DOI: 10.52694/ThPSR.125.7

Marcin Niedbała

Powszechny dostęp do informacji przestrzennych w systemie PIT a bezpieczeństwo infrastruktury krytycznej Polski

Universal access to spatial information in the IPT system and the security of Poland's critical infrastructure

Jednym z zadań, jakie ma realizować Punkt Informacyjny do spraw Telekomunikacji, jest zapewnienie operatorom sieci dostępu do szeregu informacji, w tym m.in. na temat istniejącej w Polsce infrastruktury telekomunikacyjnej. Jednakże, proces i zakres gromadzenia danych za pośrednictwem tego systemu rodzi obawy przed zagrożeniami wynikającymi z powszechnego udostępnienia informacji na temat infrastruktury krytycznej państwa. Celem artykułu jest dokonanie analizy obowiązujących regulacji prawnych, na podstawie których w ramach Punktu Informacyjnego do spraw Telekomunikacji udostępniane są dane mogące dotyczyć infrastruktury krytycznej Polski, oraz wynikających stąd potencjalnych zagrożeń dla bezpieczeństwa państwa. W opracowaniu posłużono się metodami dogmatyczno-prawną, analizy instytucjonalno-prawnej, a także historyczno-prawną. W wyniku poczynionych rozważań pozytywnie zweryfikowano tezę, zgodnie z którą rozwiązania normatywne przyjęte za podstawę funkcjonowania systemu PIT i umożliwiające udostępnianie za jego pośrednictwem kluczowych informacji przestrzennych Polski (w tym o charakterze krytycznym), nie gwarantują bezpieczeństwa państwa, przeciwnie, prowadzą do istotnych dla niego zagrożeń.

Słowa kluczowe: infrastruktura krytyczna, bezpieczeństwo, punkt informacyjny do spraw telekomunikacji, zagrożenia bezpieczeństwa

One of the tasks to be performed by the Information Point for Telecommunications is to provide network operators with access to a range of information, including i.a. on the existing telecommunications infrastructure in Poland. However, the process and scope of data being collected through this system raises concerns about the threats resulting from the widespread availability of information on the country's critical infrastructure. The aim of the article is to analyze the applicable legal regulations on the basis of which the Information Point for Telecommunications provides access to data that may concern Poland's critical infrastructure, and the resulting potential threats to state security.

Key words: critical infrastructure, security, telecommunication information point, security threats

Wstęp

Dynamicznie zmieniające się uwarunkowania geopolityczne, agresywna polityka zagraniczna Rosji, szantaż energetyczny, tragiczna w skutkach wojna na Ukrainie, a także próby destabilizacji poszczególnych państw coraz częściej prowadzą do debaty nad nowymi wyzwaniami dla ich bezpieczeństwa. Przeciwdziałanie tym nowym zagrożeniom wymaga stałego podejmowania i doskonalenia działań na rzecz ochrony porządku publicznego, sprawnego funkcjonowania aparatu państwowego oraz życia i zdrowia wszystkich członków społeczeństwa. W sposób szczególny dotyczy to Polski, która nie tylko bezpośrednio sąsiaduje z państwem będącym ofiarą niczym nieuzasadnionej i niesprowokowanej rosyjskiej agresji, ale jednocześnie sama musi się bronić przed wymierzonymi w nią atakami hybrydowymi ze strony Rosji i Białorusi. Podejmowanie działań na rzecz zapewnienia bezpieczeństwa państwa musi odbywać się we wszystkich obszarach jego działalności, w tym na gruncie ustawodawczym poprzez stałe dostosowywanie porządku prawnego do nowych wyzwań. W tym kontekście na uwagę zasługuje zagadnienie powszechnego dostępu do szeregu danych przestrzennych, z których część może dotyczyć systemów i obiektów wchodzących w skład infrastruktury

krytycznej Polski[1]. Szczególne znaczenie mają informacje udostępniane przez Punkt Informacyjny do spraw Telekomunikacji (PIT)[2], obejmujące szczegółowy przebieg infrastruktury telekomunikacyjnej. Przedmiotowe dane obejmują dokładną lokalizację obiektów o strategicznym znaczeniu, których niezakłócone działanie gwarantuje prawidłowe funkcjonowanie całego państwa.

Celem opracowania, jest zatem udzielenie odpowiedzi na następujące pytania badawcze, tj. czy powszechny dostęp do szczegółowych informacji przestrzennych udostępnianych za pośrednictwem PIT może prowadzić do realnych zagrożeń dla polskiej infrastruktury krytycznej, zaś w przypadku odpowiedzi pozytywnej, czy obowiązujące regulacje prawne w należyty sposób korespondują z aktualnymi wymogami bezpieczeństwa narodowego Polski. Podejmowane rozważania uwzględniają przy tym stan prawny oraz stan faktyczny na dzień 1 lipca 2024 r. Niniejsze opracowanie stanowi zarazem jedną z pierwszych prób podjęcia badań nad przedmiotowymi zagadnieniami. Stanowi to po części wynik niedawnych zmian na gruncie normatywnym, które znacząco poszerzyły zakres informacji gromadzonych i udostępnianych w systemie PIT, doprowadzając jednocześnie do formułowania w debacie publicznej pytań o ich racjonalność oraz wynikające z nich potencjalne zagrożenia dla bezpieczeństwa infrastruktury krytycznej Polski. Sformułowano przy tym następujące założenia badawcze:

---

[1] W rozumieniu art. 3 pkt 2 ustawy z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122, dalej „uzk").

[2] Na podstawie art. 29 i nast. ustawy z 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz. U. z 2023 r. poz. 733, dalej „wruist."). Należy przy tym wskazać, że przepisy tworzące ramy prawne funkcjonowania systemu PIT (rozdział 2a wruist.) zostały wprowadzone do polskiego porządku normatywnego z dniem 1 lipca 2016 r. na podstawie art. 1 pkt 15 ustawy z 9 czerwca 2016 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2016 r. poz. 903, dalej „zwruist2016") przy czym art. 29a i 29b weszły w życie w późniejszej dacie 1 stycznia 2017 r. Dodanie wskazanych przepisów wynikało z konieczności implementacji art. 10 ust. 4 dyrektywy Parlamentu Europejskiego i Rady 2014/61/UE z 15 maja 2014 r. w sprawie środków mających na celu zmniejszenie kosztów realizacji szybkich sieci łączności elektronicznej (Dz. U. UE. L. z 2014 r. Nr 155, str. 1, dalej „dyrektywa 2014/61"). Celem wskazanego przepisu Dyrektywy było zobligowanie państw członkowskich do utworzenia co najmniej jednego podmiotu pełniącego funkcję pojedynczego punktu informacyjnego udostępniającego informacje odnoszące się do infrastruktury technicznej dowolnego operatora sieci (art. 4 dyrektywy 2014/61), trwających lub planowanych robót budowlanych dotyczących infrastruktury technicznej określonego operatora sieci (art. 6 dyrektywy 2014/61) oraz procedury udzielania zezwoleń na roboty budowlane niezbędne w celu wdrożenia elementów szybkich sieci łączności elektronicznej (art. 7 dyrektywy 2014/61). W przypadku Polski takim pojedynczym punktem informacyjnym w rozumieniu dyrektywy 2014/61 jest PIT. Jego zadania polegają na udzielaniu posiadanych przez Prezesa UKE informacji dotyczących procedur i formalności, informacji z inwentaryzacji infrastruktury i usług telekomunikacyjnych, informacji o planach inwestycyjnych i istniejącej infrastrukturze technicznej. Tym samym celem PIT jest w uproszczeniu przyspieszenie i uproszczenie inwestycji w zakresie szybkich sieci łączności.

1. niezakłócone funkcjonowanie infrastruktury krytycznej państwa jest warunkiem jego bezpieczeństwa,
2. do systemu PIT przekazywane są szczegółowe dane dotyczące infrastruktury i usług telekomunikacyjnych, z których część może stanowić infrastrukturę krytyczną Polski,
3. przepisy prawne regulujące funkcjonowanie systemu PIT nie przewidują jasno sprecyzowanych ograniczeń w dostępie do gromadzonych w nim danych,
4. *de lege lata* nie jest możliwe jednoznaczne stwierdzenie, jakie dane dotyczące infrastruktury krytycznej powinny być przekazywane do systemu PIT, a jakie nie, zaś wątpliwości w tym przedmiocie potęguje dodatkowo brak niezbędnych aktów wykonawczych doprecyzowujących tę materię,
5. w systemie PIT są gromadzone i udostępniane informacje na temat elementów infrastruktury telekomunikacyjnej, które nie stanowią *ex lege* infrastruktury krytycznej, lecz ich niezakłócone funkcjonowanie implikuje jej bezpieczeństwo.

Przedstawione założenia badawcze zdeterminowały hipotezę badawczą, zgodnie z którą aktualnie obowiązujące rozwiązania prawne regulujące funkcjonowanie systemu PIT i udostępnianie za jego pośrednictwem szczegółowych informacji na temat kluczowych elementów infrastruktury telekomunikacyjnej Polski (w tym o charakterze krytycznym) nie gwarantują bezpieczeństwa strategicznego państwa, przeciwnie, prowadzą do istotnych dla niego zagrożeń.

Na potrzeby prowadzonych badań posłużono się typowymi dla nauk prawnych metodami badawczymi. Podstawową metodą stosowaną w celu rozwiązania problemu badawczego o charakterze prawnym jest niewątpliwie metoda dogmatyczno-prawna, polegająca na ustaleniu, jakie normy w obrębie danego systemu prawnego są obowiązujące. Dzięki analizie przepisów poszczególnych obowiązujących aktów prawnych zbadano, jakie informacje są przekazywane do systemu PIT, jakie ograniczenia w dostępie do nich zostały wprowadzone przez polskiego ustawodawcę, a także, co w polskim porządku prawnym należy rozumieć przez infrastrukturę krytyczną. W tym ostatnim przypadku pomocniczo zastosowano metodę analizy instytucjonalno-prawnej, która umożliwiła zwrócenie uwagi na postanowienia przyjmowanego przez Radę Ministrów Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) doprecyzowujące kryteria służące wyodrębnianiu elementów

infrastruktury krytycznej. Dodatkowo, przy wykorzystaniu metody historyczno-prawnej przedstawiono genezę wprowadzenia do polskiego porządku normatywnego przepisów tworzących system PIT oraz regulujących jego funkcjonowanie, jak też dokonano analizy działań zmierzających do jego uruchomienia.

Infrastruktura krytyczna – definicja i znaczenie w systemie bezpieczeństwa

Dynamiczne przemiany społeczne i rozwój technologii w XX i XXI wieku znacząco wpłynęły na ewolucję poglądów dotyczących rozumienia istoty bezpieczeństwa. Pojęcie to jest w najprostszym ujęciu definiowane jako stan wolny od zagrożeń, co nawiązuje do jego łacińskiej etymologii słowa *securitas*, które z kolei wywodzi się od wyrażenia *sine cura*[3]. Bezpieczeństwo jest także identyfikowane z pewnością istnienia, przetrwania, posiadania, funkcjonowania i rozwoju podmiotu, która to pewność stanowi wypadkową stanu wolnego od zagrożeń oraz kreatywnej działalności podmiotu[4]. W literaturze przedmiotu wyróżnia się trzy wymiary bezpieczeństwa, tj. podmiotowy (np. bezpieczeństwo narodowe, międzynarodowe), przedmiotowy (np. bezpieczeństwo polityczne, militarne, ekologiczne) oraz procesualny (odnoszący się do dynamicznego charakteru bezpieczeństwa jako stale ewoluującego procesu powodowanego przez powstawanie nowych zagrożeń i podejmowanych w reakcji na nie działań)[5]. W kontekście przedmiotowych rozważań szczególne znaczenie należy przypisać wyróżnianemu w oparciu o kryterium podmiotowe bezpieczeństwu narodowemu. Jak wskazuje W. Kitler, stanowi ono „najważniejszą wartość, potrzebę narodową i priorytetowy cel działalności państwa, jednostek i grup społecznych, a jednocześnie proces obejmujący różnorodne środki, gwarantujące trwały, wolny od zakłóceń byt i rozwój narodowy (państwa), w tym ochronę i obronę państwa, jako instytucji politycznej oraz ochronę jednostek i całego społeczeństwa, ich

[3] W. Sokała, *Paradygmat bezpieczeństwa – podstawy, historia, ewolucja*, [w:] *Transsektorowe obszary bezpieczeństwa narodowego*, pod red. K. Liedela, Difin, Warszawa 2011, s. 13.

[4] R. Zięba, *Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego*, [w:] *Bezpieczeństwo międzynarodowe po zimnej wojnie*, pod red. R. Zięby, Wydawnictwa Akademickie i Profesjonalne, Warszawa 2008, s. 15-16.

[5] Ibidem, s. 16-20.

dóbr i środowiska naturalnego przed zagrożeniami, które w znaczący sposób ograniczają jego funkcjonowanie lub godzą w dobra podlegające szczególnej ochronie”[6]. W ramach bezpieczeństwa narodowego wyróżnia się sektory: dyplomatyczny, militarny, wywiadowczy, kontrwywiadowczy, prawa i porządku publicznego, ratownictwa, kulturowy, edukacyjny, socjalny, demograficzny, migracyjny, finansowy, energetyczny, transportowy, infrastruktury krytycznej oraz środowiska naturalnego, a także transsektorowe obszary bezpieczeństwa, jak np. cyberbezpieczeństwo lub bezpieczeństwo antyterrorystyczne[7].

Infrastruktura krytyczna stanowi zatem jeden z podstawowych sektorów bezpieczeństwa narodowego. Niemniej jednak, współcześnie coraz częściej dokonuje się jej przewartościowania zwracając uwagę na jej kluczowe znaczenie dla prawidłowego funkcjonowania państwa. Infrastrukturę krytyczną tworzą systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje, usługi kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców (art. 3 pkt 2 uzk.). Obejmuje ona systemy zaopatrzenia w energię, surowce energetyczne i paliwa, łączności, sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych. Podsumowując, należy stwierdzić, iż infrastruktura krytyczna obejmuje systemy, które są niezbędne do minimalnego funkcjonowania gospodarki i państwa[8]. Tym samym, zakłócenie jej prawidłowego działania może nie tylko stanowić ogromne zagrożenie dla licznych powiązanych ze sobą sektorów bezpieczeństwa narodowego, ale także może wpłynąć na każdy aspekt życia codziennego. Ponadto, dodatkowym utrudnieniem dla zapewnienia stałej ochrony infrastruktury krytycznej jest szeroki zakres istniejących pomiędzy jej poszczególnymi rodzajami i elementami powiązań, które

[6] W. Kitler, *Bezpieczeństwo państwa a bezpieczeństwo narodowe*, [w:] *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, pod red. W. Kitlera, M. Czuryk, M. Karpiuka, Wydawnictwo Akademii Obrony Narodowej, Warszawa 2013, s. 23.

[7] Biuro Bezpieczeństwa Narodowego, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf, s. 19, dostęp 15.07.2024.

[8] A. Lasota-Jędrzak, *Bezpieczeństwo infrastruktury krytycznej państwa*, „Rocznik Bezpieczeństwa Morskiego” 2013, nr 3, s. 19.

mogą być fizyczne, cybernetyczne, geograficzne (w znaczeniu geoprzestrzennym) i logiczne (w znaczeniu relacji)[9]. W rezultacie infrastrukturę krytyczną można porównać do złożonego organizmu, zaś naruszenie jakiejkolwiek jego części może zakłócić funkcjonowanie całości.

Ryzyko powszechnego dostępu do informacji na temat infrastruktury krytycznej Polski w ramach PIT

Jednym z zadań realizowanych przez Prezesa UKE jest sporządzanie i bieżące aktualizowanie inwentaryzacji infrastruktury i usług telekomunikacyjnych dla terytorium Rzeczypospolitej Polskiej[10], przy czym szczegółowy sposób gromadzenia i prezentowania informacji uzyskanych w ramach inwentaryzacji określa w drodze rozporządzenia minister właściwy do spraw informatyzacji (art. 29 ust. 7 wruist.)[11]. Należy wskazać, iż przedmiotowy obowiązek nie stanowi sam w sobie nowego zagadnienia, gdyż znajduje swoje oparcie ustawie, która weszła w życie 17 grudnia 2010 r. (art. 29 wruist) Zgodnie z pierwotnym brzmieniem przepisu zadaniem Prezesa UKE było sporządzanie dla terytorium Polski w formie elektronicznej inwentaryzacji przedstawiającej pokrycie istniejącą infrastrukturą telekomunikacyjną i publicznymi sieciami telekomunikacyjnymi zapewniającymi lub umożliwiającymi zapewnienie

[9] S. Rinaldi, J. Peerenboom, T. Kelly, *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, „IEEE Control Systems" 2001, nr 6, https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies, s. 12, dostęp 15.07.2024.

[10] Realizacja przez Prezesa UKE wskazanego zadania następuje w wyniku gromadzenia informacji pochodzących od podmiotów wskazanych w art. 29 ust. 2 wruist, tj. państwowych jednostek organizacyjnych z wyłączeniem podmiotów, o których mowa w art. 4 pkt 1, 2, 4, 5 i 8 ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34 z późn. zm.) (pkt 1), jednostek samorządu terytorialnego prowadzących działalność, o której mowa w art. 3 ust. 1 (tj. w zakresie telekomunikacji) w formie niewyodrębnionej w ramach ich osobowości prawnej i jednostek organizacyjnych, którym jednostka samorządu terytorialnego powierzyła prowadzenie działalności, o której mowa w art. 3 ust. 1 (pkt 1a), podmiotów wykonujących zadania z zakresu użyteczności publicznej (pkt 2) oraz przedsiębiorców telekomunikacyjnych (pkt 3).

[11] Sposób gromadzenia informacji w ramach inwentaryzacji uległ istotnemu przeobrażeniu z dniem 1 stycznia 2023 r., od której to daty informacje gromadzone w ramach inwentaryzacji przekazywane są Prezesowi UKE drogą elektroniczną, za pomocą udostępnionego przez niego narzędzia teleinformatycznego, przy czym w żadnym przepisie tego narzędzia nie skonkretyzowano, § 6 ust. 1 rozporządzenia Ministra Cyfryzacji z dnia 19 grudnia 2022 r. w sprawie inwentaryzacji infrastruktury i usług telekomunikacyjnych (t.j. Dz. U. z 2024 r. poz. 45, dalej „rii."). Niemniej jednak, 27 stycznia 2023 r. dla celów inwentaryzacji uruchomiono system PIT, zaś pod koniec marca 2023 r. na oficjalnej stronie UKE udostępniono alternatywne narzędzia dla celów wykonania obowiązku inwentaryzacji (UKE Inwentaryzacja) zaznaczając przy tym, iż jest ono częścią systemu PIT.

szerokopasmowego dostępu do Internetu, z odrębnym zaznaczeniem pokrycia łączami światłowodowymi oraz sieciami bezprzewodowymi, oraz budynkami umożliwiającymi kolokację (aktualnie art. 29 ust. 1 pkt 2 wruist). W późniejszym czasie dwa razy poszerzono zakres danych gromadzonych w ramach inwentaryzacji. Pierwszy raz nastąpiło to z dniem 1 kwietnia 2013 r., gdy spektrum inwentaryzacji uzupełniono o usługi telefoniczne, usługi transmisji danych zapewniających szerokopasmowy dostęp do Internetu i usługi rozprowadzania programów radiowych i telewizyjnych, świadczone w oparciu o infrastrukturę telekomunikacyjną i publiczne sieci telekomunikacyjne zapewniające szerokopasmowy dostęp do Internetu (art. 29 ust. 1 pkt 1 wruist)[12]. W wyniku kolejnej nowelizacji z dniem 1 stycznia 2023 r. inwentaryzacja objęła dodatkowo informacje o przebiegu światłowodowych i innych niż światłowodowe linii kablowych zapewniających lub umożliwiających zapewnienie szerokopasmowego dostępu do Internetu (art. 29 ust. 1 pkt 3 wruist)[13].

Wprawdzie skala informacji przekazywanych Prezesowi UKE była olbrzymia jeszcze przed wejściem w życie nowelizacji, lecz poszerzenie katalogu zbieranych danych w sposób szczególny rodzi zastrzeżenia. Z jednej strony projektodawcy zwruist2019 zwrócili uwagę, iż celem zmiany było poszerzenie zasobu wiedzy Prezesa UKE o rzeczywiste przebiegi zrealizowanej, najbardziej nowoczesnej infrastruktury telekomunikacyjnej, które w przeszłości musiały być przez niego domniemywane na podstawie pozostałych danych wskazujących na przestrzenne relacje innych elementów tej infrastruktury, wykazywanych przez podmioty objęte obowiązkiem inwentaryzacyjnym[14]. Z drugiej strony, dodatkowe informacje dotyczą szczegółowego przebiegu elementów infrastruktury o potencjalnym znaczeniu strategicznym zapewniających dostęp do Internetu m.in. dla licznych instytucji publicznych, w tym tych, których niezakłócone funkcjonowanie ma doniosłe znaczenie dla bezpieczeństwa państwa. Należy wobec tego przeanalizować, jakie konkretnie informacje zbierane w ramach inwentaryzacji infrastruktury i usług telekomunikacyjnych, a następnie powszechnie udostępniane w systemie PIT (art. 29 ust. 6 wruist) mogą dotyczyć infrastruktury krytycznej Polski.

[12] Art. 1 pkt 2 ustawy z dnia 12 października 2012 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2012 r. poz. 1256).

[13] Art. 1 pkt 10 ustawy z dnia 30 sierpnia 2019 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2019 r. poz. 1815 z późn. zm., dalej „zwruist2019").

[14] *Projekt ustawy o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw*, druk nr 3484, Sejm VIII Kadencji, s. 34-35.

W inwentaryzacji gromadzone są m.in. informacje dotyczące poszczególnych rodzajów infrastruktury telekomunikacyjnej i publicznych sieci telekomunikacyjnych zapewniających lub umożliwiających zapewnienie szerokopasmowego dostępu do Internetu w zakresie danych identyfikujących i charakteryzujących węzły publicznych sieci telekomunikacyjnych oraz ich lokalizację, technologię i parametry, punkty elastyczności oraz ich lokalizację, technologię i parametry, światłowodowe i inne niż światłowodowe linie kablowe oraz ich przebieg, komórki stacji bazowych ruchomych publicznych sieci telekomunikacyjnych oraz ich lokalizację, technologię i parametry, linie bezprzewodowe oraz ich lokalizację, technologię i parametry, zasięg ruchomych publicznych sieci telekomunikacyjnych (§ 4 rii). Wskazane informacje są następnie prezentowane na stronie internetowej w formie zestawień tabelarycznych oraz map w skali 1:2 500 000 albo większej (§ 5 rii). Jednocześnie, z treści analizowanego rozporządzenia nie wynika w żadnej mierze, które ze gromadzonych informacji mogłyby dotyczyć infrastruktury krytycznej, a tym samym dostęp do nich mógłby zostać ograniczony. Należy wprawdzie zwrócić uwagę na pojawiające się w nim kilkukrotnie sformułowanie „infrastruktura telekomunikacyjna o dużym znaczeniu", co zgodnie z podaną definicją oznacza węzeł publicznej sieci telekomunikacyjnej, którego suma maksymalnych przepustowości aktywnych interfejsów nienależących do sieci dostępowej lub niesłużących do podłączania abonentów, przekracza wartość 500 Gb/s lub linia kablowa światłowodowa, zakończona przynajmniej z jednej strony w węźle publicznej sieci telekomunikacyjnej, w której suma przepustowości interfejsów podłączonych do pojedynczego włókna przekracza wartość 200 Gb/s[15]. Z treści przepisów rii nie sposób jednak wyinterpretować, czy „infrastruktura telekomunikacyjna o dużym znaczeniu" stanowi część infrastruktury krytycznej, ani też, czy dostęp do informacji jej dotyczących zostanie jakkolwiek ograniczony.

Problem potęguje dodatkowo fakt, iż ustawodawca nie skorzystał dotychczas z upoważnienia ustawowego do wydania rozporządzenia określającego rodzaje infrastruktury technicznej, co do której operatorzy sieci są zwolnieni z obowiązku sprawozdawczego ze względu na bezpieczeństwo i integralność infrastruktury technicznej, zdrowie publiczne, obronność, bezpieczeństwo państwa lub bezpieczeństwo i porządek

[15] Sformułowania te zawarte są w części II załącznika Nr I do rii – Wzory formularzy służących przekazywaniu informacji do inwentaryzacji infrastruktury i usług telekomunikacyjnych wraz z objaśnieniami co do sposobu ich wypełnienia.

publiczny (art. 25c wruist). Tym samym, nie jest możliwe w sposób niebudzący wątpliwości wyinterpretować z samej przytoczonej powyżej treści art. 25c ust. 1 wruist, jakie konkretnie informacje dotyczące infrastruktury technicznej powinny być przekazywane do PIT, a jakie nie.

Poszukując zatem odpowiedzi na pytanie, które elementy infrastruktury telekomunikacyjnej podlegającej inwentaryzacji w trybie art. 29 wruist stanowią infrastrukturę krytyczną należy wskazać na przywoływaną już definicję, zgodnie z którą infrastrukturę krytyczną tworzą wymienione enumeratywnie systemy, w tym m.in. sieci teleinformatyczne[16]. Ustawowe kryteria, umożliwiające wyodrębnienie infrastruktury krytycznej, mają charakter ogólny. Niemniej jednak, ich doprecyzowanie następuje w ramach NPOIK, który przyjmuje w drodze uchwały Rada Ministrów (art. 5b ust. 1 uzk). NPOIK określa m.in. szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli (art. 5b ust. 2 pkt 3 uzk). W oparciu o te szczegółowe kryteria Dyrektor RCB we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy sporządza jednolity, wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy (art. 5b ust. 7 uzk).

Zarówno wskazany, sporządzany przez Dyrektora RCB wykaz, jak też załącznik numer 2 do NPOIK określający szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, mają charakter niejawny. Niemniej jednak, możliwe jest dokonanie analizy historycznego załącznika numer 1 do NPOIK z 2013 r. – charakterystyki systemów infrastruktury krytycznej. W części 1.3 poświęconej systemowi sieci teleinformatycznych wskazano, iż organy administracji publicznej do wykonywania swoich ustawowych obowiązków, wykorzystują systemy teleinformatyczne dedykowane do przetwarzania i gromadzenia różnorodnych danych, a także wydzielone fizycznie lub logicznie, będące własnością organów administracji publicznej lub też dzierżawione od operatorów sieci telekomunikacyjnych – sieci telekomunikacyjne. Ponadto, administracja publiczna korzysta w tym względzie z usług dzierżawy sieci telekomunikacyjnych przedsiębiorców telekomunikacyjnych. Jednocześnie wskazano, iż przez

[16] Zgodnie z art. 3 pkt 2 uzk, do którego odsyła art. 2 ust. 1 pkt 5 wruist.

system sieci teleinformatycznej należy rozumieć ogół istniejących i eksploatowanych przez administrację publiczną systemów teleinformatycznych połączonych wewnętrznie za pomocą sieci telekomunikacyjnych, które stanowią jeden ze składników infrastruktury krytycznej państwa[17]. Tym samym, należy sformułować wniosek, iż objęte inwentaryzacją światłowodowe linie kablowe i inne niż światłowodowe linie kablowe, zapewniające lub umożliwiające zapewnienie szerokopasmowego dostępu do Internetu, w zakresie, w jakim są wykorzystywane przez administrację publiczną, mogą stanowić infrastrukturę krytyczną.

W kontekście tych rozważań na uwagę zasługuje także Załącznik numer 1 do NPOIK z 2020 r. – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje. W dziale 2.6.5. poświęconym propozycjom działań technicznych mających na celu zmniejszenie uzależnienia funkcjonowania infrastruktury krytycznej od zewnętrznych usług zaleca się m.in. zapewnienie zasilania obiektów, w których zlokalizowane są elementy infrastruktury krytycznej, z dwóch niezależnych sieci elektroenergetycznych, wodociągów i sieci łączności lub do transmisji danych. Ponadto, przewody powinno umieścić się pod ziemią i doprowadzić do różnych miejsc w budynku[18]. Można wobec tego sformułować pytanie, czy sens wskazanej dobrej praktyki, służącej zapewnieniu bezpieczeństwa infrastruktury krytycznej, nie zostanie wypaczony, w sytuacji, gdy informacje na temat przebiegu sieci łączności (w szczególności linii światłowodowych) będą powszechnie dostępne w ramach PIT. Co więcej, nawet ewentualne objęcie przedmiotowych danych wyłączeniem z zakresu informacji przekazywanych do PIT (art. 25c ust. 1 wruist), jedynie w nieznacznym stopniu zmniejszy potencjalne zagrożenie naruszenia infrastruktury krytycznej. Wystarczy wskazać, iż w ramach inwentaryzacji infrastruktury i usług telekomunikacyjnych gromadzone są, w tym w celu przyszłego udostępnienia, informacje m.in. na temat węzłów publicznych sieci telekomunikacyjnych. Tymczasem, ingerencja we wskazane obiekty w sposób pośredni może zakłócić działanie sieci łączności stanowiących infrastrukturę krytyczną państwa. Wprawdzie

[17] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2013. Załącznik 1 – Charakterystyka systemów infrastruktury krytycznej*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, s. 36, dostęp 15.07.2024.

[18] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, s. 57, dostęp 15.07.2024.

w dziale 2.6.6. załącznika numer 1 do NPOIK z 2020 r. wśród rekomendacji dotyczących zapewnienia bezpieczeństwa technicznego zwrócono uwagę m.in. na istotę zapewnienia możliwości kontynuacji działalności infrastruktury krytycznej w lokalizacji zapasowej. Z jednej strony, odosobniona ingerencja w określony element infrastruktury krytycznej nie powinna stanowić znacznego zagrożenia dla jej funkcjonowania. Z drugiej strony, skoordynowane działania, bezpośrednio lub pośrednio wymierzone w lokalizacje zapasowe mające zapewnić ciągłość działania infrastruktury krytycznej, podejmowane np. w trakcie konfliktu zbrojnego lub ataku terrorystycznego, bezsprzecznie zwielokrotniają przedmiotowe zagrożenie. Realność powyższego scenariusza potęguje z kolei powszechny dostęp do informacji na temat lokalizacji elementów infrastruktury krytycznej lub obiektów z nimi funkcjonalnie powiązanych.

Odnosząc się natomiast do dodanego do wruist rozdziału 2a należy wskazać, iż projektodawcy zwruist2016 także nie doprecyzowali kwestii ewentualnych dodatkowych ograniczeń w dostępie do informacji gromadzonych w PIT. Wyjątkiem jest prawo odmowy przez Głównego Geodetę Kraju i inne organy administracji publicznej przekazania posiadanych informacji do PIT, jeśli jest to niezbędne ze względu na bezpieczeństwo i integralność infrastruktury technicznej, zdrowie publiczne, obronność, bezpieczeństwo państwa lub bezpieczeństwo i porządek publiczny (art. 29d ust. 9). Z obecnego brzmienia wruist nie sposób wyinterpretować konkretnych ograniczeń w dostępie do informacji udostępnianych przez PIT. Podkreślenia wymaga, iż dostęp do nich zapewnia się każdemu operatorowi sieci (art. 29b ust. 1 wruist)[19]. Pomimo tego, dostęp do systemu PIT w wersji, która została uruchomiona z dniem 27 stycznia 2023 r., posiadał *de facto* każdy użytkownik sieci Internet, rejestrując się z wykorzystaniem m.in. profilu zaufanego. Możliwość uzyskania dostępu do szczególnie istotnych danych, jak np. szczegółowa lokalizacja punktów elastyczności czy też przebieg światłowodowych i innych niż światłowodowe linii kablowych, jest zapewniona m.in. użytkownikom będącym przedsiębiorcami telekomunikacyjnymi (operatorami sieci). Co istotne, kryterium to może w teorii spełnić każda jednostka zarejestrowana w odpowiedniej ewidencji (np. w Centralnej Ewidencji i Informacja o Działalności Gospodarczej) i mająca nadany NIP. Zarówno w obowiązujących

[19] Zgodnie z definicją zawartą w art. 2 ust. 1 pkt 8 wruist operatorem sieci jest przedsiębiorca telekomunikacyjny lub podmiot wykonujący zadania z zakresu użyteczności publicznej, w tym jednostka samorządu terytorialnego.

aktach prawnych, jak też na stronie internetowej PIT próżno szukać informacji w przedmiocie metod ewentualnej szczegółowej weryfikacji podmiotu wnioskującego o dostęp do wskazanego systemu. Tym samym, wątpliwości budzi, czy wymóg spełnienia wyłącznie kryterium posiadania przez dany podmiot przymiotu m.in. przedsiębiorcy telekomunikacyjnego gwarantuje należytą ochronę informacji o potencjalnym znaczeniu strategicznym. Nie bez znaczenia pozostaje także fakt, iż dotychczas nie zostało wydane rozporządzenie określające sposób prezentowania informacji gromadzonych w PIT i wymagania techniczne i eksploatacyjne obsługującego go systemu teleinformatycznego (art. 29f wruist), co potęguje zastrzeżenia wobec potencjalnie nieuzasadnionego zbyt prostego dostępu do danych, w tym dotyczących szczegółowej lokalizacji obiektów tworzących infrastrukturę krytyczną Polski.

Potencjalne zagrożenia fizyczne dla infrastruktury krytycznej państwa

W literaturze przedmiotu można spotkać się z rozbieżnymi poglądami w przedmiocie poszczególnych kategorii zagrożeń dla infrastruktury krytycznej państwa. J. Milewski wyróżnia zagrożenia naturalne, zagrożenia techniczne oraz terroryzm. Do pierwszej grupy zalicza m.in. powodzie, silne wiatry, długotrwałe susze, ruchy tektoniczne (powodujące trzęsienia ziemi), oblodzenia i intensywne opady śniegu oraz epidemie. Zagrożenia techniczne oznaczają z kolei awarie dotyczące w szczególności obiektów przemysłowych, obiektów komunalnych (np. awarie energetyczne, wodociągowe), obiektów budowlanych (np. zawalenie się budynku), urządzeń transportowych. Zagrożenia będące wynikiem terroryzmu mogą polegać zarówno na atakach bombowych, jak też działaniach w cyberprzestrzeni mających zakłócić funkcjonowanie określonych elementów infrastruktury krytycznej[20]. Odmienny pogląd wyraża M. Żuber wyróżniając zagrożenia obszaru środowiskowego (katastrofy naturalne, zawodność systemów energetycznych i zasilania zapasowego, sabotaż, zagrożenia terrorystyczne, włamania), zagrożenia obszaru technologicznego (brak

[20] J. Milewski, *Identyfikacja infrastruktury krytycznej i jej zagrożeń*, „Zeszyty Naukowe AON" 2016, nr 4, s. 108-112.

alternatywnych torów transmisyjnych, występowanie błędów produkcyjnych lub konstrukcyjnych), zagrożenia obszaru danych i sieci, zagrożenia obszaru czynnika ludzkiego (kradzież, sabotaż, terroryzm, nierealistyczne regulacje prawne lub luki prawne)[21]. Niemalże tożsame kategorie zagrożeń wyróżnia w odniesieniu do infrastruktury telekomunikacyjnej K. Baniak, dzieląc je na dotyczące środowiska/energii, technologii, danych/transmisji oraz czynnika ludzkiego[22]. Warto zwrócić uwagę także na dokonywane w literaturze przedmiotu wyróżnianie w odniesieniu do infrastruktury teleinformatycznej zagrożenia o charakterze zewnętrznym (np. uszkodzenie danych), wewnętrznym (np. utrata lub uszkodzenie danych, brak możliwości obsługi systemu lub sieci z powodu nieprawidłowego funkcjonowania) oraz fizycznym (zniszczeniem infrastruktury sieci, urządzeń bądź samych obiektów)[23]. W kontekście przedmiotowych rozważań dotyczących potencjalnego ryzyka związanego z powszechnym dostępem do informacji na temat infrastruktury teleinformatycznej, w tym krytycznej, podstawowe znaczenie należy przypisać zagrożeniom obszaru środowiskowego i obszaru czynnika ludzkiego, a ściślej zagrożeniom fizycznym będących wynikiem działania człowieka. W praktyce mogą one polegać na ryzyku zakłócenia działania, uszkodzenia lub trwałego zniszczenia elementów sieci lub powiązanych z nimi funkcjonalnie obiektów.

W NPOIK z 2020 r. wskazuje się, iż zapewnienie bezpieczeństwa infrastruktury krytycznej następuje wskutek działań mających na celu minimalizację ryzyka zakłócenia jej funkcjonowania poprzez:

1. zapewnienie bezpieczeństwa fizycznego (np. zapobieganie dostępowi nieuprawnionych osób na teren infrastruktury krytycznej);
2. zapewnienie bezpieczeństwa technicznego (minimalizowanie ryzyka zaburzenia realizowanych procesów technologicznych);

[21] M. Żuber, *Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego*, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, nr 2, https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/338, s. 181-182, dostęp 15.07.2024.

[22] K. Baniak, *Analiza zagrożeń telekomunikacyjnych sektora publicznego*, „Biblioteka Bezpieczeństwa Narodowego" 2007, t. 3, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/materialy-archiwalne/biblioteka-bezpieczenst/tom-3/1125,Bezpieczenstwo-w-telekomunikacji-i-teleinformatyce.html, s. 39, dostęp 15.07.2024.

[23] A. Wisz, *Bezpieczeństwo informacji w wojskowych sieciach teleinformatycznych*, „Biblioteka Bezpieczeństwa Narodowego" 2007, t. 3, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/materialy-archiwalne/biblioteka-bezpieczenst/tom-3/1125,Bezpieczenstwo-w-telekomunikacji-i-teleinformatyce.html, s. 72-73, dostęp 15.07.2024.

3. zapewnienie bezpieczeństwa osobowego (minimalizowanie ryzyka zakłócenia funkcjonowania infrastruktury krytycznej w wyniku działań uprawnionych osób);
4. zapewnienie bezpieczeństwa teleinformatycznego (minimalizowanie ryzyka zakłócenia funkcjonowania infrastruktury krytycznej w wyniku oddziaływania na aparaturę kontrolną i sieci teleinformatyczne);
5. zapewnienie bezpieczeństwa prawnego (minimalizowanie ryzyka zakłócenia funkcjonowania infrastruktury krytycznej w następstwie prawnych działań podmiotów zewnętrznych),
6. tworzenie planów ciągłości działania i odtwarzania[24].

Nie budzi wprawdzie wątpliwości, iż poważne i długotrwałe zakłócenie działania infrastruktury krytycznej w wyniku pojedynczego incydentu, np. odosobnionego aktu sabotażu, jest mało prawdopodobne. Jej kluczowe znaczenie dla funkcjonowania aparatu państwowego implikuje konieczność objęcia jej szczególną ochroną i dokładaniem starań na rzecz zapewnienia jej niezakłóconego i prawidłowego działania zarówno przez administrację rządową, jak też jej operatorów. Niemniej jednak, powszechny dostęp do informacji na temat lokalizacji poszczególnych elementów infrastruktury krytycznej oraz funkcjonalnie z nią związanych obiektów może prowadzić do zagrożeń, które z kolei mogą ulec znacznemu zwielokrotnieniu w przypadku ataku terrorystycznego lub działań zbrojnych.

Jak trafnie wskazuje P. Dela, cel ataku w cyberprzestrzeni, który ma charakter wyłącznie destrukcyjny, może zostać osiągnięty również na drodze oddziaływania kinetycznego. Zauważa przy tym, iż w warunkach pokoju próby unieszkodliwienia infrastruktury krytycznej są wprawdzie podejmowane na drodze oddziaływania informatycznego, lecz w razie zaostrzenia sporu prawdopodobne jest wykorzystanie w tym celu chociażby dronów z ładunkiem wybuchowym[25]. Przykład stanowi tragiczna w skutkach eksplozja pojazdu na przedmieściach Nashville w Boże Narodzenie 2020 r. w pobliżu budynku, w którym zlokalizowany był węzeł sieci komórkowych, internetowych i telewizyjnych. W efekcie tego zdarzenia nastąpił całkowity paraliż lotniska, systemów łączności organów ścigania i szpitali, a także brak było możliwości korzystania z bankomatów i kart kredytowych, czy nawet skorzystania z numeru alarmowego 911. Warto

[24] Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2020*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, s. 30-31, dostęp 15.07.2024.
[25] P. Dela, *Założenia działań w cyberprzestrzeni*, Wydawnictwo Naukowe PWN, Warszawa 2022, s. 121-122.

przy tym dodać, iż powstały w rezultacie chaos był wynikiem tylko jednego, odosobnionego wybuchu[26]. Doniosłość zagrożeń dla infrastruktury krytycznej można obserwować także przez pryzmat trwającej od 24 lutego 2022 r. wojny na Ukrainie. Niemalże od samego jej początku do międzynarodowej opinii publicznej docierają informacje o obieraniu przez Rosjan za cel takich obiektów, jak gazociągi, stacje elektroenergetyczne czy mosty[27]. Wnioski płynące z obserwacji tego konfliktu powinny wpłynąć na zmianę postrzegania potencjalnych zagrożeń dla bezpieczeństwa infrastruktury krytycznej w przypadku Polski.

Aby podkreślić doniosłość potencjalnych zagrożeń, jakie może stworzyć powszechny dostęp do informacji na temat infrastruktury telekomunikacyjnej za pośrednictwem PIT, należy zwrócić uwagę przede wszystkim na dwa rodzaje obiektów, jakie podlegają inwentaryzacji, tj. punkty elastyczności[28] oraz węzły publicznych sieci telekomunikacyjnych[29]. Jednocześnie, w ramach prowadzonej inwentaryzacji gromadzone są szczegółowe dane dotyczące lokalizacji, technologii i parametrów wskazanych obiektów, przy czym lokalizacja określana jest poprzez podanie jej współrzędnych w stopniach i ułamku dziesiętnym stopnia z dokładnością do 2 m[30]. Istotne znaczenie ma przy tym fakt, iż naruszenie, zakłócenie

[26] R. Rojas, J. McGee, E. Lee, S. Cavendish, *When Nashville Bombing Hit a Telecom Hub, the Ripples Reached Far Beyond*, https://www.nytimes.com/2020/12/29/us/nashville-bombing-telecommunications.html, dostęp 15.07.2024.

[27] K. Byzdra, *Infrastruktura krytyczna w ruinie. Ukraiński minister publikuje dane*, https://energetyka24.com/elektroenergetyka/wiadomosci/infrastruktura-krytyczna-w-ruinie-ukrainski-minister-publikuje-dane, dostęp 15.07.2024; N. Turak, A. Macias, *Russian strikes hit critical infrastructure in western city of Lviv; UN to vote on new peace resolution*, https://www.cnbc.com/2023/02/16/russia-ukraine-live-updates.html, dostęp 15.07.2024.

[28] Zgodnie z § 2 pkt 3 rii przez punkt elastyczności należy rozumieć punkt dostępu do usług lub fizyczny element publicznej sieci telekomunikacyjnej, w którym następuje przełączanie kabli miedzianych lub włókien optycznych, fizyczne rozdzielenie kabla światłowodowego na kable o mniejszej krotności, rozdzielanie sygnału optycznego prowadzonego jednym światłowodem na wiele światłowodów przy użyciu elementu rozgałęziającego lub zmiana rodzaju linii kablowej oraz w którym nie jest możliwe przyłączenie użytkowników końcowych do publicznej sieci telekomunikacyjnej lub zapewnienie dostępu telekomunikacyjnego wymagającego połączenia elementów publicznej sieci telekomunikacyjnej przedsiębiorcy telekomunikacyjnego z elementami sieci telekomunikacyjnej lub udogodnieniami towarzyszącymi znajdującymi się pomiędzy tym elementem a zakończeniami sieci, w szczególności: szafę kablową, studzienkę, mufę kablową, skrzynkę kablową, kontener telekomunikacyjny, słupek telekomunikacyjny, słupek kablowy, szafę telekomunikacyjną, złącze kablowe, maszt telekomunikacyjny, słup lub wieżę telekomunikacyjną.

[29] Zgodnie z § 2 pkt 3 rii przez węzeł publicznej sieci telekomunikacyjnej należy rozumieć podłączone do publicznej sieci telekomunikacyjnej urządzenie telekomunikacyjne lub zespół podłączonych do publicznej sieci telekomunikacyjnej urządzeń telekomunikacyjnych znajdujących się we wspólnej lokalizacji, zapewniających fizyczne połączenie publicznych sieci telekomunikacyjnych lub przyłączenie do publicznej sieci telekomunikacyjnej użytkowników końcowych.

[30] Co wynika z § 4 pkt 1 lit. a i b rii oraz wytycznych zawartych w załącznikach do przedmiotowego rozporządzenia.

funkcjonowania lub całkowite zniszczenie punktów elastyczności, zapewniających dostęp do usług telekomunikacyjnych konkretnego operatora, może pozbawić dostępu do tych usług wszystkie powiązane z tym operatorem podmioty, w tym instytucje publiczne. Ryzyko opisywanego scenariusza jest wprawdzie niewielkie w przypadku odosobnionego incydentu ze względu na fakt działania lokalizacji zapasowych mających zapewnić ciągłość transmisji danych. Niemniej jednak, powszechny dostęp do informacji na temat ogółu inwentaryzowanych punktów elastyczności urealnia zagrożenie w postaci zaplanowanego, bądź to przez obce państwo, bądź przez organizację terrorystyczną, skoordynowanego ataku wymierzonego w kilka wskazanych obiektów. Podobnie przedstawia się sytuacja w odniesieniu do jawności informacji na temat szczegółowych lokalizacji węzłów publicznych sieci telekomunikacyjnych, których uszkodzenie lub zniszczenie może mieć wpływ na dostęp do sieci łączności licznych podmiotów, w tym podmiotów publicznych. Jednocześnie, z treści przepisów rii nie wynika, by te rodzaje obiektów infrastruktury telekomunikacyjnej zostały uznane za stanowiące element infrastruktury krytycznej państwa, co pozwalałoby domniemywać, że ich położenie nie będzie stanowiło powszechnie dostępnej informacji. Wniosek taki wynika bowiem z faktu, iż dane na temat infrastruktury krytycznej nie są przekazywane do PIT (art. 25c ust. 1 wruist). Tymczasem, informacje odnośnie szczegółowej lokalizacji punktów elastyczności i węzłów publicznych sieci telekomunikacyjnych są gromadzone w ramach inwentaryzacji infrastruktury i usług telekomunikacyjnych, jaka jest prowadzona z wykorzystaniem tego systemu. Dane te są z kolei jawne dla każdego użytkownika Internetu, który zarejestruje się w PIT jako operator sieci (art. 29 ust. 6 i art. 29b ust. 1 pkt 2 wruist).

Podkreślenia wymaga ponadto ryzyko związane z możliwością planowania ewentualnego ataku przy wykorzystaniu tzw. „białego wywiadu" określanego również mianem OSINT (Open Source Intelligence). Pojęcie to oznacza metodę pracy wywiadowczej polegającą na studiowaniu i analizie zagranicznych materiałów publikowanych oficjalnie lub ogólnie dostępnych, jak prasa codzienna i periodyczna (polityczna, techniczna, biznesowa), dokumentacja i sprawozdania z działalności i zamierzeń rządów (oświadczenia premiera i ministrów), partii rządzących i opozycyjnych, specjalistycznych kongresów oraz prac parlamentarnych (np. wystąpień i interpelacji posłów, stenogramów z prac komisji sejmowych), ponadto wnioski patentowe, audycje radiowe i telewizyjne, Internet,

otwarte bazy danych, geoinformacja i wiele innych ogólnodostępnych źródeł[31]. Bez wątpienia źródłem takim może być PIT w obecnym kształcie przepisów regulujących jego działanie i charakter udostępnianych z jego wykorzystaniem danych. Nic bowiem nie stoi na przeszkodzie, aby określony podmiot zarejestrował swoją działalność jako przedsiębiorca telekomunikacyjny i złożył wniosek o dostęp do systemu PIT spełniając jednocześnie jedyne kryterium warunkujące ów dostęp. Związane z tym ryzyko można zobrazować odwołując się do kazusu ujawnienia za pośrednictwem serwisu WikiLeaks w 2010 r. listy kluczowych obiektów na całym świecie, w tym biegnącego przez terytorium Polski ropociągu „Przyjaźń", którą określono jako listę potencjalnych celów ataków terrorystycznych[32]. Co istotne, wskazane określenie może znaleźć zastosowanie także w odniesieniu do dostępnych w PIT danych, które, jak wynika z aktualnie obowiązujących przepisów, pozwolą poznać dokładną lokalizację obiektów o potencjalnym znaczeniu strategicznym.

Podsumowanie

Podjęte w niniejszym artykule rozważania pozwoliły pozytywnie zweryfikować hipotezę, zgodnie z którą rozwiązania normatywne przyjęte za podstawę funkcjonowania systemu PIT i umożliwiające udostępnianie za jego pośrednictwem kluczowych informacji przestrzennych Polski (w tym o charakterze krytycznym), nie gwarantują bezpieczeństwa państwa, przeciwnie, prowadzą do istotnych dla niego zagrożeń. W kontekście aktualnych uwarunkowań geopolitycznych, uwzględniając w szczególności nowe metody prowadzenia wojny hybrydowej oraz trwający konflikt zbrojny na Ukrainie, zastrzeżenia wobec gromadzenia i udostępniania informacji na temat polskiej infrastruktury teleinformatycznej, także krytycznej, są uzasadnione. PIT ma wprawdzie w założeniu doprowadzić do przyspieszenia i uproszczenia inwestycji w zakresie szybkich sieci łączności, wobec czego posiada on niewątpliwie istotne znaczenie dla rozwoju gospodarczego Polski. Jednakże proces zmierzający

[31] J. Larecki, *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Wydawnictwo „Książka i Wiedza", Warszawa 2007, s. 749-750.

[32] B. Saramak, *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Warszawa 2015, s. 116.

do uruchomienia tego systemu, a także jego funkcjonowanie zasługują na krytykę, mają nieprzemyślany charakter i mogą prowadzić do poważnych zagrożeń dla infrastruktury krytycznej państwa, a tym samym jego bezpieczeństwa, czego nie sposób zlekceważyć. Ponadto, przyjęte rozwiązania normatywne regulujące proces inwentaryzacji infrastruktury i usług telekomunikacyjnych, wykorzystywania w tym celu PIT i udostępniania za jego pośrednictwem gromadzonych danych, należy ocenić jako nieracjonalne, opracowane zbyt pośpiesznie oraz rodzące zbyt wiele wątpliwości i niedopowiedzeń. Za przedmiotowym wnioskiem dodatkowo przemawia brak odpowiednich przepisów wykonawczych (np. z art. 25c ust. 2 wruist), które gwarantowałyby, iż dostęp do informacji na temat obiektów o potencjalnym znaczeniu strategicznym byłby ograniczony. Należy przy tym zauważyć, iż przepisy regulujące funkcjonowanie PIT weszły w życie 1 stycznia 2017 r., podczas gdy jego chaotyczne uruchomienie w oparciu o naprędce opracowane przepisy nastąpiło dopiero w połowie stycznia 2023 r. Tym samym, podnoszone przez operatorów telekomunikacyjnych zastrzeżenia wyrażające obawy o zaistnienie potencjalnych zagrożeń dla infrastruktury krytycznej państwa należy uznać za w pełni uzasadnione[33]. Wymaga podkreślenia, iż prawo powinno być kształtowane w sposób zapewniający bezkonfliktowe i bezpieczne współistnienie całego społeczeństwa w ramach organizacji państwowej, umożliwiając urzeczywistnianie dobra wspólnego. Analizowane regulacje prawne, stwarzające przestrzeń dla wystąpienia potencjalnych zagrożeń dla całego państwa, stanowią natomiast zaprzeczenie powyższej misji.

[33] R. Chabasiński, *Punkt Informacyjny do spraw Telekomunikacji, czyli o tym, jak nie należy wdrażać dobrych pomysłów w fatalny sposób*, https://bezprawnik.pl/punkt-informacyjny-do-spraw-telekomunikacji/, dostęp 15.07.2024; Stowarzyszenie e-Południe, *List otwarty ws. inwentaryzacji sieci i usług w roku 2023*, https://isportal.pl/wp-content/uploads/2023/02/2023_02_09_pismo_protestacyjne_UKE_Art_29_Megaustawy_2023_PIT.pdf, dostęp 15.07.2024; M. Szutiak, *Polska wystawiona na druzgocący atak. Operatorzy przerażeni*, https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/uke-pit-mali-operatorzy-bunt, dostęp 15.07.2024; M. Maj, *Polskie światłowody, studzienki i inne obiekty, na jednej mapie… Te krytyczne też*, https://niebezpiecznik.pl/post/pit-uke-punkt-informacyjny-ds-telekomunikacji-mapa/, dostęp 15.07.2024.

Bibliografia

Akty prawne

Ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (t.j. Dz. U. z 2024 r. poz. 34 z późn. zm.)

Ustawa z 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j. Dz. U. z 2023 r. poz. 122).

Ustawa z 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych (t.j. Dz. U. z 2023 r. poz. 733).

Ustawa z dnia 12 października 2012 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2012 r. poz. 1256).

Ustawa z 9 czerwca 2016 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2016 r. poz. 903).

Ustawa z dnia 30 sierpnia 2019 r. o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw (Dz. U. z 2019 r. poz. 1815 z późn. zm.).

Rozporządzenie Ministra Cyfryzacji z dnia 19 grudnia 2022 r. w sprawie inwentaryzacji infrastruktury i usług telekomunikacyjnych (t.j. Dz. U. z 2024 r. poz. 45).

Dyrektywa Parlamentu Europejskiego i Rady 2014/61/UE z 15 maja 2014 r. w sprawie środków mających na celu zmniejszenie kosztów realizacji szybkich sieci łączności elektronicznej (Dz. U. UE. L. z 2014 r. Nr 155, str. 1).

Projekt ustawy o zmianie ustawy o wspieraniu rozwoju usług i sieci telekomunikacyjnych oraz niektórych innych ustaw, druk nr 3484, Sejm VIII Kadencji.

Literatura

Baniak K., *Analiza zagrożeń telekomunikacyjnych sektora publicznego*, „Biblioteka Bezpieczeństwa Narodowego" 2007, t. 3, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/materialy-archiwalne/biblioteka-bezpieczenst/tom-3/1125,Bezpieczenstwo-w-telekomunikacji-i-teleinformatyce.html, dostęp 15.07.2024.

Dela P., *Założenia działań w cyberprzestrzeni*, Warszawa 2022.

Kitler W., *Bezpieczeństwo państwa a bezpieczeństwo narodowe*, [w:] *Aspekty prawne bezpieczeństwa narodowego RP. Część ogólna*, pod red. W. Kitlera, M. Czuryk, M. Karpiuka, Warszawa 2013.

Larecki J., *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007.

Lasota-Jędrzak A., *Bezpieczeństwo infrastruktury krytycznej państwa*, „Rocznik Bezpieczeństwa Morskiego" 2013, nr 3.

Milewski J., Identyfikacja infrastruktury krytycznej i jej zagrożeń, „Zeszyty Naukowe AON" 2016, nr 4.

Rinaldi S., Peerenboom J., Kelly T., *Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies*, „IEEE Control Systems" 2001, nr 6, https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies, dostęp 15.07.2024.

Saramak B., *Wykorzystanie otwartych źródeł informacji w działalności wywiadowczej: historia, praktyka, perspektywy*, Wydział Dziennikarstwa i Nauk Politycznych Uniwersytet Warszawski, Warszawa 2015.

Sokała W., *Paradygmat bezpieczeństwa – podstawy, historia, ewolucja*, [w:] Liedel K. (red.), *Transsektorowe obszary bezpieczeństwa narodowego*, Warszawa 2011.

Wisz A., *Bezpieczeństwo informacji w wojskowych sieciach teleinformatycznych*, „Biblioteka Bezpieczeństwa Narodowego" 2007, t. 3, https://www.bbn.gov.pl/pl/informacje-o-bbn/publikacje/materialy-archiwalne/biblioteka-bezpieczenst/tom-3/1125,Bezpieczenstwo-w-telekomunikacji-i-teleinformatyce.html, dostęp 15.07.2024.

Zięba R., *Pozimnowojenny paradygmat bezpieczeństwa międzynarodowego*, [w:] Zięba R. (red.), *Bezpieczeństwo międzynarodowe po zimnej wojnie*, Warszawa 2008.

Żuber M., Infrastruktura krytyczna państwa jako obszar potencjalnego oddziaływania terrorystycznego, „Rocznik Bezpieczeństwa Międzynarodowego" 2014, nr 2, https://rocznikbezpieczenstwa.pl/ojs/index.php/rbm/article/view/338, dostęp 15.07.2024.

Źródła internetowe

Biuro Bezpieczeństwa Narodowego, *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, https://www.bialystok.ap.gov.pl/arch/teksty/biala_ksiega.pdf, dostęp 15.07.2024.

Byzdra K., *Infrastruktura krytyczna w ruinie. Ukraiński minister publikuje dane*, https://energetyka24.com/elektroenergetyka/wiadomosci/infrastruktura-krytyczna-w-ruinie-ukrainski-minister-publikuje-dane, dostęp 15.07.2024.

Chabasiński R., *Punkt Informacyjny do spraw Telekomunikacji, czyli o tym, jak nie należy wdrażać dobrych pomysłów w fatalny sposób*, https://bezprawnik.pl/punkt-informacyjny-do-spraw-telekomunikacji/, dostęp 15.07.2024.

Maj M., *Polskie światłowody, studzienki i inne obiekty, na jednej mapie… Te krytyczne też*, https://niebezpiecznik.pl/post/pit-uke-punkt-informacyjny-ds-telekomunikacji-mapa/, dostęp 15.07.2024.

Rojas R., McGee J., Lee E., Cavendish S., *When Nashville Bombing Hit a Telecom Hub, the Ripples Reached Far Beyond*, https://www.nytimes.com/2020/12/29/us/nashville-bombing-telecommunications.html, dostęp 15.07.2024.

Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2013. Załącznik 1 – Charakterystyka systemów infrastruktury krytycznej*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, dostęp 15.07.2024.

Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2020. Załącznik 1 – Standardy służące zapewnieniu sprawnego funkcjonowania infrastruktury krytycznej – dobre praktyki i rekomendacje*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, dostęp 15.07.2024.

Rządowe Centrum Bezpieczeństwa, *Narodowy Program Ochrony Infrastruktury Krytycznej 2020*, https://www.gov.pl/web/rcb/narodowy-program-ochrony-infrastruktury-krytycznej, dostęp 15.07.2024.

Stowarzyszenie e-Południe, *List otwarty ws. inwentaryzacji sieci i usług w roku 2023*, https://isportal.pl/wp-content/uploads/2023/02/2023_02_09_pismo_protestacyjne_UKE_Art_29_Megaustawy_2023_PIT.pdf, dostęp 15.07.2024.

Szutiak M., *Polska wystawiona na druzgocący atak. Operatorzy przerażeni*, https://www.telepolis.pl/wiadomosci/prawo-finanse-statystyki/uke-pit-mali-operatorzy-bunt, dostęp 15.07.2024.

Turak N., Macias A., *Russian strikes hit critical infrastructure in western city of Lviv; UN to vote on new peace resolution*, https://www.cnbc.com/2023/02/16/russia-ukraine-live-updates.html, dostęp 15.07.2024.

Wykaz skrótów

PIT – Punkt Informacyjny do spraw Telekomunikacji

NPOIK – Narodowy Program Ochrony Infrastruktury Krytycznej

RCB – Rządowe Centrum Bezpieczeństwa

UKE – Urząd Komunikacji Elektronicznej