązującego w danym kraju lub wynikać „w sposób dorozumiany" z realizacji statutowych zadań banków centralnych, takich jak realizacja polityki pieniężnej czy dbanie o stabilność systemu finansowego. Działania nadzorcze mogą być realizowane nie tylko poprzez ustawowe uprawnienia do egzekwowania decyzji nadzorczych, ale również za pomocą zróżnicowanych narzędzi dostępnych bankom centralnym. Narzędzia te obejmują w szczególności tzw. perswazję moralną (ang. *moral suasion*), czyli wykorzystanie, w celu wprowadzenia określonych zmian, autorytetu banku centralnego jako emitenta waluty czy banku banków (Szpringer 2014, s. 94; ECB 2016, s. 10). Narodowy Bank Polski, będący bankiem centralnym państwa członkowskiego Unii Europejskiej, podlega nie tylko przepisom prawa polskiego, ale także (chociaż w sposób ograniczony ze względu na tzw. derogację) unijnym przepisom i normom wpływającym pośrednio na kształt i funkcjonowanie polskiego systemu płatniczego[5]. Polska w ramach tzw. dobrych praktyk korzysta z rozwiązań zaprojektowanych przez Europejski Bank Centralny (EBC) i inne unijne organy. Robi to, mimo że jako kraj nienależący do strefy euro nie podlega licznym zapisom Traktatu o funkcjonowaniu Unii Europejskiej (Dz. Urz. UE C 326 z 26.10.2012) – między innymi dotyczącym uprawnień EBC czy zadań i uprawnień Europejskiego Systemu Banków Centralnych (ESBC). Należy jednak zauważyć, że niezależnie od podstawy prawnej obowiązków banku centralnego skuteczność nadzoru będzie zależeć od odpowiedniego dopasowania posiadanych w tej materii narzędzi do tych obowiązków, a nie od formy użytych narzędzi.

Ogólnymi kryteriami stosowanymi przez Narodowy Bank Polski w ramach nadzoru systemowego są kryteria sprawności i bezpieczeństwa oraz zgodności z prawem. Kryterium bezpieczeństwa zawiera ocenę cyberbezpieczeństwa. Przez pojęcie cyberbezpieczeństwa (ang. *cybersecurity*) zgodnie z definicją z Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2020 r. poz. 1369, UstKSC) rozumiana jest: „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy". Definicja ta jest bliższa definicji cyberodporności (ang. *cyber resilience*), wywodzącej się z pojęcia odporności operacyjnej, rozumianej najczęściej jako „zdolność organizacji do kontynuowania misji poprzez przewidywanie i dostosowanie się do cyberzagrożeń i innych istotnych zmian w środowisku, oraz do przetrwania, powstrzymania rozprzestrzeniania się i szybkiego odzyskania systemu po wystąpieniu cyberincydentu" (ECB 2018, s. 55). W dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 2016 r., dyrektywa NIS), którą implementuje do polskiego porządku prawnego UstKSC, pojęcie cyberbezpieczeństwa się nie pojawia. Mowa jest za to o „odporności sieci i systemów informatycznych", której definicja jest zbliżona. 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. UE L 151 z 2019 r.), stanowiące tzw. Akt o cyberbezpieczeństwie (ang. The EU

[5] W aneksie zawarto wykaz podstaw prawnych i najważniejszych wytycznych uzupełniających – m.in. standardów i rekomendacji, czyli regulacji z obszaru tzw. miękkiego prawa (ang. *soft law*), stanowiących punkt odniesienia dla sprawowania przez Prezesa NBP nadzoru systemowego.

Cybersecurity Act, CSA), wprowadza do polskiego porządku prawnego kolejną definicję. W rozporządzeniu cyberbezpieczeństwo zdefiniowano jako „działania niezbędne do ochrony sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób przed cyberzagrożeniami" (przez które rozumiane są „wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów informatycznych, użytkowników takich systemów oraz innych osób"). Wobec rozbieżności między terminami pojawiającymi się nie tylko w aktach prawnych, ale także w doktrynie (por. Szpor 2020; Szafrański 2020, s. 175–183), proponujemy, by jako tytułowe „cyberbezpieczeństwo systemu płatniczego" rozumieć działania, których celem jest osiągnięcie jak najwyższego poziomu ochrony sieci i systemów informacyjnych stanowiących komponenty infrastruktury systemu płatniczego, tj. zachowanie poufności, integralności, dostępności i autentyczności przetwarzanych płatności, rozliczeń i rozrachunków lub związanych z nimi danych.

W dokumencie „Zasady dotyczące infrastruktury rynków finansowych" („Principles for financial market infrastructures", PFMIs), opracowanym w 2012 r. przez Komitet ds. Systemów Płatności i Rozrachunku (Committee on Payment and Settlement Systems, CPSS) i Międzynarodową Organizację Komisji Papierów Wartościowych (International Organization of Securities Commissions, IOSCO), przedrostek „cyber" pojawia się jedynie 2 razy, w kontekście cyberataków w zasadzie 17., odnoszącej się do ryzyka operacyjnego. W PFMIs, zawierających standardy stosowane przy dokonywaniu konkretnych ocen nadzorczych przez Narodowy Bank Polski i europejskie banki centralne, uwagę skupiono nie na cyberbezpieczeństwie jako takim, ale na rozpoznaniu ryzyka operacyjnego i zarządzaniu nim w realizacji celu, którym jest „zwiększenie bezpieczeństwa i sprawności realizacji płatności, rozliczeń, rozrachunku i prowadzenia ewidencji, a także ograniczenie ryzyka systemowego i wspieranie przejrzystości i stabilności finansowej" (CPSS-IOSCO 2012, s. 10–11). Zgodnie z komunikatami zawartymi na stronie internetowej NBP ocenie pod kątem PFMIs podlegały m.in. dwa systemowo ważne systemy płatności w złotych:

– wysokokwotowy – system SORBNET2, którego operatorem jest NBP,

– detaliczny – system Elixir, którego operatorem jest Krajowa Izba Rozliczeniowa SA.

Przeprowadzone analizy obu systemów wykazały wysoki poziom zgodności ich działania z PFMIs. Zidentyfikowane uchybienia w opinii oceniających nie powodowały zagrożeń dla stabilności krajowego systemu płatniczego, a w konsekwencji również krajowego systemu finansowego[6]. Obecnie finalizowana jest ocena systemu BlueCash, rozpoczęta w 2020 r. Jest to system płatności natychmiastowych, a jego operatorem jest Blue Media SA.

Dokumentami odnoszącymi się *stricte* do cyberbezpieczeństwa w zakresie sprawowania *oversight* są:

– „Wytyczne w zakresie bezpieczeństwa infrastruktury rynków finansowych w cyberprzestrzeni" („Guidance on cyber resilience in financial market infrastructures", Wytyczne BIS) – autorstwa IOSCO i CPSS, działającego pod zmienioną w 2014 r. nazwą Komitet ds. Płatności i Infrastruktur Rynku (Committee on Payments and Market Infrastructures, CPMI),

– „Wymagania nadzorcze w zakresie odporności cybernetycznej dla infrastruktur rynku finansowego" („Cyber resilience oversight expectations for financial market infrastructures", CROE), będące standardami EBC.

[6] Komunikaty na stronie NBP: https://www.nbp.pl/systemplatniczy/nadzor/ocena-systemu-platnosci-sorbnet2.pdf, https://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2021/ocena-elixir.html.

Wytyczne BIS zostały przyjęte w 2016 r. przez Radę Gubernatorów Banku Rozrachunków Międzynarodowych. Są to pierwsze, uzgodnione na szczeblu międzynarodowym, wytyczne dotyczące cyberbezpieczeństwa sektora finansowego. Stanowią uzupełnienie PFMIs, przede wszystkim w kontekście standardów zarządzania (m.in. systemu kompleksowego zarządzania ryzykiem), ostateczności rozrachunku, ryzyka operacyjnego i połączeń operacyjnych. Zapewniają dodatkowe, bardziej precyzyjne wskazania odnoszące się do przygotowań i środków, które powinny zostać podjęte w celu zwiększenia cyberodporności infrastruktur, a co za tym idzie ograniczenia eskalacji ryzyka dla stabilności finansowej. Wytyczne BIS funkcjonują jako punkt odniesienia dla sprawowanego nadzoru systemowego – od 2017 r. uwzględnia się je w polityce nadzorczej w polskim systemie płatniczym. Są stosowane jako wytyczne uzupełniające i pozostają jedną z podstaw podejmowanych przez Prezesa NBP działań mających na celu zapobieganie cyberzagrożeniom występującym w działalności podmiotów i systemów tworzących infrastrukturę systemu płatniczego. W ramach monitorowania poziomu cyberodporności nadzorowanej infrastruktury Narodowy Bank Polski (w przypadku systemów rozrachunku i rozliczeń papierów wartościowych we współpracy z KNF) już w 2017 r. wziął udział w badaniu ankietowym (Cyber Resilience Survey), koordynowanym przez Europejski Bank Centralny i opartym na standardzie z Wytycznych BIS. Badanie to zawierało noty objaśniające oraz 32 pytania i objęło wiele czynności. W pierwszej kolejności operatorzy nadzorowanych systemów zostali zobligowani do samooceny i wypełnienia formularza ankietowego. Uzupełniony formularz posłużył NBP jako podstawa przeprowadzenia ewaluacji aktualnego poziomu cyberdojrzałości danego systemu. Informacja zwrotna, zawierająca wyniki oceny wraz z ewentualnymi zaleceniami co do obszar*ów* wymagających udoskonaleń, została przekazana operatorom. Finalnie, przy zastosowaniu obowiązujących zasad wymiany informacji wrażliwych, sumaryczne wyniki badań ankietowych przeprowadzonych przez NBP zostały także udostępnione Europejskiemu Bankowi Centralnemu. Stanowiło to nie tylko podsumowanie prowadzonych w Polsce prac w przedmiotowym zakresie, ale także umożliwiło wymianę doświadczeń na arenie międzynarodowej i skonfrontowanie wniosków wyciągniętych przez reprezentantów różnych jurysdykcji. Należy wyjaśnić, że wspomniana cyberdojrzałość (ang. *cybersecurity maturity*) rozumiana jest jako osiągnięcie określonego poziomu zewnętrznych wzorców odniesienia w zakresie cyberbezpieczeństwa, tj. wypełnianie założeń swoistego modelu, określającego mechanizm oceny środków kontroli, metod i procesów, zgodnie z najlepszą praktyką zarządzania. Co do zasady stanem najbardziej pożądanym powinno być osiągnięcie poziomu „najwyższego". Należy jednak pamiętać o określeniu swoistego apetytu na ryzyko w organizacji (obejmującego w szczególności cyberryzyko rozumiane jako połączenie prawdopodobieństwa wystąpienia cyberincydentów i ich następstw; ECB 2018, s. 55) oraz o dostosowaniu wymagań w zakresie pożądanego poziomu cyberdojrzałości do realnych potrzeb i możliwości. Dotychczas przeprowadzono badania ankietowe dotyczące poziomu cyberdojrzałości kluczowej infrastruktury polskiego systemu płatniczego, tj. systemów SORBNET2, SKARBNET4, Elixir, systemu rozliczeń prowadzonego przez KDPW_CCP SA oraz systemu rozrachunku prowadzonego przez KDPW SA. W rezultacie przeprowadzonych analiz stwierdzono wysoki poziom cyberdojrzałości wszystkich ww. systemów (NBP 2020a, s. 7).

„Wymagania nadzorcze w zakresie odporności cybernetycznej dla infrastruktur rynku finansowego" („Cyber resilience oversight expectations for financial market infrastructures", CROE) opierają się na Wytycznych BIS i PFMIs. W praktyce CROE stanowią metodykę Wytycznych BIS. Zgodnie z pierwotnym założeniem EBC wymagania CROE przeznaczone były głównie dla banków centralnych strefy euro. Z racji globalnego charakteru cyberryzyka i biorąc pod uwagę istotność współpracy międzyinsty-

tucjonalnej oraz konieczność podejmowania wspólnych działań na szczeblu europejskim – mających na celu ograniczenie negatywnych skutków cyberataków i ujednolicenie metod zarządzania cyberryzykiem – EBC zachęcał jednak do implementacji CROE nie tylko banki centralne Eurosystemu, ale również banki spoza strefy euro (Cœuré 2019).

CROE jest najnowszym dokumentem włączonym do katalogu narzędzi nadzoru systemowego używanych przez NBP. Na mocy uchwały zarządczej z 24 października 2019 r. Zarząd Narodowego Banku Polskiego zdecydował o zastosowaniu wymagań CROE, na rozwojowym poziomie cyberdojrzałości, w odniesieniu do systemów płatności funkcjonujących w Polsce (NBP 2019a). Wymagania zawarte w CROE służą osiągnięciu trzech głównych celów:

1) wskazaniu szczegółowych działań umożliwiających zrealizowanie Wytycznych BIS, zapewnienie możliwości rozwoju i zwiększania poziomu cyberodporności danych infrastruktur, bez określenia wymagań statycznych i pożądanego stanu końcowego, na rzecz oczekiwanego, nieustannego rozwoju i innowacji w świetle ewoluujących cyberzagrożeń,

2) wytyczeniu organom nadzoru jasnych wymagań w zakresie dokonywanej oceny – poziomy wymagań określone w CROE stanowią punkt odniesienia dla organów oceniających cyberdojrzałość systemów, zgodnie z praktykami zawartymi w Wytycznych BIS,

3) zapoczątkowaniu rzeczowej dyskusji pomiędzy operatorami nadzorowanych systemów a nadzorującymi je organami.

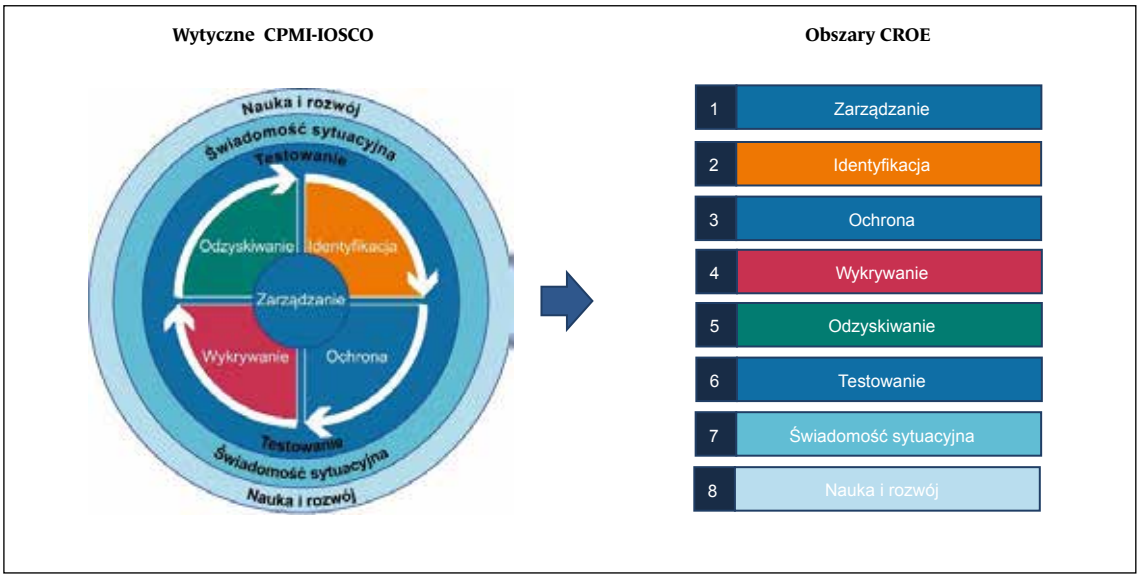
Jak wynika z wprowadzenia do CROE, podczas jego opracowywania posiłkowano się dokumentami zawierającymi międzynarodowe wytyczne, normy oraz ramy cyberbezpieczeństwa. Są to m.in.:

- „Ramy cyberbezpieczeństwa" (ang. *cybersecurity framework*), utworzone przez Narodowy Instytut Norm i Technologii Stanów Zjednoczonych (National Institute of Standards and Technology, NIST) w ramach współpracy między przemysłem a rządem. Składają się ze standardów, wytycznych i praktyk promujących w szczególności ochronę infrastruktury krytycznej.
- Norma ISO/IEC 27002 z zakresu systemów zarządzania bezpieczeństwem informacji, z tzw. rodziny norm SZBI (lub ISMS – Information Security Management Systems, potocznie: seria norm 27000). Zawiera ona praktyczne zasady zabezpieczania informacji zgodnie z normą ISO/IEC 27001 i jest przeznaczona do stosowania w organizacjach jako podstawa wyboru zabezpieczeń w ramach procesu wdrażania SZBI. Norma 27002 składa się z 14 rozdziałów poświęconych zabezpieczeniom i zawiera 35 głównych kategorii zabezpieczeń.
- Metodyka COBIT 5 (Control Objectives for Information and related Technology), stanowiąca międzynarodowe ramy kierowania i zarządzania informacją oraz technologią informacyjną przedsiębiorstwa (ISACA 2015). Została opracowana przez ISACA (Information Systems Audit and Control Association) – międzynarodowe stowarzyszenie do spraw audytu, kontroli i bezpieczeństwa systemów informatycznych oraz innych aspektów zarządzania systemami informatycznymi (obecnie funkcjonuje nowsza wersja norm COBIT 5 – COBIT 2019). Zawiera cztery kluczowe przewodniki: „Wprowadzenie i metodologia", „Cele kierownictwa i zarządzania", „Przewodnik projektowania" i „Przewodnik wdrażania".
- „Standard dobrych praktyk bezpieczeństwa informatycznego" („The Standard of Good Practice for Information Security"), czyli praktyczny i kompleksowy przewodnik dotyczący identyfikacji ryzyka dla bezpieczeństwa informacji w organizacji i zarządzania nim. Opracowało go Międzynarodowe Forum Bezpieczeństwa Informatycznego (Information Security Forum, ISF).

- „Narzędzia oceny bezpieczeństwa informatycznego" (ang. *assesment tool*) komisji federalnej ds. badań instytucji finansowych (Federal Financial Institutions Examination Council's, FFIEC).

Wymagania CROE, tak jak Wytyczne BIS, zostały podzielone na rozdziały, które obejmują pięć głównych obszarów zarządzania ryzykiem: zarządzanie (ang. *governance)*, identyfikację (ang. *identification)*, ochronę (ang. *protection)*, wykrywanie (ang. *detection)* oraz reagowanie, wznawianie i odzyskiwanie (ang. *response and recovery*), oraz trzy – jak określono w Wytycznych – nadrzędne komponenty: testowanie (ang. *testing*), świadomość sytuacyjną (ang. *situational awareness)* oraz naukę i rozwój (ang. *learning and evolving) – vide*: schemat 2. Elementy te są ściśle powiązane i powinny być rozpatrywane łącznie dla osiągnięcia celów w zakresie cyberodporności. Wymagania ujęte w każdym rozdziale CROE poprzedza preambuła pochodząca z Wytycznych, określająca nadrzędne cele każdej kategorii i każdego komponentu. Zestaw wymagań zawartych w CROE jest znacznie szerszy niż zakres zagadnień objętych badaniem ankietowym przeprowadzanym na postawie Wytycznych BIS. Tym, co odróżnia te dokumenty, jest także podział wymagań na części o różnych stopniach złożoności, zawierające określone zestawy oczekiwań dla każdego z wyodrębnionych poziomów. W CROE zostały ustalone trzy poziomy wymagań: rozwojowy, zaawansowany oraz innowacyjny. Mają one stanowić punkty odniesienia w ewaluacji cyberdojrzałości ocenianych podmiotów, przy czym spełnienie wymogów dotyczących poziomu innowacyjnego jest możliwe dopiero po spełnieniu wymagań na poziomie rozwojowym oraz zaawansowanym. Co ważne, weryfikacja spełnienia wymogów CROE odbywa się na zasadzie „wypełnij lub wyjaśnij" (ang. *meet or explain*) i umożliwia elastyczne podejście do sposobu podnoszenia poziomu cyberdojrzałości i kształtowania cyberodporności ocenianych systemów płatności. Zgodnie z informacjami zawartymi w „Ocenie funkcjonowania systemu płatniczego", sporządzanej co pół roku przez Narodowy Bank Polski, systemem, który obecnie jest oceniany pod kątem realizacji wymogów wynikających z CROE, jest system SORBNET2, prowadzony przez polski bank centralny.

Schemat 2
Wytyczne BIS a CROE



Źródło: CPMI-IOSCO (2016).

Jednym z bodźców do stworzenia i przyjęcia CROE przez banki centralne ESBC była dyrektywa NIS. Jej implementacja – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa – chociaż nie oddziałuje bezpośrednio na system płatniczy, ma znaczenie dla całego NBP i jego zadań w zakresie cyberbezpieczeństwa. Zgodnie z projektem UstKSC przy ówczesnej konstrukcji jego art. 27[7] możliwe było uznanie NBP za operatora usług kluczowych. W swoim stanowisku zgłoszonym w ramach opiniowania tego projektu Narodowy Bank Polski zgłaszał krytyczne uwagi co do możliwości wydania takiej decyzji, występując z perspektywy podmiotu będącego centralnym bankiem państwa, o określonej roli i zadaniach ustawowych, nad którym nie jest sprawowany nadzór merytoryczny. Pozostawało to w zgodzie z zasadą niezależności banku centralnego zawartą w art. 227 Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 r. i w zapisach dotyczących krajowych banków centralnych w Traktacie o funkcjonowaniu Unii Europejskiej, głównego aktu prawa pierwotnego Unii (NBP 2018b, s. 8–9). Postulowano nawet całkowite wykreślenie Narodowego Banku Polskiego z art. 4 UstKSC, określającego skład podmiotowy krajowego systemu cyberbezpieczeństwa, aby usunąć konstrukcję godzącą w niezależność polskiego banku centralnego. Było to zbieżne z działaniami innych europejskich banków centralnych mającymi miejsce podczas opiniowania przez nie dyrektywy NIS (ECB 2017, s. 2–3). „Przepisy projektu ustawy przewidują bowiem nakładanie obowiązków i nadzoru nad ich realizacją ze strony ministerstwa właściwego dla sektora finansowego, a nawet jednostki podległej temu ministerstwu" (NBP 2018c, s. 2). Zgłoszono również uwagi do projektowanego zakresu podmiotowego sektora „bankowość i infrastruktura rynków finansowych" z Załącznika I pierwotnej UstKSC. W katalogu podmiotów, które zostały zaliczone do tego sektora i – co za tym idzie – w stosunku do których mogła zostać wydana decyzja o uznaniu za operatora usługi kluczowej, znalazły się bowiem podmioty nie tylko niewskazane w implementowanej ustawą dyrektywie NIS, ale także już objęte nadzorem Prezesa NBP (Krajowa Izba Rozliczeniowa SA) lub Komisji Nadzoru Finansowego (Krajowy Depozyt Papierów Wartościowych SA, krajowe instytucje płatnicze świadczące usługę *acquiring*). Finalnie uwagi NBP zostały uwzględnione i uniknięto dublowania zadań nadzorczych wobec rzeczonych podmiotów – operatorzy systemów płatności zostali wyłączeni spod reżimu ustanowionego przez ustawę o krajowym systemie cyberbezpieczeństwa. Bank centralny w UstKSC został objęty jedynie obowiązkami, które wykonuje jako podmiot publiczny, realizujący zadania publiczne zależne od systemu informacyjnego:

– wyznaczenia osoby do kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa i przekazania jej danych do właściwego Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) na poziomie krajowym, którym dla NBP będzie CSIRT GOV prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego,

– zarządzania incydentami i zgłaszania ich do właściwego CSIRT,

– zapewniania dostępu do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa i sposobów zabezpieczania się przed tymi zagrożeniami osobom, na rzecz których zadanie publiczne jest realizowane.

Można zauważyć, że dzięki dążeniu NBP m.in. do zachowania autonomii instytucjonalnej i funkcjonalnej zasadnicza część kwestii dotyczących cyberbezpieczeństwa polskiego systemu płatniczego została pozostawiona w gestii banku centralnego, którego zadaniem jest dbanie o szeroko pojęte bezpieczeństwo (a w jego ramach cyberbezpieczeństwo), m.in. za pomocą sprawowanego nadzoru systemowego. Dzięki przyjęciu CROE i efektywnemu wykorzystaniu tego narzędzia możliwe jest zapewnienie

[7] „Art. 27. Do podmiotu publicznego, o którym mowa w art. 4 pkt 6–14, wobec którego wydana została decyzja o uznaniu za operatora usługi kluczowej, stosuje się przepisy rozdziału 2.".

poziomu wymagań zbliżonego do tego, który wynikałby z UstKSC – nawet przy braku przepisu prawa materialnego, który obligowałby operatorów systemów płatności do spełniania konkretnych wymagań z CROE jako wytycznych niebędących aktem normatywnym.

Warto wspomnieć, że już od prawie 2 lat planowana jest nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa, służąca m.in. implementacji Aktu o cyberbezpieczeństwie. Minister Cyfryzacji 7 września 2020 r. zwrócił się z prośbą o zgłoszenie uwag do udostępnionego w tym samym dniu projektu zmiany obowiązującej UstKSC (RCL 2020). Narodowy Bank Polski w stanowisku zgłoszonym na etapie konsultacji publicznych odniósł się do proponowanych zmian. Wyrażone zostały wątpliwości co do planowanych regulacji dotyczących oceny ryzyka dostawcy sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa, a także co do nowych środków ostrzeżenia i polecenia zabezpieczającego. Proponowane w projekcie rozwiązania mają umożliwić Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa wydawanie ostrzeżeń w przypadku uzyskania informacji o zagrożeniu cyberbezpieczeństwa, uprawdopodobniającej wystąpienie incydentu krytycznego, oraz poleceń zabezpieczających po wystąpieniu takiego incydentu. Zawarte w nich uprawnienia do wprowadzenia nakazów i zakazów, których adresatem mógłby być właśnie Narodowy Bank Polski jako podmiot publiczny zgodnie z UstKSC, ponownie uznano za niezgodne z konstytucyjną rolą i ustrojową pozycją banku centralnego w Polsce. Były także sprzeczne z wartościami fundamentalnymi z punktu widzenia funkcjonowania NBP, w szczególności z niezależnością banku centralnego, w tym niezależnością wobec organów państwowych. W uwagach Narodowy Bank Polski podkreślił również swoją pozycję operatora systemów płatności o kluczowym znaczeniu dla stabilności całego systemu finansowego w Polsce (tj. SORBNET2 i TARGET2-NBP). Ingerowanie w nie i, co za tym idzie, możliwe zakłócenie funkcjonowania mogłoby „…nieść za sobą skutki w postaci zaburzeń transmisji pieniądza w skali całego kraju. Dlatego też, w ocenie NBP, powierzanie Pełnomocnikowi Rządu ds. Cyberbezpieczeństwa kompetencji umożliwiających ingerowanie w systemy IT będące komponentem infrastruktury płatniczej, której operatorem jest bank centralny, nie znajduje uzasadnienia" (NBP 2020c, s. 2). Narodowy Bank Polski wyraził w swojej opinii nadzieję, że możliwość wykorzystania tych środków zostanie ograniczona i nie będą wpływały na realizację zadań banku centralnego, a decyzja o ewentualnym ograniczeniu ich wykorzystania zostanie w gestii NBP. Było to ponowne dążenie do utrzymania należnego bankowi centralnemu zakresu samostanowienia w kwestii szeroko pojętego cyberbezpieczeństwa oraz wymaganego poziomu cyberodporności własnej i nadzorowanych systemów. Działania te spowodowały dodanie w trzecim projekcie zmiany UstKSC z 16 lutego 2021 r. nowego artykułu, w którym uwzględniono uwagi zawarte w stanowiskach NBP. Do banku centralnego mają nie mieć zastosowania przepisy dotyczące: niewprowadzania do użytkowania lub wycofywania sprzętu bądź oprogramowania od dostawcy uznanego za dostawcę wysokiego ryzyka, polecenia zabezpieczającego czy żądania od podmiotów publicznych informacji przez właściwe organy nadzorcze. Prezes NBP ma zostać jedynie niezwłocznie poinformowany przez ministra właściwego ds. informatyzacji o decyzjach wydanych w tym zakresie.

Dla systemu płatniczego, będącego fundamentem obrotu bezgotówkowego, osiągnięcie jak najwyższego poziomu cyberodporności ma kluczowe znaczenie, zważywszy na możliwe skutki jego ewentualnej destabilizacji i konsekwencje krótszej lub dłuższej niedostępności systemów płatności czy schematów płatniczych. Oczywiście niemożliwe pozostaje zapewnienie stuprocentowej ochrony teleinformatycznych komponentów infrastruktury systemu płatniczego, jednak niezbędne jest podjęcie wszelkich działań służących ich jak najlepszemu zabezpieczaniu. Skuteczność działań i wdrożonych

rozwiązań z zakresu cyberbezpieczeństwa systemu płatniczego będzie miała odzwierciedlenie m.in. w długości jego ewentualnej destabilizacji wskutek cyberataków. Krótkotrwałe (kilkugodzinne) incydenty braku lub ograniczonej dostępności mogą nie mieć istotnego wpływu na system finansowy. Dłuższa destabilizacja, np. kilkudniowa, mogłaby jednak spowodować, że konieczne byłoby przejście wyłącznie na płatności gotówkowe, na co NBP również powinien być przygotowany (m.in. dzięki zgromadzeniu odpowiednich rezerw gotówki). Znaczenie kompleksowych działań w zarządzaniu cyberryzykiem dla obrotu pieniężnego zostało również podkreślone przez wyodrębnienie w NBP Departamentu Cyberbezpieczeństwa, który ma przeciwdziałać cyberzagrożeniom, monitorować je, a także koordynować obsługę cyberincydentów. W latach 2015–2017 dokonano cyberataków na wiele banków na świecie (w tym banki centralne), m.in. na ekwadorski bank Banco Del Austroz, na konta Banku Centralnego Bangladeszu znajdujące się w Banku Rezerwy Federalnej w Nowym Jorku czy na banki komercyjne w Bangladeszu, Ukrainie, Tajwanie i Nepalu (F-Secure, s. 5–9). Ataki nie były skierowane na poszczególne jednostki. Bazowały na płatnościach w sieci SWIFT (Society for Worldwide Interbank Financial Telecommunication) wykorzystywanej do przeprowadzania międzynarodowych transakcji finansowych. Co więcej, jak niedawno ujawniono, w grupie podmiotów, które ucierpiały w zeszłorocznej globalnej operacji hakerskiej związanej z oprogramowaniem firmy SolarWinds, znalazł się m.in. Centralny Bank Danii (Danmarks Nationalbank 2021). Nieustająca i, jak pokazują powyższe przykłady, nieograniczona geograficznie aktywność hakerów w sektorze finansowym potwierdza, że konieczne jest proaktywne podejście do cyberbezpieczeństwa (por. Molenda 2020, s. 82–90) i szczególne zabezpieczenie infrastruktur składających się na system płatniczy, stanowiących swojego rodzaju system naczyń połączonych, w którym awaria jednego podmiotu może spowodować efekt domina (Calliess, Baumgarten 2020, s. 1150–1155).

5. Podsumowanie

Zestawienie i analiza istniejących i planowanych uregulowań dotyczących cyberbezpieczeństwa w systemie płatniczym oraz liczba istniejących regulacji w tym zakresie i stopień ich szczegółowości świadczą o znaczeniu tego zagadnienia. Systemy płatnicze należą do najważniejszych składników systemów finansowych krajów na całym świecie. Analiza narzędzi mających wpływ na nadzór systemowy, będący jednym z rodzajów nadzoru nad systemem finansowym w Polsce, potwierdza, że cyberbezpieczeństwo polskiego systemu płatniczego ma duże znaczenie dla stabilności finansowej całego kraju. Dokumenty stanowiące podstawę ocen nadzorczych, a także obserwacje wynikające z przeglądu aktów normatywnych, międzynarodowych standardów cyberbezpieczeństwa i porównania sytuacji instytucji finansowych na świecie dowodzą, że istnieją odpowiednie instrumenty sprawowania nadzoru systemowego w zakresie cyberodporności. Narodowy Bank Polski dysponuje narzędziami do zapewnienia sprawności i bezpieczeństwa funkcjonowania polskiego systemu płatniczego. Ich źródłem są przepisy prawa umożliwiające podejmowanie władczych działań w zakresie *oversight*, jak też elastyczne sprawowanie nadzoru. Co więcej, na podstawie obserwacji funkcjonujących w Polsce systemów płatności, schematów płatniczych, systemów rozliczeń i systemów rozrachunku papierów wartościowych oraz usługi *acquiring* świadczonej przez krajowe instytucje płatnicze można stwierdzić, że cyberodporność infrastruktury polskiego systemu płatniczego utrzymuje się na wysokim poziomie, a wspomniane narzędzia nadzorcze są stosowane prawidłowo.

Sprawne, bezpieczne i efektywne funkcjonowanie systemu płatniczego stanowi wyzwanie, jednak przy wdrożeniu odpowiednich rozwiązań z dziedziny cyberbezpieczeństwa jest możliwe. Urzeczywistnia się to również dzięki wypełnianiu przez Narodowy Bank Polski jego ustawowego zadania – organizowania rozliczeń pieniężnych przez pełnienie w tym zakresie nie tylko funkcji regulacyjnej i operacyjnej, ale także funkcji nadzorczej, będącej przedmiotem niniejszego opracowania. Jest to szczególnie ważne w obliczu mnogości powiązań między podmiotami i zmieniającego się charakteru cyberataków na infrastrukturę systemu finansowego. Coraz częściej są to ataki typu APT (tzw. *advanced persistent threats*), w których wyspecjalizowani cyberprzestępcy wykorzystują zaawansowane narzędzia i często dysponują pokaźnym budżetem na swoje działania. Potwierdzają to m.in. dane statystyczne będące podstawą publikowanych przez NBP cyklicznych materiałów, w których funkcjonowanie polskiego systemu płatniczego w ciągu ostatnich 10 lat było oceniane wyłącznie pozytywnie[8]. O prawidłowym i stabilnym działaniu systemu płatniczego, zapewniającym sprawne i bezpieczne przeprowadzanie rozliczeń i rozrachunków, świadczą nie tylko dane w raportach. Dowodzi tego przede wszystkim bezpieczeństwo, łatwość i dostępność usług płatniczych dla konsumentów, którzy nawet w obliczu sytuacji kryzysowej (np. pandemii) mogą nadal korzystać z pieniędzy, przy zachowaniu niepogorszonych standardów m.in. obsługi ich płatności.

Bibliografia

Calliess C., Baumgarten A. (2020), Cybersecurity in the EU the example of the financial sector: a legal perspective, *German Law Journal*, 21(6), 1149–1179.

Cœuré B. (2019), *Cyber resilience as a global public good (Speech at the G7 conference),* https://www.ecb.europa.eu/press/key/date/2019/html/ecb.sp190510_2~2e988cb439.pl.html.

CPSS-IOSCO (2012), *Principles for financial market infrastructure,* April, Bank for International Settlements and International Organization of Securities Commissions.

CPMI-IOSCO (2016), *Guidance on cyber resilience for financial market infrastructures*, June, https://www.bis.org/cpmi/publ/d146.pdf.

Danmarks Nationalbank (2021), *Danmarks Nationalbank's comments on media reports about SolarWinds,* https://www.nationalbanken.dk/en/pressroom/ speeches/Pages/2021/Danmarks Nationalbank%E2%80%99s-comments-on-media-reports-about-SolarWinds.aspx.

ECB (2016), *Eurosystem Oversight Policy Framework*, July, European Central Bank.

ECB (2017), *Opinion of the European Central Bank of 6 April 2017 on the identification of critical infrastructures for the purpose of information technology security (CON/2017/10*), April, European Central Bank.

ECB (2018), *Cyber resilience oversight expectations for financial market infrastructure,* December, European Central Bank.

F-Secure (2019), *Threat Analysis SWIFT Systems and the SWIFT Customer Security Program,* https://www.f-secure.com/content/dam/f-secure/en/business/common/collaterals/f-secure-threat-analysis-swift.pdf.

ISACA (2015), *Glossary of Terms – Polish 3rd Edition*, Information Systems Audit and Control Association.

[8] Na podstawie danych i analiz ze strony NBP – *Ocena funkcjonowania systemu płatniczego*, https://www.nbp.pl/home.aspx?f=/systemplatniczy/ocena/ocena.html.

Molenda K. (2020), Rozpoznanie adwersarzy w wojskowych systemach teleinformatycznych, w: A. Gryszczyńska, G. Szpor (red.), *INTERNET Cyberpandemia*, C.H. Beck.

NBP (2003), *Rynek kart płatniczych w Polsce*, Narodowy Bank Polski.

NBP (2018a), *Nadzór systemowy w zakresie systemu płatniczego*, Narodowy Bank Polski.

NBP (2018b), *Odniesienie się wnioskodawcy do uwag – tabela uwag do Projektu ustawy o krajowym systemie cyberbezpieczeństwa na Komitet do Spraw Europejskich,* https://legislacja.rcl.gov.pl/docs//2/12304650/12466724/12466727/dokument331765.pdf.

NBP (2018c), *Uwagi zgłoszone do projektu ustawy o krajowym systemie cyberbezpieczeństwa*, https://legislacja.rcl.gov.pl/docs//2/12304650/12466724/12466726/dokument331474.pdf.

NBP (2019a), *Komunikat – aktualizacja polityki sprawowania przez Narodowy Bank Polski nadzoru systemowego w zakresie systemu płatniczego*, https://www.nbp.pl/home.aspx?f=/aktualnosci/wiadomosci_2019/nadzor-systemplatniczykomunikat2019.html.

NBP (2019b), *Polityka sprawowania przez Narodowy Bank Polski nadzoru systemowego w zakresie systemu płatniczego*, Narodowy Bank Polski.

NBP (2020a), *Raport o nadzorze systemowym w zakresie polskiego systemu płatniczego za 2019 r.,* Narodowy Bank Polski, Warszawa.

NBP (2020b), *System płatniczy w Polsce*, Narodowy Bank Polski.

NBP (2020c), *Uwagi zgłoszone do projektu z dnia 7 września 2020 r. ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych*, https://legislacja.gov.pl/docs//2/12337950/12716608/12716611/dokument470301.pdf.

RCL (2020), *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych (UD68),* https://legislacja.rcl.gov.pl/projekt/12337950/katalog/12716602#12716602.

Szafrański B. (2020), Bezpieczeństwo procesów informacyjnych a długotrwałe przechowywanie zasobów cyfrowych, w: A. Gryszczyńska, G. Szpor (red.), *INTERNET Cyberpandemia*, C.H. Beck.

Szpor G. (2020), Nowelizacja siatki pojęciowej cyberbezpieczeństwa, *Monitor Prawniczy*, 22, 1189–1192.

Szpringer W. (2014), *Instytucje nadzoru w sektorze finansowym. Kierunki rozwoju*, Poltext.

Aneks

Podstawy prawne i wytyczne uzupełniające dla nadzoru systemowego sprawowanego przez NBP

Schematy płatnicze i usługa *acquiring*	Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (Dz. U. z 2020 r. poz. 794 ze zm.), wraz z aktami wykonawczymi		Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz. Urz. UE L 123 z 2015 r., rozporządzenie MIFREG) wraz z aktami wykonawczymi Rozporządzenie delegowane Komisji Europejskiej (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów komunikacji (Dz. Urz. UE L 69 z 2018 r., rozporządzenie SCA)
Systemy płatności			
Systemy rozrachunku papierów wartościowych	Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (Dz. U. z 2020 r. poz. 89 ze zm.), wraz z aktami wykonawczymi	Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (Dz. U. z 2019 r. poz. 212), wraz z aktami wykonawczymi	Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 909/2014 z dnia 23 lipca 2014 r. w sprawie usprawnienia rozrachunku papierów wartościowych w Unii Europejskiej i w sprawie centralnych depozytów papierów wartościowych, zmieniające dyrektywy 98/26/WE i 2014/65/UE oraz rozporządzenie (UE) nr 236/2012 (Dz. Urz. UE L 257 z 2014 r., rozporządzenie CSDR) wraz z aktami wykonawczymi
Systemy rozliczeń papierów wartościowych			Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 z dnia 4 lipca 2012 r. w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji (Dz. Urz. UE L 201 z 2012 r., rozporządzenie EMIR) wraz z aktami wykonawczymi

Wytyczne uzupełniające	Dokumenty opracowane przez działające przy BIS – CPSS / CPMI oraz IOSCO: Zasady dotyczące infrastruktury rynków finansowych (*Principles for financial market infrastructure*, Zasady IRF) Zasady przekazywania informacji i metodologia (*Disclosure framework and assessment methodology*) Stosowanie zasad dotyczących infrastruktury rynków finansowych do infrastruktury rynków finansowych prowadzonej przez banki centralne (*Application of the PFMIs to central bank FMIs*) Wytyczne w zakresie bezpieczeństwa infrastruktury rynków finansowych w cyberprzestrzeni (*Guidance on cyber resilience in financial market infrastructures*, Wytyczne BIS) Zasady publikowania danych ilościowych przez kontrahentów centralnych (*Public quantitative disclosure standards for central counterparties*)
	Regulacje i standardy Europejskiego Banku Centralnego: Zaktualizowane ramy nadzorcze dla systemów płatności detalicznych (*Revised oversight framework for retail payment systems*) Wymagania nadzoru systemowego względem powiązań pomiędzy systemami płatności detalicznych (*Oversight expectations for links between retail payment systems*) Ramy nadzorcze dla kartowych schematów płatniczych – standardy (*Oversight framework for card payment schemes – standards*) Wytyczne w zakresie oceny kartowych schematów płatniczych pod kątem standardów nadzorczych (*Guide for the assessment of card payment schemes against the oversight standards*) Zharmonizowane podejście nadzorcze i standardy nadzorcze dla instrumentów płatniczych (*Harmonised oversight approach and oversight standards for payment instruments*) Wymagania nadzorcze w zakresie odporności cybernetycznej dla infrastruktur rynku finansowego (*Cyber resilience oversight expectations for financial market infrastructures,* CROE) Wytyczne w zakresie oceny bezpieczeństwa płatności internetowych (*Assessment guide for the security of internet payments*) Wytyczne końcowe w zakresie bezpieczeństwa płatności internetowych (*Final guidelines on the security of internet payments*)
	Pozostałe rekomendacje: Rekomendacje w zakresie bezpieczeństwa płatności internetowych (*Recommendations for the security of internet payments,* European Forum on the Security of Retail Payments) – SecuRe Pay Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe – KNF

Źródło: opracowanie własne na podstawie NBP (2019b).

Cybersecurity of the Polish payment system within the oversight performed by Narodowy Bank Polski

Abstract

The ubiquitous use of ICT systems and high digitalisation are nowadays core features of activities ongoing in the economy. The importance of cybersecurity, leading to reaching and maintaining a high level of cyber resilience of infrastructures, is increasing not just in the financial system. The efficient and safe functioning of the national payment system, which constitutes the financial system's so-called specific system of communicating vessels, is crucial for its stability – being further an essential element for the real economy and its participants. Whereas previous works on the payment system were focused on its operational performance, covering statistical and, to some extent, legal aspects, noticing the information gap, this paper is devoted to cybersecurity measures.

The main objective of the study is to verify the thesis statement that Narodowy Bank Polski is equipped with adequate oversight tools which allow NBP to not only ensure a sufficient level of cyber resilience of the overseen financial market infrastructures, but also, in a broader perspective, enable the fulfilment of the statutory responsibilities of the central bank as an entity responsible for organising monetary clearing and ensuring and maintaining the stability of the national financial system as a whole. It is also an attempt to gain new insights into the matter of financial market infrastructure by focusing on the field of its cybersecurity.

The analysis included in the article was based on the national and international legal acts along with the soft law and regulations on cybersecurity in the form of standards, guidelines and other documents applying to the infrastructure of the payment system. Due to limitations, the sources used were narrowed to publicly available information and official releases. The author undertook an extensive literature survey with applied research on central bank oversight. The research was therefore descriptive, primarily carried out from a legal perspective, nonetheless with thorough consideration of historical changes and interdisciplinarity at the interface between law and IT, regarded as an issue of particular relevance to the discussed topic.

The steps taken to verify the accuracy of the assumptions made in the article confirm that the Polish central bank has diverse tools to perform its oversight activities of the infrastructure of the payment system. Such measures are based on both the legal basis *sensu stricte*, allowing the undertaking of authoritative actions, as well as on more flexible forms of conducting oversight exerting moral suasion. A reflection of their application can also be found in the statistical information on the Polish payment system; however, what should be considered as the main indication giving hard evidence, is the efficient functioning of its components: systems, schemes and services. The aforementioned is visible in the security and availability of payment services for consumers who, even in the face of a crisis such as a pandemic, can still use their money with non-deteriorated standards, e.g. in the field of handling their payments.

Considering the high interconnectivity of its infrastructures, the broad range of entry points through which they could be compromised, and the overall risks in the ecosystem, the smooth uninterrupted operation of the financial market in Poland should be the main indicator of the high

level of cyber resilience of the payment system infrastructures. This is particularly important nowadays, when cyberattacks are performed by more and more active, persistent and advanced adversaries. A strong situational awareness in the field of cybersecurity is crucial for all the institutions, giving them the foundations to ensure their own protection and preparedness even for the worst case scenario, e.g. a successful attack, when an ability to resume their business operations quickly will be a critical factor.

Keywords: oversight, cybersecurity, payment system, CROE