Piotr LEWANDOWSKI
Łukasiewicz – ORGMASZ
Centrum Oceny Technologii;
Akademia Sztuki Wojennej[1]
piotr.lewandowski@orgmasz.lukasiewicz.gov.pl
https://orcid.org/0000-0002-3664-4815
https://doi.org/10.34739/dsd.2022.01.09

RACJA STANU POLSKI W CYBERPRZESTRZENI I CYBERBEZPIECZEŃSTWIE

ABSTRAKT: Artykuł ma za zadanie rozpocząć dyskusję nad problemem polskiej racji stanu w cyberprzestrzeni. Dlatego założeniem pracy jest odniesienie się do dokumentów strategicznych i wypracowanie na ich podstawie warunków brzegowych dla weryfikacji pojęcia racji stanu w cyberprzestrzeni. Praca dostarcza dwa elementy naukowe. Pierwszym z nich jest propozycja pomiaru na wysokim szczeblu ogólności racji stanu w cyberprzestrzeni przy użyciu narzędzi wywodzących się z realizmu i konstruktywizmu. Drugi to weryfikacja możliwości aplikacji owego narzędzia w stosunku do dokumentów o znaczeniu strategicznym oraz określenie jakościowej racji stanu na zaproponowanym modelu badawczym. Tekst otwiera metodyczne rozważania nad budowa narzędzi do badania racji stanu Polski w obszarze cyberprzestrzeni. Artykuł wskazuje na sekurytyzację jako główny czynnik rozpatrywania racji stanu w cyberprzestrzeni w Polsce połączony z właściwością działań defensywnych.

SŁOWA KLUCZOWE: bezpieczeństwo międzynarodowe, cyberbezpieczeństwo, cyberprzestrzeń, racja stanu

THE RAISON D'ETRE OF POLAND IN CYBERSPACE AND CYBERSECURITY

ABSTRACT: The aim of the article is to start a discussion on the problem of the Polish reason of state in cyberspace. Therefore the assumption of the work is to refer to strategic documents and to work out on their basis the boundary conditions for the verification of the notion of the reason of state in cyberspace. The work provides two scientific elements. The first one is a proposal to measure at a high level of generality the reason of state in cyberspace using tools derived from realism and constructivism. The second is the verification of the applicability of this tool to documents of strategic importance and the determination of a qualitative reason of state on the proposed research model. The text opens with a methodical consideration of the construction of tools for researching Poland's reason of state in the area of cyberspace. The article points to securitization as the main factor for considering Poland's reason of state in cyberspace combined with the property of defensive actions.

KEYWORDS: international security, cybersecurity, cyberspace, reason of state

[1] The War Studies University, Poland.

WSTĘP

Cyberprzestrzeń to nowy obszar aktywności politycznej państw. Rozwój technologii wykształcił przestrzeń społeczną o niesprecyzowanych granicach i właściwościach, która staje się naturalnym obszarem rywalizacji państw. W związku z tym ważne jest określenie prymarnych właściwości na potrzeby realizacji interesu państwa polskiego w tym w szczególności określenie percepcji racji stanu w obszarze cyberprzestrzeni.

Celem niniejszej pracy jest wypracowanie i zaproponowanie ram analizy pojęcia racji stanu w cyberprzestrzeni. W związku z tym problemem badawczy sformułowany został w postaci pytania: w jaki sposób państwo polskie określa na poziomie strategicznym wymiary teoretyczne racji stanu w cyberprzestrzeni? By odpowiedzieć na to pytanie skonstruowany został operat teoretyczny w postaci matrycy skupiający się na ogólnych wyznacznikach semantycznych racji stanu. Tekst określa rację stanu jako przedmiot badania i ostatecznie wypracowuje kategorię teoretyczną i operacyjną racji stanu polski w cyberprzestrzeni w oparciu o akty normatywne odniesione do klas zagrożeń.

Racja stanu jest pojęciem wywodzącym się z jeszcze z czasów starożytnych. Przez wieki koncepcja racji stanu ewoluowała do czasów współczesnych, w których to mierzy się z nowymi zjawiskami społeczno-politycznymi. Zakres zmian, jakie zachodzą w środowisku bezpieczeństwa poprzez globalizację i usieciowienie relacji międzynarodowych, powoduje, że racja stanu z jednej strony traci istotnie na znaczeniu, z drugiej zaś wyjątkowo zyskuje w relacjach międzypaństwowych. Przede wszystkim następuje odarcie pojęcia racji stanu z zakresu jej przeszłości odnoszącej się do tradycji arystotelesowsko-tomistycznej, machiawelicznej oraz XIX-wiecznej odnoszącej się do narodowych koncesji tworzenia państw narodowych. To, co pozostaje, to uznanie racji stanu za zbiór nadrzędnych interesów państwa w środowisku bezpieczeństwa międzynarodowego.

Dotychczasowa różnorodność definiowania racji stanu zmusza do konstatacji, iż jest to pojęcie o „wyraźnie określonej treści, ale o nieostrych granicach”[2] interpretacyjnych. Przystępowanie zatem do badania racji stanu każdorazowo wymaga konceptualizacji na gruncie teoretycznym owego pojęcia oraz jego operacjonalizacji do narzędzia poznawczego.

Poprzez konceptualizację należy dokonać merytorycznego uzasadnienia wyboru określonego pryzmatu racji stanu, poprzez który dokonana zostanie analiza i proces badawczy. Z uwagi na charakter badania należy zwrócić się u koncepcjom realistycznym, takim, które łączą pojęcie racji stanu bezpośrednio z polityką państwa. Można tu zwrócić się ku pojęciu Agnieszki Kasińskiej-Metryki, która ujmuje rację stanu jako status „dyrektywy nakazującej prowadzić politykę tak, by

[2] J. Pietraś, *Racja stanu w polityce zagranicznej państwa* [w:] *Racja stanu. Historia, teoria, współczesność*, red. E. Olszewski, Lublin 1989, s. 39.

nieustannie powiększać potęgę państwa”[3]. Jest to jednak rozumienie ofensywne i wymaga uzupełnienia poprzez pryzmat obrony, a właściwie ochrony (sekurytyzacji).

Paradygmatem właściwym do rozstrzygania racji stanu jest realizm[4]. Należy wskazać, że zmieniający się charakter państwa w stosunkach i bezpieczeństwie międzynarodowym powoduje uszczuplenie prerogatyw suwerennych. Realizm polityczny pozwala sprowadzić pojęcie racji stanu do kategorii poznawczych o strukturze hierarchicznej[5]. W zakresie weryfikacji „koncepcja racji stanu modeluje proces prowadzenia polityki państwa czyli proces kierowania”[6]. Istnieje zatem możliwość badania racji stanu poprzez uwzględnienie państwocentrycznego odniesienia wywodzącego się z realizmu politycznego, z przyjęciem jego założeń oraz poprzez naniesienie na nie działań politycznych. W przypadku cyberbezpieczeństwa należy jednak wskazać, że w odniesieniu do „uwarunkowań o charakterze superterytorialnym nie można zawiązać trwale z określonym miejscem w przestrzeni, nad którym państwo mogłoby sprawować absolutną kontrolę”[7]. Dlatego cyberprzestrzeń pozostaje materią eksterytorialną, która w pewnej mierze stanowi nieodzowną domenę państwa. Do badania tej przestrzeni warto wykorzystać konstruktywizm (analiza dyskursu)[8], który w połączeniu z realizmem politycznym stworzy matrycę analityczną dla weryfikacji założeń strategicznych w zakresie sekurytyzacji cyberprzestrzeni.

Proponowana matryca analizy racji stanu Polski w zakresie bezpieczeństwa będzie odnosić się do realizmu politycznego wraz z jego wersjami w kategoriach postulatywnych i w tym wymiarze będzie czerpać z konstruktywizmu (analiza aktów prawnych). Dzięki temu powstanie możliwość skonceptualizowania racji stanu w cyberprzestrzeni, gdzie skalę stanowić będą wersje odnoszące się do realizmu politycznego. Racja stanu „przynależy przede wszystkim do poziomu praktyki politycznej” i jej analiza odnosi się do weryfikacji podmiotów decydujących oraz treści[9].

Rację stanu obecnie ujmuje się w zakresie pojęć odnoszących się do bezpieczeństwa (geopolitycznego i ekonomicznego) ze szczególnym uwzględnieniem aspektów gospodarczych[10]. Pryzmat panowania nad przestrzenią, w tym cyberprzestrzenią, posiada silny walor geoekonomicznej rywalizacji, zawłaszczania domeny państwowej, budowania granic legislacyjnych i wyznaczania żywotnych interesów. Wszystko to sprowadza rację stanu do uznania jej jako warunków rozwoju i formułowania reguł[11]. Cyberprzestrzeń nie wyklucza tradycyjnego podej-

[3] A. Kasińska-Metryka, *Racja stanu – teoretyczne dylematy, praktyczne wątpliwości* [w:] *Racja stanu Polski w Europie*, red. I. Kraś, R. Kubicki, Warszawa 2020, s. 25.
[4] I. Galewska, *Spór o rozumienie polskiej racji stanu na arenie Unii Europejskiej – wymiar teoretyczny i praktyczny*, „Zeszyty Naukowe Uniwersytetu Szczecińskiego” 2014, nr 837, s. 6–7.
[5] A. Krzynówek-Arndt, *Rzeczpospolita jako dobro wspólne* [w:] *Kryterium etyczne w koncepcji racji stanu*, Kraków 2013, s. 86.
[6] R. Stemplowski, *O kryterium etycznym w koncepcji racji stanu* [w:] *Kryterium etyczne w koncepcji racji stanu*, red. A. Krzynówek-Arndt, Kraków 2013, s. 15.
[7] J. A. Scholte, *Globalizacja. Krytyczne wprowadzenie*, Sosnowiec 2006, s. 212.
[8] T. G. Grosse, *Wejście do strefy euro a polska racja stanu* [w:] *Racja stanu Polski w Europie*, red. I. Kraś, R. Kubicki, Warszawa 2020, s. 92.
[9] R. Zenderowski, K. Cebul, *Polska racja stanu w obszarze Europy Środkowo-Wschodniej – wyznaczniki i wyzwania* [w:] *Racja stanu Polski w Europie*, red. I. Kraś, R. Kubicki, Warszawa 2020, s. 71.
[10] Ibidem, s. 92.
[11] K. Łastawski, *Polska racja stanu po wstąpieniu do Unii Europejskiej*, Warszawa 2009, s. 14.

ścia do racji stanu, ale rozkłada inaczej akcenty na hierarchizację interesów narodowych. Głównym punktem odniesienia będzie w tym wymiarze prowadzenie rzetelnej polityki informacyjnej oraz dążenie do wzmocnienia (zachowania) pozycji międzynarodowej państwa[12].

Racja stanu jako przedmiot poznania w cyberprzestrzeni należy do elementów jakościowej zmiany cywilizacyjnej. Zostało to dostrzeżone i wydaje się, że na gruncie działań polityczno-prawnych dochodzi do coraz silniejszego akcentowania aspektów takich jak uwzględnienie konieczności przyśpieszenia rozwoju technologicznego i ekonomicznego, a przez to (akumulację kapitałów) zwiększenie podmiotowości w strukturze międzynarodowej. Do tego potrzebne jest zwiększanie potencjałów (potęgi) w wymiarach m. in: gospodarczym, konkurencyjnym, innowacyjnym, intelektualnym (edukacyjnym)[13]. Polskie doświadczenia geopolityczne winny przekładać się na rywalizację geoekonomiczną w cyberprzestrzeni.

Wypada wskazać również i rozszerzyć zakres operacyjny pojęcia racji stanu o pryzmat sekurytyzacji. Do tej pory badania i analizy teoretyczne skupiały się na wymiernych aspektach sekurytyzacji militarnej, gospodarczej państwa[14]. Należy dokonać rozszerzenia ujęcia racji stanu w odniesieniu do sekurytyzacji w całości aktywności państwa, w tym również w cyberprzestrzeni. Istota racji stanu sprowadza się do „ochrony państwa traktowanego w kategoriach szczególnej wartości”[15] i odnosi się do „najistotniejszych właściwości państwa poprzez strategie i interesy narodowe z uwzględnieniem metod, etapów i środków działania na rzecz ochrony istoty państwa”[16].

Powyżej zaprezentowane podejście jest oryginalne i wynika z połączenia teoretycznych konceptualizacji oraz coraz częściej przejawiających się praktycznych wyników analiz racji stanu. Na przestrzeni zastosowanej tu metodologii przenikają się realizm i konstruktywizm. Takie połączenie jest właściwe do proponowanej metody analizy kluczowych aktów prawnych z zakresu cyberprzestrzeni i cyberbezpieczeństwa Polski: Ustawy o krajowym systemie cyberbezpieczeństwa z 2018 r. oraz Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019–2024. Celem analizy jest określenie, w jakim stopniu realizowana jest racja stanu Polski w cyberprzestrzeni, oraz zidentyfikowanie strategicznych zagrożeń dla racji stanu Polski w cyberprzestrzeni. Przy organizacji stopnia posłużono się zaproponowaną poniżej matrycą i miarą wyniesioną z nurtów realizmu politycznego, której uzupełnienie możliwe jest poprzez deskryptywną analizę tworzącą strategię państwa (konstruktywizm).

[12] M. Molendowska, *Od Trójkąta Wyszehradzkiego do Unii Europejskiej – pozycja Polski w zjednoczonej Europie* [w:] *Racja stanu Polski w Europie*, red. I. Kraś, R. Kubicki, Warszawa 2020, s. 168.
[13] K. Kik, *Polska racja stanu w warunkach członkostwa w UE i NATO* [w:] *Racja stanu Polski w Europie*, red. I. Kraś, R. Kubicki, Warszawa 2020, s. 57.
[14] P. Lewandowski, *Poland's Reason of State in the Creation of a New International Order. Foreign Policy as Poland's Reason of State in the 21st Century*, „Polish Political Science Yearbook” 2021, nr 50, s. 1–15.
[15] R. Zenderowski, K. Cebul, op. cit., s. 71.
[16] P. Lewandowski, *Racja stanu w warunkach postsuwerenności i sieciowości międzynarodowej państw* [w:] *Polska racja stanu w perspektywie globalnych przemian*, red. P. Grochmalski, P. Lewandowski, P. Paszak, Warszawa 2020, s. 97.

Rozumienie racji stanu w realizmie		
ofensywne w wersji mocnej	ofensywno-defensywne	defensywne w wersji słabej
ofensywne w wersji słabej		defensywne w wersji mocnej

Tabela 1. Matryca interpretacji racji stanu w zależności od nurtu realizmu politycznego
Źródło: Opracowanie własne.

W zakresie racji stanu ofensywnej w wersji mocnej zakłada się dominację jednoznacznych sformułowań ukierunkowujących działania samowładne, mówiące o narodowym rozwoju systemów autonomicznych, pomnażaniu potęgi krajowej, dążeniu do pozycji mocarstwowej. Będą to postulaty aktywne, zaczepne, ukierunkowane na działania wyprzedzające. Racja stanu ofensywna w wersji słabej pozwala określić się w narracjach odnoszących się do wypracowywania potęgi współdzielonej, wykreowanej wspólnotowo w ramach sojuszy, układów przy jednoczesnym akcentowaniu dążenia do uzyskania przewag.

Racja stanu w rozumieniu ofensywno-defensywnym odnosi się do takich sformułowań, które będą łączyć i równoważyć narracje zarówno wynikające z działań ofensywnych w wersji mocnej i słabej, jak i defensywnej w wersji mocnej i słabej. Racja stanu w wersji defensywnej słabej posiada aspekty mówiące o potrzebie ochrony, przeciwdziałania a także rozbudowie systemów bezpieczeństwa krajowego w oparciu o rozwiązania zewnętrzne. W wersji tej pojawiają się deklaracje o budowie pozycji międzynarodowej w szerszym kontekście strategicznym, jak również o konieczności ciągłego doskonalenia się (dążenie do potęgi) w zakresie zdolności obronnych. Racja stanu w wersji defensywnej mocnej to wskazanie na konieczność budowy własnych, narodowych systemów bezpieczeństwa skupionych na działaniach zachowawczych, obronnych, ochronnych i protekcyjnych względem dobrych praktyk i rozwiązań międzynarodowych[17].

Powyższa matryca i kompleks znaczeniowy posłużyły do przeprowadzenia analizy aktów prawnych pod względem ich właściwości dla racji stanu Polski w środowisku cyberprzestrzeni. Racja stanu prezentowana jest jako model poznawczy, pryzmat rozstrzygania o jakości strategii bezpieczeństwa państwa oraz definiowaniu zagrożeń w cyberprzestrzeni.

CYBERPRZESTRZEŃ JAKO OBSZAR REALIZACJI RACJI STANU PAŃSTWA

Obecną sytuację cyberprzestrzeni w Polsce reguluje Ustawa o krajowym systemie cyberbezpieczeństwa z 2018 r., która stanowi implementację Dyrektywy NIS (Dyrektywa 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

[17] Na podstawie: A. Wojciuk, *Dylemat potęgi*, Warszawa 2010.

Unii)[18]. Dyrektywa narzuca trzy filary realizacji działań narodowych i wspólnotowych, których rozwinięcie stanowi ustawa.

Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa definiuje cyberbezpieczeństwo jako „odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te system"[19]. W ten sposób definiowane jest całe środowisko cyberprzestrzeni obejmujące zarówno infrastrukturę w postaci systemów, jak i aspekt społeczny odnoszący się do autentyczności i działalności w tychże systemach. Należy jednak zwrócić uwagę, że systemy te obejmują całość infrastruktury telekomunikacyjnej co przekłada się na aspekt nie tylko bezpieczeństwa informatycznego, lecz także informacyjnego, co również osobno ujmuje ustawa. W zakresie racji stanu w definicji przebija się wyraźnie aspekt defensywny realizmu politycznego poprzez uznanie cyberbezpieczeństwa jako odporności. Z założenia systemy mają być odporne na ataki, a jednocześnie brakuje jakichkolwiek form wyprzedzających (prewencyjnych).

Racja stanu przejawia się tu w zdefiniowaniu pola działalności, które jest obszerne poprzez objęcie całości działań komunikacyjnych odbywających się w obszarze systemów informatycznych (teleinformatycznych) oraz procesach i zjawiskach społecznych z tym związanych. Nie ulega przy tym wątpliwości, że są one składową „żywotnych interesów państwa" w zakresie rozumienia definicyjnego racji stanu[20]. Ustawa dookreśla, że cyberbezpieczeństwo to zakres „niezakłóconego świadczenia usług kluczowych i usług cyfrowych, przez osiągnięcie odpowiedniego poziomu bezpieczeństwa systemów informacyjnych służących do świadczenia tych usług oraz zapewnienie obsługi incydentów".

Pojawiają się tu dwa rozróżnienia racji stanu: ofensywne i defensywne przy czym akcent zdecydowanie silniej pada na ten drugi aspekt. Ofensywność racji stanu w zakresie cyberbezpieczeństwa reprezentowany jest poprzez sekurytyzację systemów zarówno techniczną, jak i społeczną. Pojawiają się przy tym dwa niemierzalne poziomy realizacji: ciągłość świadczenia usług oraz osiągnięcie odpowiedniego poziomu ochrony. W przypadku pierwszego przebija się tu konieczność zwrócenia uwagi, że każdy incydent będzie spowalniał, zakłócał ciągłość (tu istnieje możliwość weryfikacji)[21].

Znacznie bardziej interesujące w kontekście racji stanu jest podejście do osiągnięcia odpowiedniego poziomu w cyberbezpieczeństwie. Założenie to wynika z realizmu politycznego i zwraca uwagę na paradoks bezpieczeństwa oraz konieczność budowania potęgi rozumianej jako

[18] *Dyrektywa 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,* https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/dyrektywa_NIS-1-Dyrektywa-NIS-3.pdf

[19] *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa* [dalej: *Ustawa o KSC*], https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560 (20.01.2022).

[20] W. Pokruszyński, *Etymologia polityki i strategii bezpieczeństwa w świetle wyzwań i zagrożeń xxi wieku*, „Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje" 2016, nr 22, s. 375.

[21] *Agile cybersecurity, czyli bezpieczeństwo w dobie chmury i powszechności pracy zdalnej, Raport specjalny*, red. A. Gontars, s. 15, https://www.atsummit.pl/wp-content/uploads/2020/11/ATS2020_online.pdf (21.01.2022).

zdolności ofensywnej i defensywnej państwa. Powyższe przeświadczenie uniemożliwia osiągnięcie bezpieczeństwa państwa w kwestii poziomu. Osiągnięcie go jest niemożliwe. Ciągłe doskonalenie się w zakresie bezpieczeństwa cybernetycznego powoduje popadnięcie w paradoks bezpieczeństwa. Jest ono silnie reprezentowane zarówno w Ustawie, jak i w Strategii.

Racja stanu Polski w zakresie cyberbezpieczeństwa podlega instytucjonalizacji i organizacji. W skład krajowego systemu cyberbezpieczeństwa wchodzą podmioty prywatne, państwowe oraz instytucje nadzoru. W przypadku instytucji prywatnych rozróżnia się je na operatorów i dostawców. W sumie ustawa wyróżnia 20 podmiotów odpowiedzialnych za cyberbezpieczeństwo w Polsce. Nie jest to jednak suma wszystkich podmiotów, gdyż wśród nich znajdują się „instytuty badawcze" czy „organy właściwe ds. cyberbezpieczeństwa". Niemniej da się wyróżnić kilka kluczowych podmiotów, za które uznać należy: CSIRT MON, CSIRT NASK, CSIRT GOV, które wraz z organami właściwymi ds. cyberbezpieczeństwa, ministrem właściwym do spraw informatyzacji i pełnomocnikiem ds. cyberbezpieczeństwa stanowią system zarządzania ryzykiem na poziomie krajowym[22].

Ustawa nakłada obowiązki na operatorów, dostawców oraz podmioty publiczne oraz wskazuje zadania dla CSIRT MON, CSIRT NASK, CSIRT GOV. W przypadku tych ostatnich zostały one obarczone odpowiedzialnością za krajowy system bezpieczeństwa. Posiadają szereg zadań i prerogatyw względem pozostałych podmiotów, jak również zobowiązane są do współpracy krajowej i zagranicznej w ramach kształtowania międzynarodowego środowiska cyberbezpieczeństwa. Do zadań CSIRT MON, CSIRT NASK, CSIRT GOV należą: monitoring zagrożeń, szacowanie ryzyka, agregowanie informacji o incydentach, reagowanie na incydenty, klasyfikowanie ich, prowadzenie badań, prowadzenie współpracy między instytucjami krajowymi, współpraca międzynarodowa z siecią CSIRT, raportowanie, budowa zaplecza analitycznego, przyjmowanie zgłoszeń[23]. W rzeczywistości to właśnie te trzy instytucje stoją na straży cyberbezpieczeństwa w Polsce posiadając najszersze kompetencje oraz zadania.

Powyższy zakres działań wyraźnie plasuje polską rację stanu w zakresie cyberbezpieczeństwa po stronie realizmu defensywnego. Ustawa odnosi się do budowy systemu obronnego, w którym jednym z założeń jest prowadzenie badań, w których to można upatrywać się właściwości rozwojowych w zakresie technologii cyfrowej. W szerokiej mierze ustawa bazuje na podmiotach prywatnych, w których to gestii pozostaje znaczna część infrastruktury cyfrowej. To one też będą stanowić czynnik rozwojowy w zakresie innowacji i wdrożeń technologicznych.

Do uszczegółowienia zagadnień została uchwalana Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019–2024, która zastąpiła dotychczasowy dokument strategiczny – Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022. Strategia Cyberbezpieczeństwa RP określa, że cyberprzestrzeń to „przestrzeń

[22] *Ustawa o KSC.*
[23] *Ibidem.*

przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne”[24]. Tak szeroka definicja mieści w sobie wszystkie systemy komunikacji i przetwarzania informacji. W zakresie racji stanu jest to spojrzenie holistyczne, rozszerzające, a zatem odnoszące się do istoty cyberprzestrzeni, która jest eksterytorialna i narodowa jednocześnie.

Strategia określa powyższy paradoks poprzez pryzmat idei neoliberalnych, co jednoznacznie stawia ujęcie racji stanu w nurcie defensywnym, traktując, że cyberbezpieczeństwo to „bezpieczeństwo obrotu gospodarczego, poczucie bezpieczeństwa obywateli, sprawność funkcjonowania instytucji sektora publicznego, przebieg procesów produkcyjnych i usługowych, a w rezultacie na ogólnie pojmowane bezpieczeństwo narodowe”[25]. Jednocześnie Strategia określa, że cyberbezpieczeństwo realizowane jest w krajowych systemach cyberbezpieczeństwa, o których szczegółowo traktuje Ustawa, oraz międzynarodowych ramach kształtowanych przez UE, ONZ, NATO, OBWE[26].

Strategia ma istotne znaczenie w zakresie definiowania polskiej racji stanu w obszarze cyberbezpieczeństwa zarówno w wymiarze bezpieczeństwa wewnętrznego, jak i zewnętrznego[27]. Strategia powinna uwzględniać rację stanu państwa w obszarze nieobjętym granicami państwa, które odnoszą się do zagrożeń takich jak: naruszenie poufności, integralność czy autentyczność i dostępność przetwarzania danych.

Strategia ma jednak wadę prawną z uwagi na sposób jej uchwalenia w drodze uchwały a nie ustawy, co powoduje, że nie wszystkie podmioty ujęte w Ustawie zostaną zobligowane do jej realizacji. Niemniej odnosząc się do organów administracji państwowej prezentuje realną wizję i cele, które są istotne w kontekście analizy racji stanu Polski w cyberprzestrzeni i cyberbezpieczeństwa[28].

Strategia w zakresie cyberbezpieczeństwa Polski odnosi się do nurtu defensywnego. Kontekst strategiczny bezpieczeństwa RP określony został jako „odporności systemów informacyjnych operatorów usług kluczowych, operatorów infrastruktury krytycznej, dostawców usług cyfrowych oraz administracji publicznej na cyberzagrożenia, a także zwiększenie poziomu ochrony informacji w systemach informacyjnych przez standaryzację zabezpieczeń”[29]. Jednocześnie mowa o podniesieniu zakresu bezpieczeństwa narodowego i zwiększeniu skuteczności organów państwowych. Uchwała w wymiarze strategicznym kwalifikuje się do nurtu defensywnego w wersji słabej.

---

[24] *Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019–2024* [dalej: *Strategia CRP*], https://www.dziennikustaw.gov.pl/MP/rok/2019/pozycja/1037 (20.01.2022).
[25] Ibidem.
[26] K. Chałubińska-Jentkiewicz, *Cyberspace as an Area of Legal Regulation* [w:] *Cybersecurity in Poland Legal Aspects*, red. K. Chałubińska-Jentkiewicz, Springer Open Acces 2021, s. 24–30.
[27] B. Olszewski*, Ewolucja cyberbezpieczeństwa w strategiach NATO*; *The Evolution of Cybersecurity in NATO Strategies*, [w:] *Bezpieczeństwo europejskie po szczycie NATO w Warszawie*, pod red. P. Turczyński, Kraków 2019.
[28] W. Kitler, *Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej*, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, Warszawa 2019, s. 2.
[29] *Strategia CRP*.

Istotnie czynnik defensywny przeważa nad ofensywnym w polskiej myśli strategicznej w zakresie cyberbezpieczeństwa. Podporządkowanie całości procesów siłom zbrojnym RP odbywa się poprzez określenie ich zdolności w układzie sieciowym (państwo-sojusznicy) do prowadzenia działań o charakterze militarnym, jednak każdorazowo, w momencie, w którym pojawi się „konieczność działań obronnych".

Wizja zakłada rozwój gospodarczy Polski: zasobność, efektywność, sprawność, wzrost aktywności społecznej, co wymaga wzmacniania potencjału cyberbezpieczeństwa, wdrożenia rozwiązań systemowych (organizacyjnych, operacyjnych, technologicznych, prawnych) czy kreowania postaw społecznych i naukowych. Wizja jest nieprecyzyjna, ale pozwala na wskazanie dominującego w niej czynnika geoekonomicznego, który przerzuca ciężar rywalizacji międzynarodowej z dziedzin militarnej i politycznej na właściwości ekonomiczno-gospodarcze. Ta właściwość powoduje zwrot ku ujęciu neoliberalnemu. Jednak w założeniu ogólnym widać podejście ofensywno-defensywne, za które odpowiada wizja rozwoju systemów cyberbezpieczeństwa. Do nich dochodzą jeszcze aspekty etyczne odnoszące się do ideologizacji relacji społecznych w zakresie promowania wolności i zasad demokratycznych.

Dla zobrazowania polskiej racji stanu w zakresie cyberbezpieczeństwa należy dokonać dekonstrukcji narracyjnej celu Strategii, która traktuje o odporności, poziome ochrony i promowaniu. Przebija się tu założenie defensywne w wersji słabej poprzez budowę systemów ochronnych przy jedynym założeniu promowania postaw społecznych ukierunkowanych przeciw zagrożeniom płynącym z cyberberprzestrzeni. Trzykrotnie w celu pojawia się aspekt defensywny: odporność, poziom ochrony i ochrona, i raz aspekt ofensywny: promocja jako działanie.

Inaczej rzecz ma się w przypadku celów szczegółowych. Dokonując ich dekompozycji, należy wskazać, że stoją w sprzeczności z wcześniejszymi przekazami odnoszącymi się do nurtu defensywnego. Na pięć celów szczegółowych cztery można uznać za ofensywne, a jeden za defensywny. W odniesieniu do weryfikacji narracyjnej trzeba wskazać, że ofensywne są te mówiące o rozwoju, zwiększaniu potencjału, budowie i silnej pozycji Polski w cyberprzestrzeni, a defensywne sformułowania to te traktujące o odporności i zapobieganiu. W świetle tego przekazu można uznać, że cele polskiej racji stanu w cyberprzestrzeni o charakterze ofensywnym to działania na rzecz rozwoju wewnętrznego systemu cyberbezpieczeństwa, zwiększanie świadomości i kompetencji oraz potencjału narodowego na jego rzecz, a także maksymalizacja statusu do poziomu uzyskania potęgi o znaczeniu regionalnym w tym obszarze. Racja stanu realizuje się w wymiarze teleologicznym jako wizja ofensywna o wysokim statusie operacyjnym z wysokim poziomem znaczenia międzynarodowego Polski.

Analizując wizję cyberbezpieczeństwa w kontekście racji stanu jako modelu realizacji polityki bezpieczeństwa (sekurytyzacji)[30] należy wskazać, że następuje przeniesienie ciężaru odpowiedzialności państwa na sektor pozapaństwowy wraz ze stymulowaniem jego rozwoju. Jest to widoczne chociażby po kompetencjach poszczególnych instytucji i organów, jak np.

[30] P. Lewandowski, *Racja stanu…*, op. cit.

Kolegium ds. Cyberbezpieczeństwa przy Radzie Ministrów, które z założenia ma być organem opiniodawczo-doradczym, oraz prerogatywach operatorów i dostawców, po których stronie leży zapewnienie bezpieczeństwa usług.

Podniesienie efektywności systemu cyberbezpieczeństwa w Polsce będzie realizowane poprzez współpracę, rekomendowanie, obsługę incydentów, szacowanie ryzyk, ostrzeganie i zalecenia kierowane do instytucji i społeczeństwa. W zakresie operacyjnym dużo uwagi poświęca się wymianie doświadczeń, dzieleniu wiedzy, wdrożeniu komponentów poznawczych oraz kształtowaniu kompetencji technologicznych do budowy cyberodporności. Wdrożenie standaryzacji dla podmiotów państwowych i prywatnych pozwoli na uzyskanie wysokiego stopnia efektywności. Polska racja stanu realizuje się w zakresie ciągłego kształtowania systemów defensywnych łącznie z ćwiczeniami Sił Zbrojnych w tym właśnie zakresie.

Racja stanu Polski w cyberprzestrzeni odnosi się do żywotnych interesów państwa. Cyberbezpieczeństwo odpowiada za ciągłość działania państwa a zatem za jego egzystencjonalną istotę. Cyberprzestrzeń jest w istocie infrastrukturą krytyczną państwa, a systemy IT i OT zostały w strategii uznane za strategiczne dla istnienia wybranych sektorów np. energii. Oznacza to, że cyberprzestrzeń jest elementem prymarnym, wyznacznikiem państwa łączącym i rozszerzającym pojęcia terytorium, społeczeństwa i władzy. Rozprasza je geograficznie i skupia poprzez pryzmat rozwiązań legislacyjnych.

W zakresie operacyjnym, ofensywnym zakłada się włączenie dostawców i operatorów usług z zakresu cyberbezpieczeństwa w system zarządzania kryzysowego na szczeblu krajowym oraz poddanie pod współpracę sojuszniczą rozwiązań międzynarodowych z zakresu cyberbezpieczeństwa. Istotą zwiększania cyberbezpieczeństwa na szczeblu krajowym ma być stworzenie systemu do szacowania ryzyka. Ma to być metodyka rozumiana jako narzędzie do rozpoznawania poziomu zagrożeń. Została określona Narodowa Platforma Cyberbezpieczeństwa realizowana przez NASK PIB, Politechnikę Warszawską, Narodowe Centrum Badań Jądrowych oraz Instytut Łączności[31].

Racja stanu określana w zakresie rozwoju krajowego systemu cyberbezpieczeństwa ma charakter ofensywno-defensywny poprzez określanie narzędzi i metod działania, do których należy ściślejsza współpraca podmiotów prywatnych (cywilnych) i państwowych, wymiana informacji na szczeblu międzynarodowym, stworzenie bezpiecznych narzędzi komunikacji strategicznej, zwiększenie intensywności wymiany doświadczeń, podjęcie działań profilaktycznych, unikanie skutków cyberprzestępstw, stworzenie ścieżki działań na rzecz osób poszkodowanych.

Podniesienie poziomu odporności cyberprzestrzeni zakłada wdrożenie:

- zaleceń oraz dobrych praktyk w działaniach administracyjnych;
- norm bezpieczeństwa (Polskich Norm) opartych o standardy międzynarodowe;
- zabezpieczeń technicznych oraz legislacyjnych;

[31] *Narodowa Platforma Cyberbezpieczeństwa*, https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2088,Narodowa-Platforma-Cyberbezpieczenstwa-NPC.html (22.01.2022).

- ocen i certyfikacji dla sprzętu i produktów działających w cyberprzestrzeni;
- krajowego systemu oceny i certyfikacji oraz testów i audytu.

Są to realne działania zmierzające do poprawy bezpieczeństwa. Bazują na działaniach wyprzedzających, są prewencyjne i zmierzają do zawłaszczenia, zagospodarowania cyberprzestrzeni. Dodatkowo powstający krajowy system oceny i certyfikacji ma powstać jako wynik współpracy międzynarodowej, ale jego zadaniem jest wypracowanie przewag rynkowych i konkurencyjnych dla polskich producentów.

W przypadku zwiększenia potencjału narodowego w obszarze cyberbezpieczeństwa rząd zakłada zwiększenie inwestycji infrastrukturalnych, rozbudowę systemów cyberbezpieczeństwa oraz poprawę warunków funkcjonowania obecnych podmiotów ds. cyberbezpieczeństwa. Zakłada się przy tym inicjowanie i rozwój start-upów czy nowych ośrodków naukowo-badawczych. Widoczna staje się również priorytetyzacja celów działania, które można określić jako ofensywne, a będą to: rozwój kompetencji w zakresie projektowania, programowania jako szczególnych umiejętności polskiego sektora IT, które mają przełożyć się na wzrost konkurencyjności polskiego przemysłu cybernetycznego. Podnosi się przy tym kwestię pozyskania inwestycji międzynarodowych.

Za elementy systemu bezpieczeństwa uznaje się wiedzę. Jej rozwój ma gwarantować wzrost jakości cyberbezpieczeństwa krajowego. Wiedza rozumiana poprzez pryzmat innowacyjności ma być rozwijana w sposób systemowy i strategiczny poprzez wsparcie biznesu (tu głównie w aspekcie wyrównywania szans względem międzynarodowej konkurencji), wypracowanie systemu partnerstw między sektorem publicznym i prywatnym (PPP, ang. *public-private partnership*) oraz między biznesem a nauką (B+R, ang. *business to research*) oraz poprzez programy badawcze realizowane we współpracy z NCBiR (programy oceny, metod i procesów cyberbezpieczeństwa).

Potencjał narodowy cyberbezpieczeństwa będzie realizowany również przez pryzmat militarny jako nadrzędny wobec ochrony bezpieczeństwa i suwerenności państwa. Stosując matrycę narracyjną można wskazać, że konceptualizacja działań militarnych ma charakter ofensywno-defensywny. Widać to poprzez silne zorientowanie na skupieniu aspektów militarnych w zakresie spectrum: rozpoznania, ochrony, obrony i zwalczania. Do aspektów ofensywnych można zaliczyć prewencję w postaci rozpoznania, pozostałe aspekty są defensywne.

Za działania ofensywne w kontekście realizacji militarnego aspektu racji stanu w cyberprzestrzeni należy uznać:

- planowanie operacji (samodzielnie oraz w działaniach sojuszniczych i międzynarodowych),
- udoskonalanie i tworzenie nowych formacji ds. cyberbezpieczeństwa,
- rozwój zdolności rozpoznawania, zapobiegania i zwalczania cyberzagrożeń,
- przyjęcie strategii interoperacyjności opartej o działanie sieciowe i kooperację służb,
- podnoszenie kwalifikacji kadr,

– kreację lub nabycie nowych, innowacyjnych narzędzi i metod operacyjnych w cyberprzestrzeni.

Można zatem uznać, że włączenie czynnika militarnego w działania z zakresu cyberbezpieczeństwa najsilniej koreluje z nurtem ofensywnym w wersji słabej.

Strategia zakłada zwiększanie świadomości i kompetencji społecznych, które sytuują się w działaniach defensywnych i są to m.in. stałe podnoszenie kwalifikacji kadry administracyjnej, budowa określonych modeli edukacyjnych z planem wyłonienia ekspertów ds. cyberbezpieczeństwa, a także zmiany w programach edukacyjnych i programach studiów. Rząd zakłada realizację szkoleń sektorowych dla służb. Z miękkich działań społecznych przewidziany został plan zachęt, zmiany zarobków, uwrażliwianie społeczeństwa na cyberzagrożenia oraz działanie w mediach (kampanie społeczne). Rząd zamierza rozwijać sektor *fact checking*.

Budowa silnej pozycji międzynarodowej w zakresie polskiej racji stanu w cyberprzestrzeni odnosi się do współpracy w ramach NATO i UE. Celem tej współpracy ma stać się wypracowanie jednolitego rynku prawnego i gospodarczego dla podmiotów i społeczeństw, wytworzenie bezpiecznego środowiska współpracy międzynarodowej w cyberprzestrzeni, jak również działanie na rzecz wzrostu gospodarczego i poziomu innowacji. Prerogatywy strategiczne takie jak odstraszanie, obronność i odporność oraz reagowanie na zagrożenia jednoznacznie określają defensywny charakter racji stanu w zakresie budowy pozycji międzynarodowej. Przebija się pasywne stanowisko kładące strategiczny nacisk na rozwiązania głównego filaru w postaci NATO. Jednocześnie wzmocnienie polskiej pozycji międzynarodowej jako element polskiej racji stanu w zakresie cyberprzestrzeni polega na promowaniu rozwiązań Karty Narodów Zjednoczonych dla cyberprzestrzeni, promowaniu współpracy regionalnej w ramach Grupy Wyszehradzkiej i Trójmorza, zawieraniu umów wielostronnych i bilateralnych oraz ścisłej wewnętrznej koordynacji w celu wypromowania zaplecza kadrowego i technologicznego dla tychże porozumień.

ANALIZA DOKUMENTÓW STRATEGICZNYCH Z ZAKRESU CYBERBEZPIECZEŃSTWA POD WZGLĘDEM IDENTYFIKACJI ZAGROŻEŃ

Strategia podaje definicję cyberzagrożenia zgodną z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA, w którym to „cyberzagrożenie to wszelkie potencjalne okoliczności, zdarzenie lub działanie, które mogą wyrządzić szkodę, spowodować zakłócenia lub w inny sposób niekorzystnie wpłynąć w przypadku sieci i systemów teleinformatycznych, użytkowników takich systemów oraz innych osób". W projekcie zmiany ustawy z 2021 r. możemy znaleźć rozszerzoną definicję cyberzagrożeń, która odnosi się do „systemów informacyjnych, użytkowników takich systemów oraz

innych osób”[32]. Rozszerzenie nastąpiło poprzez wykluczenie sieci jako domeny realizacji cyberprzestrzeni oraz zastąpienie systemów teleinformatycznych systemami informacyjnymi. Jest to o tyle istotne, iż w związku z działaniami hybrydowymi podjętymi przeciwko Polsce w postaci działań dezinformacyjnych, propagandowych można szerzej objąć spectrum działań zapobiegawczych.

Racja stanu Polski realizowana jest poprzez ofensywne działania wykierowane w zapobieganie incydentów (zagrożenia), które określane są jako materialne i wizerunkowe. W zakresie materialnych odnoszą się do aspektów geoekonomicznej rywalizacji oraz strat wynikających z działań jednostek i grup przestępczych. Straty wizerunkowe w kontekście racji stanu odnoszą się bezpośrednio do państwa, jego stabilności, zdolności ofensywnych, prestiżu międzynarodowego umniejszając *soft power*. W zakresie racji stanu głównymi zagrożeniami są grupy sponsorowane przez państwa „prowadzące ofensywne działania” w cyberprzestrzeni. W tym zakresie mowa o cyberszpiegostwie i rozpoznaniu zdolności operacyjnych. Jednocześnie racja stanu w kontekście zagrożeń rozumiana jest silnie jako ochrona. To jednoznacznie nakazuje usytuować rozumienie polskiej racji stanu w nurcie defensywnym.

W kontekście strategicznym pojawiają się defensywne odniesienia w zakresie bezpieczeństwa narodowego traktujące o konieczności zwiększenia skuteczności działań organów ścigania oraz wymiaru sprawiedliwości. Zakłada się przy tym możliwość występowania działań o charakterze hybrydowym i terrorystycznym w cyberprzestrzeni. Jednym z głównych zagrożeń pozostaje natomiast szpiegostwo.

W przypadku szczególnych zagrożeń dla racji stanu w Strategii zostały zidentyfikowane te odnoszące się do inżynierii społecznej w postaci: manipulacji, dezinformacji, działalności inspiracyjnej oraz dezintegracji. Przy czym błędnie przypisano tylko manipulacji identyfikację w obszarze działań hybrydowych. Całość działań zaliczonych do inżynierii społecznej można włączyć w zakres tychże działań.

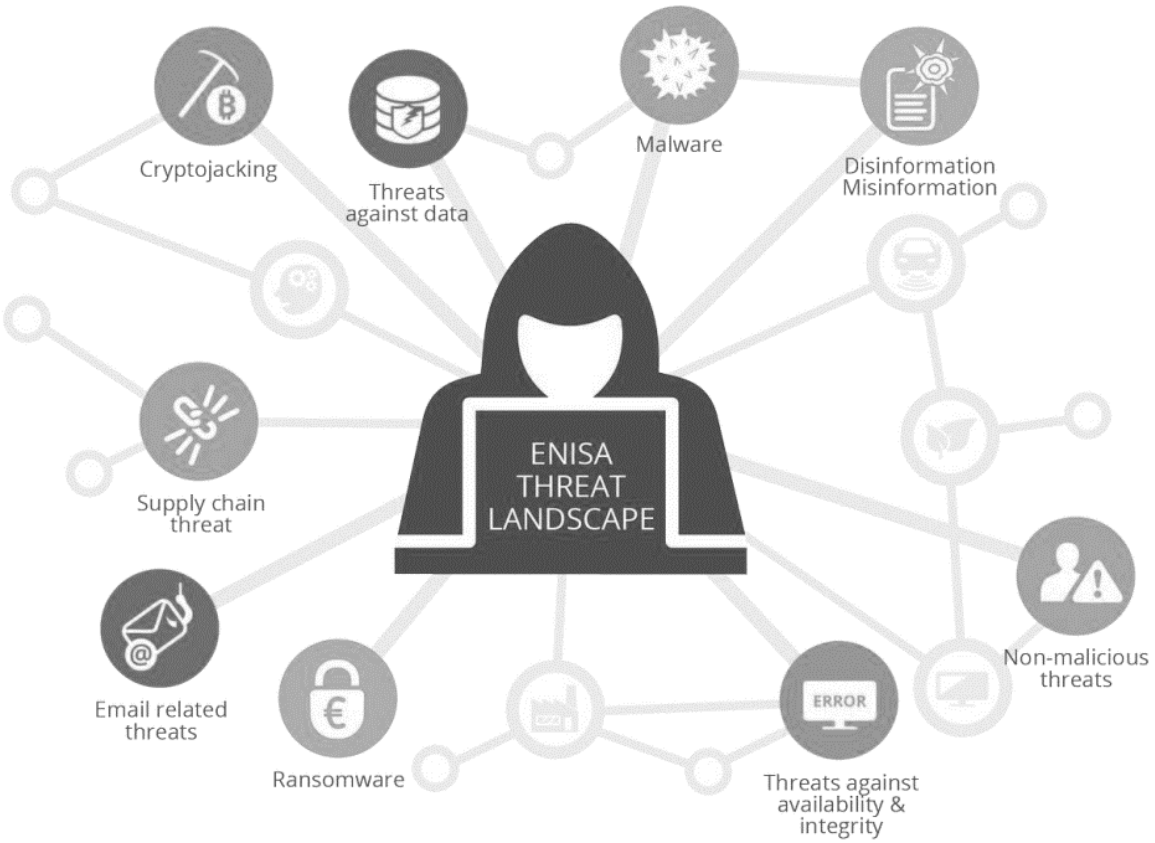
Przechodząc do identyfikacji zagrożeń, Strategia posiada pewne braki w tym wymiarze. Przede wszystkim w sposób niewystarczający określa środki gotowości, reagowania i przywracania stanu normalnego w kontekście zarządzania kryzysowego, o którym traktuje. W szczególności brakuje w niej źródeł ryzyk.

Ustawa ani strategia nie dokonuje identyfikacji ryzyk ani zagrożeń. Przerzuca odpowiedzialność za zarządzanie ryzykiem i incydentami na dostawców i operatorów oraz na CSIRT MON, CSIRT NASK i CSIRT GOV. Niemniej chcąc dokonać analizy głównych zagrożeń cyberbezpieczeństwa, rząd odsyła[33] do corocznych raportów Agencji UE ds. Cyberbezpieczeństwa (ENISA). Obecny raport za 2021 r. wskazuje kilka grup istotniejszych zagrożeń dla

[32] *Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy Prawo telekomunikacyjne,* https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne (20.01.2022).

[33] *15 głównych cyberzagrożeń – raport ENISA*, https://www.gov.pl/web/baza-wiedzy/15-glownych-cyberzagrozen--raport-enisa (20.01.2022).

państw europejskich. Za najważniejsze uznano: ransomware, złośliwe oprogramowanie (malware), Cryptojacking, zagrożenia poczty elektronicznej, zagrożenia danych, zagrożenia dostępności i integralności, dezinformację i zagrożenia o charakterze niezłośliwym[34]. Jednocześnie dokonano zestawienia zagrożeń cyberprzestrzeni odnosząc je do czterech zasadniczych kategorii: podmioty sponsorowane przez państwo, podmioty zajmujące się cyberprzestępczością, hakerzy na zlecenie, haktywiści.



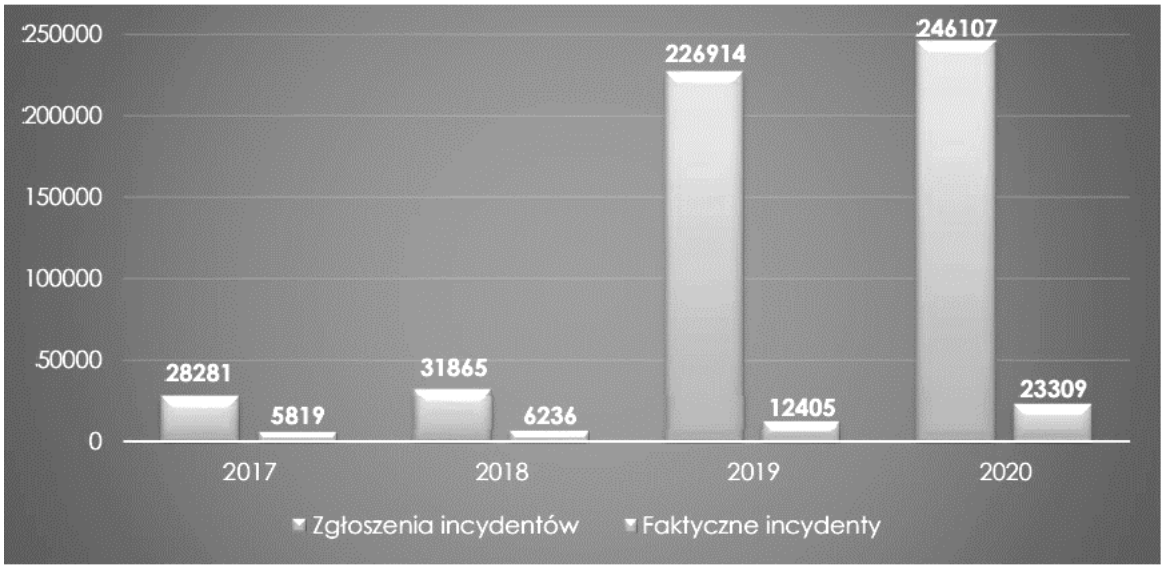
Wykres 1: Główne zagrożenia cyberprzestrzeni[35]

Główne trendy w zakresie cyberzagrożeń w 2021 r. to: ataki na dostawców usług, szpiegostwo, zaangażowanie rządów w walkę między podmiotami, ataki na infrastrukturę krytyczną, silny wzrost tendencji szantażu i żądania okupu, nowe lub niepopularne języki kodowania używane do ataku, rekordowa ilość ataków cryptojackingowych, wzrost ilości ataków typu *Business E-mail Compromise*, znaczny wzrost naruszeń danych w obszarze opieki zdrowotnej, przeniesienie ataków na Internet rzeczy (IoT) oraz sieci mobilne, nowy rodzaju ataków DoS (*Ransom Denial of Service*), wsparcie dezinformacji sztuczną inteligencją (AI), bezprecedensowy wzrost dezinformacji, wyłonienie się usługi *Disinformation-as-a-Service* (DaaS). Większość z tych działań umożliwiła pandemia Covid-19, która osłabiła czujność administracyjną oraz wytworzyła możliwości szerzenia ataków w cyberprzestrzeni.

[34] Ibidem.
[35] Za: *Threat Landscape 2021 – Prime threats*, Enisa Threat Landscape 2021, April 2020 to mid-July 2021, October 2021, s. 9.

Polska znajduje się w pierwszej dziesiątce krajów najczęściej atakowanych poprzez DDoS[36]. W przypadku polskich statystyk CERT Polska odnotował w 2020 r. około 35 tys. zgłoszeń (incydentów)[37]. Do zagrożeń występujących w Polsce należy zaliczyć: emotet, phishing, fałszywe faktury, trojany mobilne, ransomware, wyłudzanie i wycieki danych, dezinformacja, działalność grup przestępczych.

Raport Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego CSIRT GOV („Raport o stanie bezpieczeństwa w cyberprzestrzeni RP w 2020 r.") z sierpnia 2021 r. wskazuje, że pandemia Covid-19 spowodowała blisko dwukrotny wzrost zidentyfikowanych i sklasyfikowanych incydentów. Od kilku lat utrzymuje się w Polsce trend podwajania ilości zagrożeń w cyberprzestrzeni.



Wykres 2. Liczba zarejestrowanych zgłoszeń oraz incydentów w poszczególnych latach[38]

Najczęstszymi zagrożeniami w cyberprzestrzeni w Polsce są wirusy (72% wszystkich incydentów i wzrost w stosunku do 2019 r. o 132%), skanowanie, phishing oraz podatność. Do najczęściej atakowanych sektorów należą urzędy, infrastruktura krytyczna, instytucje publiczne, administracja publiczna, ministerstwa, służby i wojsko. Zwłaszcza w wojsku, infrastrukturze i instytucjach widać największy wzrost ataków (dwukrotny a nawet trzykrotny)[39].

Pojawia się wyraźna tendencja do wzrostu zagrożeń w instytucjach publicznych. Stwarza to konieczność dalszej integracji Krajowego Systemu Cyberbezpieczeństwa. W zakresie pandemii Covid-19 należy wskazać, że wykorzystano przekazy medialne do motywów stosowanych w atakach socjotechnicznych[40].

[36] Ibidem, s. 71.
[37] *Krajobraz bezpieczeństwa polskiego internetu. Raport roczny z działalności CERT Polska*, Warszawa 2021, s. 23.
[38] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku*, Warszawa 2021, s. 10.
[39] Ibidem, s. 8–14.
[40] Ibidem, s. 68–70.

Incydenty w cyberprzestrzeni nie znajdują odzwierciedlenia w aktach legislacyjnych. Na szczeblu krajowym należy wskazać, że zgodnie z racją stanu w zakresie strategicznym pojawiają się tylko te odnoszące się do podmiotów sponsorowanych przez państwo, które realnie wpływają na relacje i pozycję międzynarodową Polski. Obecne działania legislacyjne dążą do ustrukturalizowania incydentów, wyznaczają nowe modele i mechanizmy przeciwdziałania im, znajdują się jednak w procesie prac.

Zgodnie z zapowiedzią ujętą w Strategii w październiku 2021 r. rząd opublikował Narodowe Standardy Cyberbezpieczeństwa w postaci podręcznika dla administracji publicznej[41]. Tu znajdują się szczegółowe wytyczne dotyczące przeciwdziałania. Dodatkowo rząd publikuje poradniki ds. cyberzagrożeń[42]. Pojawiła się także nowa wersja Ustawy o krajowym systemie cyberbezpieczeństwa, która tworzy m.in. Fundusz Cyberbezpieczeństwa (500 mln zł), centra wymiany informacji i analiz o cyberbezpieczeństwie (ISAC), zespół CSIRT INT przy Agencji Wywiadu, nowe instrumenty jako reakcja na incydenty czy powołuje spółkę Polskie 5G[43].

Wszystko to wskazuje, że racja stanu Polski w zakresie zagrożeń cyberprzestrzeni jest *in tatus nascendi*. Obecne jej określenie silnie wiąże się z zagrożeniami uderzającymi w suwerenność państwa i narodu. Zarówno Ustawa, jak i Strategia nie wymieniają tych zagrożeń, które istotnie dotyczą cyberprzestrzeni. Z tego punktu widzenia na poziomie najważniejszych aktów prawnych pojawiają się te ryzyka i incydenty, które zagrażają istocie państwowości (naruszają niezachwiany proces komunikacji, naruszają przestrzeń, wolność, ograniczają suwerenność władzy państwowej, stwarzają zagrożenia dla żywotnych interesów państwa i narodu).

PODSUMOWANIE

Zastosowana metodologia oraz analiza narracyjna aktów prawnych nakazuje stwierdzić, że polska racja stanu w zakresie paradygmatu bezpieczeństwa międzynarodowego sytuuje się w nurcie defensywnym w wersji słabej. Pojawiające się zapisy traktujące o odporności, prewencji, działaniach zmierzających do reakcji na incydent jednoznacznie określają ulokowanie polskiej myśli strategicznej w tym wymiarze po stronie defensywnej. Jednocześnie działania zmierzające do rozwoju polskiego sektora cyberbezpieczeństwa i bezpieczeństwa informacyjnego oraz hasła mówiące o wypracowaniu pozycji międzynarodowej Polski w ich zakresie można określić jako wariant przesuwający orientację nurtu z wersji silnie defensywnej na słabo defensywną. Nie znajdujemy przy tym równoważnika deklaracji, działań, metod ani środków między zakresem ofensywnym a defensywnym, co wyklucza możliwość sytuowania polskiej racji stanu w nurcie ofensywno-defensywnym.

[41] *Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego* https://www.gov.pl/web/baza-wiedzy/podrecznik-postepowania-z-incydentami-naruszenia-bezpieczenstwa-komputerowego, (20.01.2022).
[42] *Nowe poradniki partnerów technologicznych Programu Współpracy w Cyberbezpieczeństwie (PWCyber)* https://www.gov.pl/web/baza-wiedzy/nowe-poradniki-partnerow-technologicznych-pwcyber, (20.01.2022).
[43] *Kluczowa faza prac nad ustawą o KSC*, https://www.gov.pl/web/baza-wiedzy/kluczowa-faza-prac-nad-ustawa-o-ksc, (21.01.2022).

Przechodząc do określenia, czym jest polska racja stanu w środowisku cyberprzestrzeni, należy rozumieć ją jako sekurytyzację systemów infrastrukturalnych i informacyjnych oraz budowę i rozwój systemów reagowania na szczeblu państwowym, prywatnym (dostawcy, operatorzy i odbiorcy), a także instytucji nadzoru w celu maksymalizacji odporności na zagrożenia. Natomiast racja stanu w zakresie zwalczania i przeciwdziałania zagrożeniom wynikającym z cyberprzestrzeni odnosi się do takich zjawisk jak: rywalizacja geoekonomiczna, walka o prestiż/wizerunek państwa, zagrożenia o charakterze hybrydowym, dezinformacja i terroryzm.

BIBLIOGRAFIA

15 głównych cyberzagrożeń – raport ENISA, https://www.gov.pl/web/baza-wiedzy/15-glownych-cyberzagrozen--raport-enisa.

Agile cybersecurity, czyli bezpieczeństwo w dobie chmury i powszechności pracy zdalnej, Raport specjalny, red. A. Gontars, https://www.atsummit.pl/wp-content/uploads/2020/11/ATS2020_online.pdf.

Chałubińska-Jentkiewicz Katarzyna. 2021. Cyberspace as an Area of Legal Regulation. W Cybersecurity in Poland Legal Aspects, Springer Open Acces.

Dyrektywa 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, https://cyberpolicy.nask.pl/wp-content/uploads/2019/04/dyrektywa_NIS-1-Dyrektywa-NIS-3.pdf.

Galewska Iwona. 2014. „Spór o rozumienie polskiej racji stanu na arenie Unii Europejskiej – wymiar teoretyczny i praktyczny". Zeszyty Naukowe Uniwersytetu Szczecińskiego 28: 5-21.

Grosse Tomasz Grzegorz. 2020. Wejście do strefy euro a polska racja stanu. W Racja stanu Polski w Europie, Warszawa.

Kasińska-Metryka Agnieszka. 2020. Racja stanu – teoretyczne dylematy, praktyczne wątpliwości. W Racja stanu Polski w Europie. Warszawa.

Kik Kazimierz. 2020. Polska racja stanu w warunkach członkostwa w UE i NATO. W Racja stanu Polski w Europie. Warszawa.

Kitler Waldemar. 2019. Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej. W Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz. Warszawa.

Kluczowa faza prac nad ustawą o KSC, https://www.gov.pl/web/baza-wiedzy/kluczowa-faza-prac-nad-ustawa-o-ksc.

Krajobraz bezpieczeństwa polskiego internetu. Raport roczny z działalności CERT Polska. 2021. Warszawa.

Krzynówek-Arndt Anna. 2013. Rzeczpospolita jako dobro wspólne. W Kryterium etyczne w koncepcji racji stanu. Kraków.

Lewandowski Piotr. 2021. „Poland's Reason of State in the Creation of a New International Order. Foreign Policy as Poland's Reason of State in the 21st Century". Polish Political Science Yearbook 50: 133-147.

Lewandowski Piotr. 2020. Racja stanu w warunkach postsuwerenności i sieciowości międzynarodowej państw. W Polska racja stanu w perspektywie globalnych przemian. Warszawa.

Łastawski Kazimierz. 2009. Polska racja stanu po wstąpieniu do Unii Europejskiej. Warszawa: Wydawnictwa Akademickie i Profesjonalne.
Molendowska Magdalena. 2020. Od Trójkąta Wyszehradzkiego do Unii Europejskiej – pozycja Polski w zjednoczonej Europie. W Racja stanu Polski w Europie. Warszawa.
Narodowa Platforma Cyberbezpieczeństwa. https://www.nask.pl/pl/dzialalnosc/nauka-i-biznes/projekty-badawcze/2088,Narodowa-Platforma-Cyberbezpieczenstwa-NPC.html.
Nowe poradniki partnerów technologicznych Programu Współpracy w Cyberbezpieczeństwie (PWCyber) https://www.gov.pl/web/baza-wiedzy/nowe-poradniki-partnerow-technologicznych-pwcyber.
Olszewski Bogusław. 2019. Ewolucja cyberbezpieczeństwa w strategiach NATO; The Evolution of Cybersecurity in NATO Strategies. W Bezpieczeństwo europejskie po szczycie NATO w Warszawie. Kraków.
Pietraś Jacek. 1989. Racja stanu w polityce zagranicznej państwa. W Racja stanu. Historia, teoria, współczesność. Lublin.
Wojciuk Anna. 2010. Dylemat potęgi. Warszawa.
Podręcznik postępowania z incydentami naruszenia bezpieczeństwa komputerowego. https://www.gov.pl/web/baza-wiedzy/podrecznik-postepowania-z-incydentami-naruszenia-bezpieczenstwa-komputerowego.
Pokruszyński Witold. 2016. „Etymologia polityki i strategii bezpieczeństwa w świetle wyzwań i zagrożeń xxi wieku", Kultura Bezpieczeństwa. Nauka – Praktyka – Refleksje 22: 363-383.
Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy Prawo telekomunikacyjne. https://www.gov.pl/web/krmc/projekt-ustawy-o-zmianie-ustawy-o-krajowym-systemie-cyberbezpieczenstwa-oraz-ustawy-prawo-telekomunikacyjne.
Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2020 roku. Warszawa 2021.
Scholte Jan Aart. 2006. Globalizacja. Krytyczne wprowadzenie. Sosnowiec.
Stemplowski Ryszard. 2013. O kryterium etycznym w koncepcji racji stanu. W Kryterium etyczne w koncepcji racji stanu. Kraków.
Strategia Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2019-2024. https://www.dziennikustaw.gov.pl/MP/rok/2019/pozycja/1037.
Threat Landscape 2021. Prime threats, Enisa Threat Landscape. 2021.
Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa. https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001560.
Zenderowski Radosław, Cebul Krzysztof. 2020. Polska racja stanu w obszarze Europy Środkowo-Wschodniej – wyznaczniki i wyzwania, W Racja stanu Polski w Europie. Warszawa.