Państwo w obliczu współczesnych wyzwań. O cyberbezpieczeństwie i innych zagrożeniach na przykładzie wybranych państw azjatyckich

Redakcja naukowa
Joanna Marszałek-Kawa

wydawnictwo adam marszałek

Seria
Biblioteka Azji i Pacyfiku

Redaktor Serii
Joanna Marszałek-Kawa

Sekretarz Serii
Bartosz Płotka

Recenzenci tomu
prof. dr hab. Zenon Trejnis
dr hab. Jarosław Piątek, prof. US

Redaktor prowadzący: *Paweł Jaroniak*
Redakcja techniczna: *Ryszard Kurasz*
Korekta: *Zespół*
Projekt okładki: *Krzysztof Galus*

Toruń 2020

ISBN 978-83-8180-306-9

Wydawnictwo prowadzi sprzedaż wysyłkową:
tel./fax 56 648 50 70, marketing@marszalek.com.pl

Wydawnictwo Adam Marszałek, ul. Lubicka 44, 87–100 Toruń
tel. 56 664 22 35, 56 660 81 60, e-mail: info@marszalek.com.pl, www.marszalek.com.pl
Drukarnia, ul. Warszawska 54, 87–148 Łysomice, tel. 56 678 34 78

Spis treści

Wstęp 5

Piotr Grochmalski
Amerykańsko-chiński wyścig technologiczny
w obszarze sztucznej inteligencji 9

Monika Nowikowska
Światowy Indeks Cyberbezpieczeństwa na przykładzie
wybranych państw Azji i Oceanii 47

Katarzyna Badźmirowska-Masłowska
Cyberbezpieczeństwo Australii. Wybrane aspekty
strategiczne 67

Katarzyna Chałubińska-Jentkiewicz
System prawny cyberbezpieczeństwa w Rosji –
charakterystyka 92

Malwina Ewa Kołodziejczak
Uwarunkowania prawne cyberbezpieczeństwa w Republice
Chińskiej (Tajwan) 114

Agnieszka Brzostek
Prawno-administracyjne podstawy cyberbezpieczeństwa Japonii 130

Filip Radoniewicz
Przestępstwa przeciwko danym oraz systemom komputerowym w japońskim prawie karnym 153

Tadeusz Detyna
Timor Wschodni – 20 lat nadziei i rozczarowań 175

Michał Bielecki
Zbrodnia bez nazwy? O zasadności użycia terminu *ludobójstwo* w odniesieniu do indonezyjskich masowych mordów z lat 1965–1966 216

Wstęp

Współczesny świat zmienia się w szybkim tempie na wielu płaszczyznach. Przeobrażenia te dotyczą w oczywisty sposób również gospodarki. Układ sił na świecie, który określa rolę mocarstw, ewoluuje, a dynamika tych zmian jest bardzo duża. Stany Zjednoczone Ameryki Północnej rywalizują z Chińską Republiką Ludową o pozycję lidera w grupie państw – największych potęg gospodarczych.

Ważnym graczem na arenie międzynarodowej jest w dalszym ciągu Federacja Rosyjska. Co warto zaznaczyć, udział Rosji w produkcie światowym konsekwentnie jednak maleje. Rosyjskie władze starają się więc podejmować działania, które pozwolą utrzymać pozycję światowego mocarstwa. Również rządy Japonii, Niemiec, Korei Południowej koncentrują swe wysiłki na realizacji planów budowy i utrzymania silnej gospodarki. Wielka Brytania i Francja natomiast ogniskują swe działania na realizacji polityki, której główną osią jest rozwijanie potęgi gospodarczej, przy zachowaniu silnej armii.

Znaczenie nowoczesnych technologii we współczesnym świecie jest ogromne. Określają one naszą przyszłość, mają wpływ na losy świata. Możliwości z nimi związane wyznaczają również pozycję państw na świecie. Zdają sobie z tego doskonale sprawę rządy wielu państw. W tym kontekście warto choćby wskazać na działania Izraela, Indii czy Pakistanu – państw, których celem jest również osiągnięcie wiodącej pozycji w światowej gospodarce.

Nowoczesne technologie wpływają na nasze życie, z ich wykorzystaniem wiąże się wiele korzyści. Tworzą one jednak wiele zagrożeń, wyzwań, których diagnozowaniem, omawianiem, a następnie poszukiwaniem na nie rozwiązań zajmują się także przedstawiciele świata nauki. W rezultacie prowadzonych badań, analiz powstają liczne publikacje poświęcone tej problematyce, z których dużą grupę stanowią opracowania dotyczące cyberbezpieczeństwa. Prezentacji tego zagadnienia dedykowana jest również niniejsza publikacja.

W problematykę cyberbezpieczeństwa wprowadza artykuł Piotra Grochmalskiego *Amerykańsko-chiński wyścig technologiczny w obszarze sztucznej inteligencji*.

Autorką kolejnego opracowania, zatytułowanego *Światowy Indeks Cyberbezpieczeństwa na przykładzie wybranych państw Azji i Oceanii,* jest Monika Nowikowska, która na przykładzie wybranych państw regionu Azji i Pacyfiku (tj. Australii, Malezji i Singapuru) omawia Światowy Indeks Cyberbezpieczeństwa. Podstawę jej dociekań stanowi publikowany przez Międzynarodowy Związek Telekomunikacyjny dokument zawierający przeprowadzoną w skali światowej analizę tego, w jaki sposób rządy poszczególnych państw zarządzają cyberryzykiem.

Problemowi cyberbezpieczeństwa Australii poświęcony jest rozdział autorstwa Katarzyny Badźmirowskiej-Masłowskiej. Badaczka prowadzi rozważania dotyczące celów oraz strategicznych kierunków prowadzonych działań. Omawia także prawno-instytucjonalne aspekty cyberbezpieczeństwa.

Katarzyna Chałubińska-Jentkiewicz, znakomita znawczyni problematyki cyberbezpieczeństwa, pomysłodawczyni i redaktor naukowy prestiżowej serii wydawniczej Prawo Cyberprzestrzeni, rozdział swego autorstwa zatytułowała *System prawny cyberbezpieczeństwa w Rosji – charakterystyka*. Zdaniem badaczki obecnie nie ma państwa, które posiadałoby całkowicie bezpieczną cyberprzestrzeń. Z tego powodu rządy podejmu-

ją konsekwentne i zdeterminowane działania zmierzające do zminimalizowania strat spowodowanych cyberatakami. Autorka analizuje podstawowe dokumenty strategiczne Federacji Rosyjskiej, takie jak doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej oraz Strategia Rozwoju Społeczeństwa Informacyjnego w Federacji Rosyjskiej na lata 2017–2030.

Autorką kolejnego rozdziału jest Malwina Ewa Kołodziejczak, która omawia *Prawne uwarunkowania cyberbezpieczeństwa w Republice Chińskiej (Tajwan)*. Jak wskazuje, doświadczenia Tajwanu są warte szerszej analizy ze względu na dużą częstotliwość cyberataków. Ponadto Tajwan umiejętnie prowadzi politykę *soft power*, czego dowodzą wysokie lokaty w rankingach pokazujących zdolność państw do wykorzystywania technologii cyfrowej oraz zabezpieczenia przed cyberzagrożeniami.

Szeroki wykład poświęcony prawno-administracyjnym podstawom cyberbezpieczeństwa Japonii przygotowała z kolei Agnieszka Brzostek. W jej ocenie częste ataki hakerów na japońską administrację i agencje rządowe stały się ważnym argumentem na poparcie budowy systemu cyberbezpieczeństwa. Zaplanowane na 2020 r. igrzyska olimpijskie zdopingowały władze do zwiększenia wysiłków mających na celu zagwarantowanie bezpieczeństwa w trakcie tego wydarzenia. W tym celu przyspieszono wiele procesów legislacyjnych, aby stworzyć podstawy prawne do działań podejmowanych przez instytucje cywilne i wojskowe.

Kolejny rozdział monografii zawiera analizę przygotowaną przez Filipa Rodoniewicza z Akademii Sztuki Wojennej, która dotyczy przestępstw przeciwko danym oraz systemom komputerowym w japońskim prawie karnym. Badacz prezentuje m.in. przepisy ustawy nr 128 z 1999 r. o zakazie nieuprawnionego dostępu oraz ustawy nr 86 z 1984 r. o działalności telekomunikacyjnej.

Autorem opracowania poświęconego Timorowi Wschodniemu jest związany z Uniwersytetem Opolskim Tadeusz Detyna. Omawia on drogę tego państwa do niepodległości ze wskaza-

niem udziału rządów Indonezji, Australii oraz organizacji międzynarodowych w realizacji tego celu. Wskazuje przy tym, że waśnie plemienne oraz nieurodzaje utrudniały proces, a rolę stabilizatora pełniły okresowo wojska ONZ.

Ostatni rozdział książki, który opracował Michał Bielecki, zatytułowany jest *Zbrodnia bez nazwy? O zasadności użycia terminu* ludobójstwo *w odniesieniu do indonezyjskich masowych mordów z lat 1965–1966*. Autor w swych rozważaniach prezentuje pogląd, że indonezyjska przemoc w badanym okresie to jedna z największych tragedii, jakie wydarzyły się po II wojnie światowej. W ciągu kilku miesięcy życie straciło wówczas pół miliona ludzi. Zdaniem badacza w opisie tych dramatycznych wydarzeń powinien być stosowany termin ludobójstwo.

Tom, który oddajemy do rąk czytelnika, stanowi kompendium wiedzy na temat wielu ważnych zagadnień dotyczących bezpieczeństwa we współczesnym świecie, w szczególności w cyberprzestrzeni. Mam nadzieję, że najnowsza publikacja z serii Biblioteka Azji i Pacyfiku spotka się z życzliwym przyjęciem czytelników, uzupełniając, na polu poznawczym, dostępną literaturę przedmiotu.

Joanna Marszałek-Kawa

Piotr Grochmalski
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0002-5671-3339

Amerykańsko-chiński wyścig technologiczny w obszarze sztucznej inteligencji

Wprowadzenie

Świat się zmienia, a wraz z nim granice jego interpretacji i interpretacji naszego miejsca w nim. Nassim Nicholas Taleb uważa, że w coraz większym stopniu żyjemy w rekurencyjnej rzeczywistości. Przez pojęcie to rozumie świat, w którym działa „coraz więcej pętli sprzężenia zwrotnego, przez co określone zdarzenia stają się przyczyną kolejnych zdarzeń”[1]. Jest to zbliżony mechanizm opisu rzeczywistości do teorii zapętleń i związaną z nią metodą zapętleń jako metodą analityczną, która zostanie przybliżona w części metodologicznej artykułu. Istotnym elementem wpływającym na rosnącą złożoność zachodzących procesów jest narastająca technicyzacja środowiska społecznego a także obiektywny wzrost populacji ludzkości. Następuje, coraz bardziej dynamiczna, ewolucja granic interpretacji rzeczywistości, którą uosabiają coraz bardziej złożone modele systemowe. To z kolei stwarza problem ich punktów bifurkacji, w którym system nierównowagi znajduje się w krytycznym punkcie. „Najmniejsze przypadkowe wahania mogą przechylić skale i nieodwołalnie określić przyszły los systemu”[2]. W wymiarze globalnym coraz

[1] N.Ni. Taleb, *Czarny łabędź*, Warszawa 2015, s. 23, prz. 6.

[2] P. Ball, *Masa krytyczna. Jak jedno z drugiego wynika*, Kraków 2007, s. 141.

częściej za taki punkt bifiurkacji uznaje się rywalizację chińsko-amerykańską. Jeszcze z perspektywy XX w. Federico Mayor, prognozując przyszłość świata, ostrzegał: „Wystrzegajmy się jednak, przejawiając troskę o ochronę, błędu ingerencji. XXI w. nie należy do nas; należy do przyszłych pokoleń. Człowiek przyszłości, będąc naszym bratem, nie jest naszą repliką. Należy do innego czasu, czasu, którego wyzwań, niebezpieczeństw i pragnień jeszcze nie znamy"[3]. F. Mayor, były dyrektor generalny UNESCO, ukazując u progu XXI wieku, razem z Jérôme'em Bindém, byłym dyrektorem Biura Analiz i Prognoz UNESCO, przyszłość świata, buduje go w ramach pozimnowojennej logiki, w której nie dostrzega się Chin jako państwa, które wkrótce będzie miało drugą gospodarkę świata. Paul Kennedy, autor szeroko omawianej w świecie książki *Wielkie mocarstwa. Narodziny, rozwój, upadek*, na kanwie swoich historycznych analiz, próbuje pod koniec lat 90. XX w. stworzyć prognozę przyszłości[4]. Uważa Japonię za państwo, które posiada najbardziej obiecujący plan dla przyszłego świata. Ma nowoczesną gospodarkę, rozbudowany potencjał naukowy i najniższy na świecie współczynnik analfabetyzmu wynoszący 0,7%. Chiny natomiast, z analfabetyzmem sięgającym 31% w 1990 r., a więc obejmującym 220 mln ludzi[5], są państwem Trzeciego Świata, w którym jedna trzecia naukowców jest bez pracy[6]. Dwadzieścia lat później ChRL wyprzedziły Japonię i stały się drugą potęgą gospodarczą świata[7]. Zagroziły też hegemonii USA. Graham Allison, amerykański wybitny specjalista od problematyki bezpieczeństwa narodowego, uznał, iż sytuacja ta

[3] Fe. Mayor, J. Bindé (wsp.), *Przyszłość świata*, Warszawa 2001, s. 490.

[4] P. Kennedy, *U progu XXI wieku (przymiarka do przyszłości)*, London 1994, s. 162.

[5] Ibidem, s. 206.

[6] Ibidem, s. 208.

[7] B. Góralczyk, *Wielki renesans. Chińska transformacja i jej konsekwnecje*, Warszawa 2018, s. 282.

grozi konfliktem między USA i Chinami. Analizując podobny model w dziejach świata – wzrost potęgi jednego państwa zagraża utratą hegemonii przez inne mocarstwo – opisał szesnaście takich sytuacji. W dwunastu z nich doszło do wybuchu wojny[8]. Allison próbuje ukazać punkty krytyczne tego procesu i ocenić prawdopodobieństwo uniknięcia takiego konfliktu. Z kolei John Mearsheimer, w publikacji szeroko komentowanej w Chinach, mocno akcentuje znaczne prawdopodobieństwo konfrontacji USA–ChRL. Uznaje je za większe niż starcie zbrojne USA–ZSRR w okresie zimnej wojny[9]. W wymiarze cywilizacyjnym John D. Barrow uważa, że „skłonność do krótkoterminowych świadczeń, a nie bardzo długoterminowe planowanie nie pozwoli nam zatrzymać katastrofy, które są powoli i stopniowo coraz bardziej realne, choć niezauważalne, w trakcie jednego ludzkiego życia"[10].

Nie mamy i nie uzyskamy narzędzia do przełamania horyzontu czasu. Sam czas też ulega rozwarstwieniu. Nie tylko jesteśmy zmuszani do dylatacji czasu (dla satelitów obsługujących system GPS muszą być dokonywane obliczenia, aby kompensować efekt relatywistyczny). Następuje też relatywizacja czasu w strukturach społecznych.

Strategiczna rywalizacja między USA i ChRL może przyspieszyć proces opracowywania nowych technologii i badań nad sztuczną inteligencją. Odd Arne Westad uważa, że możemy być w przeddzień konfliktu między Stanami Zjednoczonymi a Chinami, który będzie podobny do zimnej wojny[11]. Oddziele-

---

[8] G. Allison, *Skazani na wojnę? Czy Ameryka i Chiny unikną pułapki Tukidydesa*, Bielsko-Biała 2018, s. 18.

[9] J. Mearsheimer, *Tragizm polityki mocarstw*, Kraków 2019, s. 473.

[10] J.D. Barrow, *Kres możliwości? Granice poznania i poznanie granic*, Opole 2005, s. 490.

[11] O.A. Westad, *The Souces of Chinese Conduct. Are Washington and Beijing Fighting a New Cold War?*, „Foreign Affairs", wrzesień/październik, vol. 98, nr 5, s. 86 ; R. Miśkiewicz, *Knowledge transfer in the prospect of Industry 4.0 in terms of developing innovative technologies for electromobility*,

nie przewidywalnego od nieprzewidywalnego jest trudnym zadaniem. Ale możemy dostrzec podstawowe trendy w relacjach między obu tymi państwami. Posiadają one rozwinięty potencjał analityczny, który wykorzystywany jest do prognozowania globalnych trendów politycznych, ekonomicznych i technologicznych. Nie uchroniło to jednak zarówno USA, jak i ChRL od popełniania strategicznego błędów w ocenie drugiej strony. W artykule postaram się zweryfikować poniższe tezy, które ukażą nieco inny kontekst rywalizacji chińsko-amerykańskiej:

1. Różne kultury strategiczne w USA i w Chinach są mocno zakorzenione historycznie i prowadzą do wzajemnie błędnych ocen strategii realizowanych przez obie strony.
3. Chiny bardzo ostrożnie realizowały strategię wzrostu unikając konfrontacji z USA.
3. Dojście do władzy Xi Jinpinga spowodowało wzrost retoryki konfrontacyjnej.
4. Między Stanami Zjednoczonymi a Chinami ma miejsce najbardziej niebezpieczny i nieprzewidywalny wyścig zbrojeń w historii ludzkości zmierzający do tego, aby zdobyć strategiczną przewagę nad przeciwnikiem dzięki sztucznej inteligencji.
5. Amerykański-chiński wyścig o strategiczną dominację w dziedzinie sztucznej inteligencji może doprowadzić do powstania superinteligencji, która stanie się niezależna od ludzkości.

Metody badawcze

Kluczowym problemem jest analiza wyścigu technologicznego jako jednego z elementów strategicznej rywalizacji dwóch

[w:] *Urban Electromobility in the context of industry 4.0*, red. W. Drożdż, R. Miśkiewicz, F. Elżanowski, J. Pokrzywniak Toruń 2019, s. 82.

ośrodków siły. Jego charakter jest konsekwencją zderzenia dwóch kultur strategicznych i dwóch modelów modernizacji. Samo pojęcie modernizacji traktowane jest w ramach nieliniowej logiki modernizacji (proces, który ma wewnętrzną logikę i ma ona cechy nieliniowe). Modernizacja traktowana jest jako dynamiczny, strukturalny proces współzależnych zbiorów i podzbiorów. Do jej analizy, a także powiązania go z procesem wyścigu technologicznego wykorzystana będzie metoda zapętleń. Jest ona rozumiana „jako opis dynamicznych zmian jakie są interakcją między sumą zbiorów strukturalnych »a« i »b«. W efekcie wzajemnych zapętleń tworzy się dodatkowy zbiór »c«, który nie jest prostą sumą obu zbiorów, ale nową wartością dodaną. Przy czym ta nowa wartość dodana wchodzi, w wyniku zapętleń, w strukturalne interakcje z istniejącymi zbiorami, tworząc kolejny zbiór »c«"[12]. Metoda ta pozwala wyjaśnić dlaczego nie ma jednego uniwersalnego modelu modernizacji, nie ma jednej, uniwersalnej kultury i dlaczego procesy te mają charakter nieliniowy. Jakub Bernoulli, który wprowadził do epistemologii pojęcie „prawdopodobieństwa", nadał mu też wymiar mierzalny[13]. Dzięki temu możemy stopniować prawdopodobieństwo wystąpienia danego wydarzenia, co pozwala na tworzenie precyzyjniejszych prognoz i ich skuteczniejszą weryfikację. W publikacji użyjemy skali Kenta[14]. W ramach przyjętych założeń czas nie stanowi kryterium obiektywnego, jego historyczność obecnie nie ma charakteru liniowego, ale wykładniczy. Nie

[12] Metoda zapętleń użyta została po raz pierwszy przez autora tekstu w 2010 r. do analizy zjawiska autorytaryzmu centroazjatyckiego. Zob. P. Grochmalski, *Autorytaryzm centroazjatycki a kwestia transformacji systemowej – próba poszukiwania modelu metodologicznego*, [w:] *Przywództwo, elity i transformacje w krajach WNP. Problemy metodologii badań*, t. 1, Warszawa 2010, s. 513–514.

[13] M. Heller, *Filozofia przypadku*, Kraków 2014, s. 65–66.

[14] Szerzej: B. Grenda, P. Grochmalski, H. Świeboda (red.), *National Security Forecast. Polish Perspective*, Poznań 2019, s. 7.

jest też niezależny od obserwatora i opisywanego procesu. Ray Kurzwail zauważa, że „...w XXI wieku będziemy świadkami nie stu lat postępu technologicznego, ale postępu rzędu 20 tys. lat (oczywiście w stosunku do dzisiejszej szybkości postępu) lub tysiąc razy większego niż ten osiągnięty w XX w.[15] Czas ulega też rozwarstwieniu – czas społeczny, który ma charakter pokoleniowy jest coraz bardziej relatywnie wolniejszy od czasu postępu technologicznego, a różnica ta będzie logarytmicznie nadal wzrastać. Skutki tego procesu mocno będą dostrzegalne w wyniku wyścigu technologicznego między USA i Chinami.

* * *

I. Różne kultury strategiczne w USA i w Chinach są mocno zakorzenione historycznie i prowadzą do wzajemnie błędnych ocen strategii realizowanych przez obie strony

Współczesna Zachodnia koncepcja stosunków międzynarodowych pojawiła się w XVI i XVII w. Struktura Europy kształtowana była przez grupę państw o mniej więcej równej sile. Żadne państwo nie było wystarczająco silne, aby narzucić swoją wolę. Pojęcia suwerenności i równości prawnej państw stały się podstawą prawa międzynarodowego i dyplomacji. Jest to obce doświadczenie dla Chin, które w swojej długiej historii nigdy nie opierały swoich kontaktów z innym państwem na równych prawach. Nigdy bowiem Chińczycy nie spotkali społeczeństwa o porównywalnej do nich kultury i potęgi. Ich elity były przekonane o wyjątkowości cywilizacji chińskiej. Wybitny znawca problematyki Państwa Środka, Marcel Granet, podkreśla, że: „Żadna inna cywilizacja nie była przez tak

[15] R. Kurzweil, *Nadchodzi osobliwość. Kiedy człowiek przekroczy granice biologii*, Warszawa 2013, s. 26.

długie wieki czynnikiem łączącym społeczeństwo”[16]. Była też pierwszą, która stworzyła unikalny model scentralizowanego państwa, cesarstwo. Jak trafnie zauważa C.P. Fitzgerald: „Długa historia Chin zna jedynie dwie rewolucje, które w sposób radykalny przeobraziły polityczną i społeczną strukturę państwa. Pierwszą z nich była wielka rewolucja w roku 221 p.n.e.; zburzyła ona gruntownie feudalny system starożytnych Chin, na miejsce którego ukształtowała się scentralizowana monarchia; druga z tych rewolucji, w 1911 r., obaliła starożytną monarchię i Chińczycy, pod wpływem zetknięcia się z kulturą Zachodu, spróbowali przystosować polityczne i społeczne warunki do nowej ery międzynarodowych kontaktów”[17]. Jak zauważa H. Kissinger: „Chiny tradycyjnie przekraczały granice państw europejskich pod względem liczby ludności i wielkości terytorium; do czasu wielkiej rewolucji przemysłowej były też znacznie bogatsze”[18]. Samuel Huntington przypomniał światu w połowie lat 90. XX w. w jego głośnej pracy *Zderzenie cywilizacji*, że w 1750 r. Chiny produkowały około jednej trzeciej globalnej produkcji, a Zachód około jednej piątej. Dopiero po 1830 r. Po raz pierwszy Zachód nieznacznie wyprzedził Państwo Środka[19]. Nie ma przesady w opinii H. Kissingera, gdy stwierdził: że „Przez osiemnaście z dwudziestu ostatnich stuleci Chiny miały większy udział w światowym PKB niż jakiekolwiek zachodnie społeczeństwo”[20] (z drugiej strony fakt ten był ściśle powiązany z populacją danego państwa. Dlatego w połowie XVII w. Indie wytwarzały jedną czwartą globalnej produkcji)[21].

---

16 M. Granet, *Cywilizacja chińska*, Warszawa 1973, s. 13.

17 C.P. Fitzgerald, *Chiny. Zarys historii kultury*, Warszawa 1974, s. 149.

18 H. Kissinger, *O Chinach*, Wołowiec 2014, s. 28.

19 S. Huntington, *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2000, s. 114.

20 H. Kissinger, *O Chinach*..., op.cit., s. 28.

21 S. Huntington, *Zderzenie cywilizacji*..., op.cit., s. 114.

Władca Chin, zasiadający na Smoczym Tronie w Zakazanym Mieście w Pekinie, w tradycji imperium był osią kosmicznego porządku. Traktat o wielkim systemie (*Hongfan*), który przedstawia porządek społeczno-polityczny Chin, ukazuje „królewską doskonałość" *(huang ji)* owego uniwersalnego władcy, który stanowi oś całego kosmicznego systemu[22]. Linearny, obiektywny czas, nie istnieje. Cykl historii wyznacza bowiem nowy władca. Ale nie jest on automatycznie dostosowany do swojego pola historycznego. Musi poszukiwać z nim harmonii, dostosowywać się do przemian[23]. Władca, jako Syn Niebios, otrzymywał mandat do sprawowania władzy od *Tian,* by rządzić światem (*tianxia*)[24]*.* Tianxia był tez synonimem Chin. Syn Niebios był więc nominalnie władcą całego świata. Charakterystyczna jest odpowiedź, jaką w 1793 r. cesarz Qianlonga udzielił brytyjskiemu władcy Jerzemu III. W liście wręczonym brytyjskiemu posłowi pisał: „Co do twej usilnej prośby, by jeden z twych rodaków mógł być akredytowany przy mym neibiańskim dworze i nadzorować wymianę handlową twego kraju z Chinami, jest ona sprzeczna ze zwyczajami mej dynastii i nie może w żadne sposób być wysłuchana. [...]. Jeśli zapewniasz, że twoja cześć dla naszej niebiańskiej dynastii napełnia cię pragnieniem przyswojenia sobie naszej cywilizacji, to nasze ceremonie i prawa różnią się tak kompletnie od twoich własnych, że choćby nawet twój poseł był w stanie przyswoić sobie zasady naszej cywilizacji, nie zdołałbyś żadną miarą przeszczepić naszych obyczajów i nawyków na twą obcą glebę"[25].

Cechą charakterystyczną Chin w ich dziejach jest ich wielki pragmatyzm. Jest to jeden z głównych powodów fundamen-

---

22 B.L. Schwartz, *Starożytna myśl chińska*, Kraków 2009, s. 373.

23 Ibidem, s. 372

24 Ibidem, s. 54.

25 A.F. Whyte, *China and Foreign Powers*, Oxford 1928, s. 41.

talnej różnicy w chińskich i zachodnich podejściach do strategii. W chińskiej tradycji kultura strategiczna jest integralnym elementem holistycznego cyklu historii, w którym przeszłość i przyszłość, słabości i siły – wszystko jest ze sobą powiązane. Istotą owego podejścia jest relacja do kwestii przemian. W cywilizacji zachodniej istnieje głęboka obawa przed niestałością otaczającego świata, a przemiana jest często traktowana jako zasadnicze zagrożenie. Dąży się do przeciwstawieniu takiej groźbie, do odkrycia stabilnych praw i zasad, którymi można się posługiwać, aby przeciwdziałać niestabilności, labilności świata. Dla Chińczyków cały wszechświat ciągle ulega przemianom[26]. Stąd silne powiązanie koncepcji przemiany z procesem działania. Jest on też mocno widoczny w pojmowaniu przez Chińczyków pojęcia strategii. A także szczególna rola jaka przypadła w próbach odczytywania owych przemian za pomocą *Księgi przemian* (I Ching). Przy czym samego „pojęcia przemian nie traktowano w Chinach jako zderzenia przeciwieństw, lecz raczej jako ich wzajemne uzupełnianie się oraz współpracę"[27]. W takim ujęciu „Strategia i sposób sprawowania rządów stają się narzędziem »wojowniczego współistnienia« z przeciwnikami"[28]. Dobrze ilustruje współcześnie takie podejście tzw. „dwugłowa strategia" (*shuangtou zhanlüe*) wobec USA, którą zaproponował Shi Yinhonga na początku XXI w. – „z jednej strony, zachować skromność i absolutnie unikać konfrontacji z tym krajem, ...z drugiej strony, nie pozwolić się zdominować »teorią chińskiego zagrożenia«, przyspieszyć modernizację armii i za wszelką cenę nie dopuścić do niepodległości Tajwanu"[29]. W chińskim podejściu do strategii celem jest

[26] J. Gernet, *Inteligencja Chin. Społeczeństwo i mentalność*, Warszawa 2008, s. 335.

[27] Ibidem, s. 336.

[28] H. Kissinger, *O Chinach...*, op.cit., s. 45.

[29] J.-P. Cabestan, *Polityka zagraniczna Chin*, Warszawa 2013, s. 208.

cierpliwe osiąganie stopniowej przewagi tak, aby przeciwnik – jeszcze przed ewentualną konfrontacją – uznał swoją porażkę ze względu na utratę zdolności do skutecznej rywalizacji. Jest to proces, część większego cyklu. Kissinger trafnie zauważa, że „najbardziej zdumiewającym przejawem fundamentalnego pragmatyzmu Chińczyków był ich stosunek do najeźdźców. Gdy obce dynastie odnosiły zwycięstwo na polu bitwy, chińska elita biurokratyczna oferowała im swoje usługi i przekonywała, że krajem tak rozległym iu wyjątkowym można rządzić tylko za pomocą chińskich metod, chińskiego języka i istniejącej chińskiej biurokracji. Z każdym pokoleniem najeźdźcy coraz bardziej asymilowali się z porządkiem, który próbowali wcześniej zdominować. W końcu ich ojczyste tereny, z których rozpoczynali inwazje, zaczynały być uważane za część Chin. Okazywało się, że działają na rzecz tradycyjnego chińskiego interesu narodowego, a kierunek podboju się zmieniał”[30].

Zgodnie chińską tradycją, najważniejszym tekstem strategicznym jest *Sztuka wojny* Sun Tzu i pochodzi z Epoki Wiosen i Jesieni za panowania dynastii Zhou i ma być autorstwa Sun Wu, a więc powstał pod koniec VI w. p.n.e.[31] Kolejna wybitna praca *Metody wojskowe* pochodzi z Epoki Walczących Królestw i prawdopodobnie został stworzony przez Sun Pina między 356 i 341 r. p.n.e.[32] W okresie Walczących Królestw (475–221 p.n.e.), który jest powszechnie uważany za złoty wiek w historii chińskiej myśli i filozofii, powstała również Chińska Szkoła Strategów. Epoka Walczących Królestw zawiera również pierwsze informacje o grze *Weiqi,* bardziej znanej na Zachodzie pod japońskim imieniem *„go”*. Do dziś jest ona podstawową grą dla edukacji strategicznej w Chinach.

---

[30] H. Kissinger, *O Chinach*..., op.cit., s. 38.

[31] W. Rodziński, *Historia Chin*, Wrocław–Warszawa–Kraków–Gdańsk 1974, s. 51.

[32] Sun Tzu, Sun Pin, *Sztuka wojny*, Gliwice 2014, s. 9.

W tych najstarszych dokumentach strategia nie jest pojmowana jako analiza konkretnej sytuacji, ale jako definiowanie kontekstu wydarzenia i jego delikatnych powiązań, oraz kierunku dokonującej się przemiany. Znalazło to odzwierciedlenie w chińskim pojęciu 實 *shi* – „potencjalna energia" rozwijającego się stanu militarnego – jego tendencja rozwojowa. Koncepcja *shi* nie ma prostego odpowiednika w kulturze zachodniej. Istotą chińskiej strategii jest więc akumulacja elementów względnej przewagi. Jest to diametralnie przeciwne podejście do zachodniego pojmowania strategii (choć coraz częściej używane jest w Chinach pojęcie *zhànlüè* (战略), szczególnie w kontekście strategii biznesowej, które składa się ze znaków wojna i lekkość).

Klasyk europejskiej myśli strategicznej, Antoine-Henri Jomini, uważał, że strategia składa się z niezmiennych reguł, tworząc uniwersalne zasady walki. „Cel, jaki stawiał przed sobą, był utylitarny: sprowadzić wojnę do prostego zbioru zasad, które – zrozumiane w teorii i poprawnie zastosowane w praktyce – miały gwarantować zwycięstwo"[33]. Carl von Clausewitz podkreślał z kolei złożoność wojny jako zjawiska. Uważał, że tak wiele różnych okoliczności ma wpływ na przebieg wojny, że trzeba je możliwie szeroko brać pod uwagę. Nie istnieją żadne ogólne, identyczne zasady prowadzenia konfliktów zbrojnych. Strateg odpowiedzialny za ocenę całości musi mieć intuicję, dzięki której widzi prawdę w każdej chwili zmieniającej się rzeczywistości. Obaj wierzyli jednak, że trzeba dążyć do skutecznego zadania decydującego ciosu przeciwnikowi. Jest to istota zachodniego myślenia strategicznego – dążenie do decydującego zderzenia sił i złamania przeciwnika militarną przewagą. W chińskiej myśli strategicznej mądrością jest pokonanie przeciwnika bez potrzeby walki. Sun Tzu uważa, że „Wojna to Tao podstępu.

[33] S.P. Górka, *Antoine-Henri Jomini – twórca nowoczesnej strategii*, „Kwartalnik Bellona" 2018, nr 1 (692), s. 60.

Choć jesteś zdolny, udawaj przed wrogiem mało zdolnego. Gdy gotujesz się do działania, stwarzaj pozory bierności. Jeśli twój cel jest bliski, zachowuj się tak, jakby był odległy. A gdy jest odległy, udawaj, że jest bliski"[34]. W chińskiej strategii ogromną rolę odgrywa analiza psychologiczna, umiejętne wykorzystanie ludzkich słabości i pokus. Sun Tzu doradza „Zwab przeciwnika wizją zysków"[35]. Umiejętność manipulacji wrogiem pozwala wywołać w nim frustrację, osłabia jego zdolność do podejmowania dobrych decyzji. To zasadniczo odmienne podejście do istoty strategii ze strony Chin skutkowało przyjęciem przez USA błędnej perspektywy.

Większość wpływowych amerykańskich analityków uważała, że przystąpienie Chin do gospodarki światowej, jej otwarcie na globalizację, prędzej czy później doprowadzi do demokratyzacji ChRL. Model Hongkongu upowszechni się w Państwie Środka, stanie się rodzajem konia trojańskiego, pułapką dla reżimu komunistycznego. Kolejni amerykańscy prezydenci ulegli również presji wielkich korporacji, które były przekonane, że ich wejście na olbrzymi rynek chiński jest ekonomicznie i politycznie korzystne dla Stanów Zjednoczonych. Jak zauważa B. Góralczyk: „Dopiero teraz dociera do Amerykanów, że źle skalkulowali, jak też zbyt często ulegali pokusom zdobycia wielkiego chińskiego rynku. Kierowali się bardziej doraźnym interesem niż strategiczną wyobraźnią"[36]. Wśród wielu amerykańskich polityków dominowało przekonanie, iż Stany Zjednoczone potrafią właściwie rozumieć Chiny, a przez to umiejętnie wpływać na kierunek ich rozwoju. W 1967 r. R. Nixon powiedział: „Świat nie może być bezpieczny, dopóki Chiny się nie zmienią. Dlatego naszym celem, w zakresie, w jakim może-

[34] Sun Tzu, Sun Pin, *Sztuka wojny*..., op.cit., s. 15.

[35] Ibidem.

[36] B. Góralczyk, *Wielki renesans*..., op.cit., s. 448.

my wpływać na wydarzenia, powinno być doprowadzenie do tych zmian"[37]. Kurt M. Cambell, jeden z najbardziej wpływowych amerykańskich analityków specjalizujących się w problematyce chińskiej (w latach 2009–2013 odpowiadał w Departamencie Stanu za region Azji) podkreślał jak zasadniczą rolę w polityce USA wobec Chin odegrało to nastawienie Nixona. Jego zdaniem „Od tamtej pory założenie, że pogłębienie więzi handlowych, dyplomatycznych i kulturowych przekształci wewnętrzny rozwój Chin i ich zewnętrzne zachowanie, jest fundamentem amerykańskiej strategii"[38].

Taka logika działania okazała się bardzo kosztownym błędem dla Stanów Zjednoczonych. Jak zauważa autor: „Zaangażowanie dyplomatyczne i handlowe nie przyniosło politycznej i gospodarczej otwartości. Ani siła militarna USA, ani równowaga regionalna nie powstrzymały Pekinu przed próbą rozbicia podstawowych elementów systemu kierowanego przez USA. A liberalny porządek międzynarodowy nie zdołał zachęcić Chin tak mocno, jak oczekiwano. Zamiast tego Chiny podążyły własnym kursem, opierając się przy tym przed szeregiem amerykańskich oczekiwań"[39].

Analityk, który współtworzył błędną strategię Stanów Zjednoczonych wobec Chin, pisze dziś: „Punktem wyjścia do stworzenia lepszego podejścia winna być większa pokora co do zdolności Stanów Zjednoczonych do zmiany Chin. Ani próby izolowania i osłabiania ich, ani próby przekształcenia ich na lepsze nie powinny być podstawą strategii amerykańskiej w Azji. Zamiast tego Waszyngton powinien bardziej skupić się na eks-

---

[37] R. Nixon, *Asia After Viet Nam*, „Foreign Affairs", październik 1967, vol. 46, nr 1, s. 111–125.

[38] K.M. Cambell, E. Ratner, *The China Reckoning. How Beijing Defied American Expectations*, „Foreign Affairs", marzec/kwiecień 2018, vol. 97, nr 2, s. 60.

[39] Ibidem, s. 61.

pozycji własnej siły i zachowania, a także na sile i zachowaniu swoich sojuszników i partnerów. Oparcie polityki na bardziej realistycznych założeniach dotyczących Chin lepiej służyłoby interesom Stanów Zjednoczonych i nadało stosunkom biraterlnym bardziej zrównoważony charakter. (...) pierwszy krok jest stosunkowo prosty: uznanie, jak bardzo nasza polityka nie spełniła naszych aspiracji"[40].

Thomas J. Christensen, zastępca sekretarza stanu w ekipie prezydenta George'a W. Busha, uważa, że od początku chińskiej transformacji żaden kraj nie zrobił więcej, aby rozbudować siłę Chin niż USA. Same Stany Zjednoczone stworzyły największe zagrożenie dla swoich globalnych interesów. Po raz pierwszy konkurują one z państwem o porównywalnym potencjale gospodarczym i posiadającym ogromne doświadczenie strategiczne oparte na historycznej wyjątkowości Chin[41].

Zasadnicze, strategiczne błędy USA wynikały z niewłaściwej oceny charakteru kultury strategicznej Chin. W efekcie powstałego wzajemnego zapętlenia obu kultur strategicznych, powstała zasadniczo nowa sytuacja – obie strony przypisują przeciwnikowi odpowiedzialność za narastanie rywalizacji, co z dużym prawdopodobieństwem będzie wpływało na pogłębienie tego procesu i narastanie jego dysfunkcjonalności.

II. Chiny bardzo ostrożnie realizowały strategię wzrostu unikając konfrontacji z USA

Elity chińskie dokładnie przeanalizowały skutki porażki ZSRR w zimnej wojnie a także przyczyny rozpadu tego państwa. Ilość wnikliwych, pragmatycznych opracowań, poświęconych

[40] Ibidem, s. 70.

[41] T.J. Christensen, *The China Challenge*: *Shaping the Choices of a Rising Power*, New York–London 2015.

tej problematyce skutkowała przyjętymi zaleceniami dla partii i państwa. Miały też ogromny wpływ na decyzję o pacyfikacji studenckich protestów na Placu Tienanmen w 1989 r. Niedoceniana jest wśród większości analityków zachodnich zajmujących się współczesnymi Chinami i Komunistyczną Partią Chin skala traumy Tiananmen wśród partyjnej elity ChRL. Obawa przed niekontrolowanym wybuchem społecznym, który może zaprzepaścić wielką modernizację chińską, stoi u źródła wielu decyzji chińskich elit. Ważną przesłanką było przekonanie, że Chiny nie powinny stać się liberalną demokracją. Lee Kuan Yew, analizując tę kwestię z perspektywy Republiki Singapuru jednoznacznie twierdzi, iż gdyby Chiny wybrały tę drogę czeka je upadek. „Mam co do tego całkowitą pewność, a rozumie to również chińska inteligencja. Jeśli ktoś wierzy, że w Chinach może dojść do jakiejś rewolucji na rzecz demokracji, to jest w błędzie. Gdzie są teraz studenci z placu Tiananmen? Nie liczą się. Naród chiński chce odrodzonych Chin”[42] – zauważa Yew. To dlatego w wymiarze fundamentalnym nadal KPCh jest rdzeniem chińskiego systemu politycznego. Nadal też obowiązuje myśl Mao Zedonga, że „Komunistyczna Partia Chin jest kierowniczym trzonem całego narodu chińskiego. Bez takiego trzonu zwycięstwo sprawy socjalizmu jest niemożliwe”[43]. Deng Xiaoping był głównym twórcą strategii odbudowy władzy Chin. Warto pamiętać, że ma on za sobą długą karierę wojskową. Dowodził armią, która podbiła Tybet w 1950 r. Następnie, jako sekretarz generalny KPCh, po kampanii „100 kwiatów”,

[42] Lee Kuan Yew, *Wywiad dla Grahama Alllisona i Roberwa D. Blackilla, 11 maja 2011 r.*, [w:] *Chiny, Stany Zjednoczone i świat w oczach wielkiego mistrza Lee Kuan Yewa*, oprac. A. Graham, R.D. Blackwill, A. Wyne, Warszawa 2014, s. 41.

[43] Wystąpienie Mao Zedonga na spotkaniu z delegatami III Zjazdu Nowodemokratycznego Związku Młodzieży Chin, 25 maja 1957 r., – przytaczam za: *Wyjątki z dzieł przewodniczącego Mao Tse-Tunga (Czerwona książeczka)*, Wrocław 2005, s. 3.

brutalnie eliminował „elementy antypartyjne" na polecenie Mao Zedonga. Był odpowiedzialny za tak zwany Wielki Skok w latach 1958–1962, który doprowadził do tragedii „wielkiego głodu". Zgodnie z ustaleniami F. Dikötter liczba ofiar mogła osiągnąć 44 mln ludzi[44]. Jest to uważany za największą klęskę głodu w historii świata. Dopiero w okresie rewolucji kulturalnej Deng Xiaoping doświadczył prześladowań ze strony aparatu państwa komunistycznego. Te osobiste doświadczenia miały istotny wpływ na jego koncepcję modernizacji Chin i strategii realizowane wobec USA. Deng Xiaoping zostawił wskazówki dla swoich następców. Mają charakter krótkich porad (chengyu). Przedstawiają strategię Chin na przyszłość. Jak zauważa B. Góralczyk, „zwrócił się do swoich następców z następującymi zaleceniami, a nawet przykazaniami: – *lengjing guancha* – uważnie obserwować sytuację i analizować ją chłodno; – *yousuo zuowei* – próba wniesienia wkładu; – *wen zhu zhenjiao* – trzymać się mocno ziemi i mocno bronić własnych interesów; – *chenzhuo yingfu* – zbliżyć się do zmian w postępie spokojnie i z ufnością; – *shanyu shouzhuo* – uważaj, aby nie wywyższać się; – *Jue bu dang tou* – nie staram się być liderem; – *taoguang yanghui* – ukryj umiejętności i zamiary"[45].

Zwłaszcza ostatnie trzy rady – *shanyu shouzhuo*, *jue bu dang tou* i *taoguang yanghui* wskazują, że Deng zaleca wielką ostrożność w stosunkach z USA. Wyraźnie zaleca, aby nie prowokować Stanów Zjednoczonych – ukrywać nie tylko własny potencjał, ale także elementy stosowanej strategii. Wszyscy kolejni przywódcy ChRL przestrzegali tych zasad, aż do prezydentury Xi Jinpinga.

Lee Kuan Yew trafnie charakteryzuje strategię pozostawioną Chinom przez Deng Xiaopinga, gdy stwierdza, że polega

[44] F.Z. Dikötter, *Wielki głód. Tragiczne skutki polityki Mao 1958–1962*, Wołowiec 2013, s. 455.

[45] B. Góralczyk, *Wielki renesans...*, op.cit., s. 161.

ona „na wzroście w ramach istniejącego układu, uznawanego za wiążący, do momentu, gdy kraj stanie się na tyle silny, aby z powodzeniem dokonać przewartościowania porządku politycznego i gospodarczego”[46]. Gdy Chiny rozpoczynały proces swojej transformacji, dokonały bardzo gruntownej analizy zarówno przypadków udanej modernizacji azjatyckich państw, w tym głównie dokonań Lee Kuan Yew w Singapurze, jak również prób wprowadzania do gospodarki państw socjalistycznych elementów rynkowych. Nie mniejszą wagę przypisywano analizie historycznych chińskich doświadczeń. Autor *Sztuki wojny* zauważa, że: „W walce najtrudniejsze jest uczynienie skomplikowanego prostym, zamiana przeciwności w korzyści. Jeśli więc pokrzyżujesz plany wroga i zwabisz go zyskami, będziesz o krok przed nim, choćbyś później wyruszył. Potrafi to uczynić ten, kto zna taktykę dróg krętych i prostych”[47]. W toczącej się w Chinach dyskusji pomiędzy frakcją antyamerykańską (*fan Meipai*), proamerykańską (*qin Meipan*) a realistami, następowała stopniowa ewolucja stanowisk. Jednym z jej kluczowych elementów była coraz bardziej ożywiona dyskusja nad interesem narodowym ChRL, która od 2008 r. kładła nacisk na ochronę chińskich interesów narodowych[48]. Powodowało to, że większość stanowisk dostrzegała dwoistość relacji z USA. Doskonale odzwierciedla to stanowisko Wang Jisi, który w 2005 r. wyraził pogląd, iż Stany Zjednoczone nie są ani przyjacielem, ani wrogiem ChRL[49]. Chiny powinny umiejętnie wykorzystywać istniejącą sytuację wzajemnego gospodarczego

[46] Lee Kuan Yew, *Wywiad dla Grahama Alllisona...*, op.cit., s. 38; R. Miśkiewicz, *Przedsiębiorstwa we współczesnej gospodarce globalnej*, „Organizacja i Zarządzanie” 2018, nr 118, s. 410.

[47] Sun Tzu, Sun Pin, *Sztuka wojny...*, op.cit., s. 52.

[48] J.-P. Cabestan, *Polityka zagraniczna Chin*, Warszawa 20123, s. 126.

[49] Wang Jisi, *China's Search for Stability with America*, „Foreign Affairs”, wrzesień/październik 2005, vol. 84, nr 5, s. 39–40.

uzależnienia od siebie dwóch państw do zwiększania potęgi ekonomicznej ChRL, ale unikając zbyt radykalnych sytuacji. Równocześnie stopniowo Chiny winny rozbudowywać swój potencjał militarny, co musiało jednak skutkować narastającą rywalizacją strategiczno-wojskową między USA a ChRL. Paradoksalnie więc, pomimo zasadniczo odmiennej kultury strategicznej Stanów Zjednoczonych i Chin, oba państwa przyjmowały zbliżone założenia – że jest dla nich korzystna wzajemna współpraca gospodarcza – ale musiało to prowadzić do rosnącej między nimi rywalizacji. W 2015 r. w USA ukazał się głośny raport RAND Corporation, który ukazywał skalę zagrożeń, jakie stoją przed Stanami Zjednoczonymi ze strony Chin już w bliskiej perspektywie. Autorzy zauważali, że już do 2017 r. chińska armia uzyska zbliżony potencjał równowagi a nawet przewagi wobec sił USA rozmieszczonych w Azji na 6 z 9 analizowanych obszarów konwencjonalnej rywalizacji militarnej[50]. Według tego raportu w ciągu od 5 do 15 lat będzie się stopniowo kurczyła granica wpływów USA w Azji[51]. Widać wyraźnie, że ogólny schemat strategii Chin, pozostawiony przez Deng Xiaopinga, prowadził do sytuacji, w której narastała wzajemna sprzeczność między wyznaczanymi celami dla Chin a metodami ich realizacji. Analiza na gruncie metody zapętleń ukazuje, iż realizowana modernizacja chińskiego państwa wytworzyły zasadniczo nowe napięcia w jego strukturze i w jego relacjach z USA. Skala narastającej dysfunkconalności wymagała poszukiwania nowych rozwiązań.

[50] E. Heginbotham et al., *The US-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996–2017*, Santa Monica 2015, s. 29–30.

[51] Ibidem, s. 30,

III. Dojście do władzy Xi Jinpinga i kumulacja przez niego władzy spowodowało wzrost retoryki konfrontacyjnej z USA

Dlatego na długo przed XVIII Zjazem KPCh, który odbył się w listopadzie 2012 r. narastał wewnętrzny spór w chińskich elitach partyjnych dotyczący wyboru dalszej strategii. Elementem toczącej się rozgrywki stała się wielka afera korupcyjna, która zmarginalizowała Bo Xilaja i wspierającego go Zhou Yongkanga. Ostatecznie sytuacja ta wzmocniła frakcję wspierającą Xi Jinpinga. Jeszcze przez zjazdem, w kwietniu 2012 r. Bo Xilaj został zawieszony w prawach członka KC. Ten mer 33-milionowej metropolii Chongqing, zwolennik modelu rozwojowego Chin, który miałby wracać do pewnych założeń kolektywizacji, poważny kandydat do Stałego Komitetu Biura Politycznego KPCh, został oskarżony i skazany za udział w aferze korupcyjnej na dożywotnie więzienie. Jego ojciec, Bo Yibo, był bliskim współpracownikiem Mao Zedonga. Bo Yibo, planista i minister finansów, jeden z ulubionych przez Mao towarzyszy[52], w początkowym okresie rewolucji kulturalnej aktywnie uczestniczył w czystkach i namawiał do brutalności[53]. Potem sam był prześladowany razem ze swoją rodziną (jego żona popełniła samobójstwo lub została śmiertelnie pobita, a syn Bo Xilai już jako 16-latek trafił do więzienia). Bo Yibo, po piętnastu latach spędzonych w więzieniu, powrócił na szczyty władzy w epoce Deng Xiaopinga, stając się jednym z Ośmiu Nieśmiertelnych członków KPCh[54]. Odegrał istotną rolę w kolejnych awansach

[52] J. Fenby, *Chiny. Upadek i narodziny wielkiej potęgi*, Kraków 2009, s. 545

[53] F. Dikötter, *Rewolucja kulturalna. Historia narodu 1962–1976*, Wołowiec 2018, s. 96–97.

[54] J. Fenby, *Chiny*..., op.cit., s. 639.

syna. W 2002 r. jego Bo Xilaj wszedł w skład KC KPCh, a dwa lata później został ministrem finansów. Na zjeździe KPCh w 2007 r. został już członkiem Biura Politycznego i – jako sekretarz Komitetu Miejskiego w Chongqingu, zaczął kierować tą największą chińską metropolią. Droga awansu, fakt, że jego ojciec w historii KPCh miał szczególną pozycję, wskazywało, że może być jednym z najważniejszych osób w hierarchii partyjnej. Był też naturalnym rywalem Xi Jinpinga, którego ojciec, Xi Zhongxuna, już w wieku piętnastu lat został członkiem KPCh. W latach 1959–1962 był wicepremierem Chin, po czym został usunięty z partii podczas rewolucji kulturalnej i doświadczył prześladowań. W epoce Deng Xiaopinga został sekretarzem prowincji Guandong. Tutaj w 30-tysięcznym mieście graniczącym z Hong Kongiem stworzył pierwszą wolną strefę ekonomiczną w Chinach. W 1982 r. wysłano do niej dziesiątki tysięcy żołnierzy do tamtejszych firm budowlanych[55]. Jednak Xi Zhongxun już w 1981 r. powrócił do Pekinu i został wybrany do Biura Politycznego KPCh. W 1987 r. opowiedział się po stronie sekretarza generalnego KPCH Hu Yaobanga, zwolennika reform, którego Deng Xiaoping zmusił do złożenia urzędu. Rok później Xi przeszedł na emeryturę. Jego syn, dzięki wsparciu ze strony Geng Biao, sekretarza generalnego Centralnej Komisji Wojskowej KPCh, został w 1979 r. jego sekretarzem, co otworzyło mu drogę do dalszej kariery. W 1997 r. Xi Jinping, najmniejszą liczbą głosów, został wybrany do KC KPCh[56]. Na początku XX w. Nie był jednak brany pod uwagę wśród partyjnych elit jako jeden z potencjalnych przyszłych przywódców. Przełom nastąpił, gdy prezydent Hu Jintao wyznaczył go na początku 2007 r. do walki z korupcją. Sprawność z jaką zreali-

[55] R. McGregor, *Partia. Sekretny świat komunistycznych władców Chin*, Kraków 2013, s. 139.

[56] G. Allison, *Skazani na wojnę? Czy Ameryka i Chiny unikną pułapki Tukidydesa?*, Bielsko-Biała 2018, s. 146.

zował zadanie spowodowała, że w październiku 2007 r. został wybrany do 9-osobowego Stałego Komitetu Biura Politycznego i został zastępcą Hu Jintaja[57]. Gdy w 2012 r. stanął na czele partii, powszechne było oczekiwanie, iż będzie realizował model przywództwa wypracowany przez Deng Xiaopinga, a oparty na podejmowaniu decyzji w ramach Stałego Komitetu Biura Politycznego na zasadach konsensusu. Jednak Xi wykorzystał ten sam mechanizm, który otworzył mu drogę do władzy. Dokonał wielkiej kampanii antykorupcyjnej, której wykonawcą był Wang Qishana. W 2013 r. na dożywocie skazany został Bo Xilaj. Xi Jinping złamał tym samym „niepisaną dotychczasową zasadę, by najwyżsi rangą przywódcy w państwie nie podlegali ani śledztwom karnym ani nie ponosili odpowiedzialności karnej"[58]. W 2015 r. dożywotni wyrok otrzymał także Zhou Yongkan (członek Stałego Komitetu Biura Politycznego KC KPCh – w latach 2002–2012 odpowiadał m.in. za chińską bezpiekę. Jak zauważa B. Góralczyk „nawet Mao Zedong nigdy nie zdecydował się zaatakować »chińskiego Berii« Kang Shenga"[59]. Rok później Ling Jihua – osobisty sekretarz poprzedniego prezydenta – Hu Jintao, został skazany na dożywocie. Na ławie oskarżonych zasiadł także gen. Xu Caiho i gen. Guo Boxiong (były wiceszef Komisji Wojskowej) oraz gen. Fang Fenghui (były szef sztabu generalnego ChALW). Natomiast gen. Zhang Yang popełnił samobójstwo, gdy rozpoczął się proces przeciwko niemu. Łącznie, w ramach szerokiej operacji dokonanej z ramienia Xi Jinpinga, skazano 31 byłych i aktualnych członków KC KPCh, 122 ministrów i szefów lub wiceszefów prowincji, 36 generałów, a także 1,2 mln urzędników niższego szczebla[60]. Xi Jinping skumulował w swoich rękach władzę, której nikt nie

[57] Ibidem, s. 147.

[58] B. Góralczyk, *Wielki renesans...*, op.cit., s. 290.

[59] Ibidem, s. 290.

[60] Ibidem, s. 291–292.

miał w ChRL od czasów Mao Zedonga. Doprowadził też do nowelizacji konstytucji w marcu 2018 r. Usunięty został z niej zapis o dwukadencyjności. „Konsolidując władzę, Xi sam przyjął kilkadziesiąt tytułów, w tym przewodniczącego nowej narodowej rady bezpieczeństwa oraz głównodowodzącego sił zbrojnych, którego nie przyznano nawet Mao. Sam namaścił siebie jako »Najwyższego Przywódcę« Chin"[61]. Wybitny znawca problematyki chińskiej Andrew J. Nathan stwierdza" „W 2023 r. Xi Jinping zakończy swoją drugą kadencję jako prezydent Chin. Od czasu, gdy Deng Xiaoping zrewidował konstytucję kraju ponad trzydzieści pięć lat temu, dwie kolejne kadencje były największą, jaką prezydent może legalnie służyć. Ale jest coraz bardziej jasne, że Xi nie ma planów przejścia na emeryturę. W marcu Narodowy Kongres Ludowy... zatwierdził poprawkę do konstytucji, która zniosła ograniczenia kadencji na prezydenta, skutecznie otwierając drogę Xi do utrzymania stanowiska na czas nieokreślony. Xi wyłonił się jako rewanż Mao nad Dengiem. Deng uczynił bowiem to, czego Mao obawiał się, że zrobią jego następcy – zakończył permanentną rewolucję. Natomiast Xi zrobił dokładnie to, czego najbardziej obawiał się po swoich sukcesorach Deng – odnowił jednoosobowe rządy"[62]. Kumulacja władzy przez Xi definitywnie przekreśla model zarządzania państwem wypracowany przez Deng Xiaopinga, ale równocześnie sięga on do historycznej tradycji, w której dominował kult władzy cesarskiej. Xi Jinping już na XVIII Zjeździe KPCh w 2012 r. rzucił hasło o „wielkim renesansie narodu chińskiego" (*Zhonghua minzu weida fuxing*)[63]. Jest to program otwarcia nastawiony na konfrontację z USA. Xi postawił też

[61] G. Allison, *Skazani na wojnę...*, op.cit., s. 148.

[62] A.J. Nathan, *China: Back to the Future*, „The New York Review of Books", https://www.nybooks.com/articles/2018/05/10/china-back-to-the-future/,

[63] B. Góralczyk, *Wielki renesans...*, op.cit., s. 364.

przed narodem dwa cele na XXI stulecie – zbudowanie do 2012 r. społeczeństwa umiarkowanego dobrobytu, a do 2049 r. – na setną rocznicę powstania komunistycznych Chin – przyłączenie Tajwanu do ChRL. W 2017 r., na XIX Zjeździe dodał cel trzeci, pośredni – przekształcenie do 2035 r. Chin w społeczeństwo i państwo innowacyjne[64]. Xi wierzy, że uzyskanie przewagi przez Chiny w badaniach i technologicznych wdrożeniach sztucznej inteligencji zrealizuje sen o chińskim panowaniu nad światem. Ale to wyzwanie, jeśli analizujemy je w kategoriach metody zapętleń, z dużym prawdopodobieństwem jedynie zaostrzy rywalizację między USA a Chinami.

IV. Między Stanami Zjednoczonymi a Chinami, najbardziej niebezpieczny i nieprzewidywalny wyścig zbrojeń w historii ludzkości ma miejsce, aby zdobyć strategiczną przewagę nad przeciwnikiem dzięki sztucznej inteligencji

W lipcu 2017 r. rząd Chin przyjął krajowy program rozwoju sztucznej inteligencji[65]. Silnym impulsem do jego stworzenia było wydarzenie z marca 2016 r. Algorytm AlhaG pokonał chińskiego mistrza Lee Sedola, jednego z najwyżej ocenianych graczy na świecie w grze Go. Algorytm opierał się na heurystyce MCTS (*Monte Carlo Tree Search*) stworzonej przez brytyjską firmę DeepMind, nabytą w 2014 r. przez korporację Google. Stworzenie programu, który mógłby pokonać profesjonalnego gracza w Go było bardzo trudne ze względu na wielką złożoność tej gry. Do analizy trzech ruchów naprzód trzeba

[64] Ibidem, s. 364.

[65] J. Ding, *Deciphering China's AI Dream The context, components, capabilities, and consequences of China's strategy to lead the world in AI*, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf, s. 31 [dostęp: 12.01.2019].

obliczyć 8 mln kombinacji. Obliczenie piętnastu ruchów do przodu wymaga analizy liczby kombinacji większej niż liczba atomów we wszechświecie[66]. W chińskiej tradycji ta gra odgrywała szczególną rolę w rozwijaniu zdolności strategicznych. Algorytm AlphaGo wykorzystuje sztuczne sieci neuronowe Deep Learning. Tom Walsh porównuje algorytm AlphaGo z programem komputera Deep Blue, który pokonał w szachach Garri Kasparowa w 1997 r. Jak zauważa: „Deep Blue wykorzystywał specjalistyczny sprzęt do zbadania około 200 mln ruchów na sekundę. Dla porównania, AlphaGo wyznacza tylko 60 tys. pozycji na sekundę. Podejście prezentowane przez Deep Blue wykorzystywało brutalną siłę, aby znaleźć dobry ruch – ale to nie daje się dobrze przełożyć na bardziej skomplikowaną grę w Go. W przeciwieństwie do niego, AlphaGo miał znacznie większą zdolność do oceny pozycji, a umiejętności tej nauczył się rozgrywając miliardy gier ze sobą"[67].

Fakt, że firma która jest częścią amerykańskiej korporacji, a także współtworzy, z IBM, Microsoft, Amazon i Facebook, „Partnerstwo dla sztucznej inteligencji dla dobra ludzi i społeczeństwa" (Partnership on Artificial Intelligence to Benefit People and Society[68]), opracowała tak zaawansowany algorytm, było silnym impulsem dla chińskich polityków do zwiększenia nakładów na AI w ChRL.

Instytut Przyszłości Ludzkości (*Future of Humanity Institute* FHI) Uniwersytetu Oksfordzkiego, w swoim raporcie „Deciphering China's AI Dream The context, components, capabilities, and consequences of China's strategy to lead the world in AI", szczegółowo analizuje chiński program rozwoju sztucznej inteligencji. Analitycy FHI wskazują, że państwo to systematycznie

[66] T. Walsh, *To żyje. Sztuczna inteligencja. Od logicznego fortepianu po zabójcze roboty*, Warszawa 2018, s. 51.

[67] Ibidem, s. 101–102.

[68] PAIBP powstało w 2016 r.

zwiększało swoje wydatki na rozwój sztucznej inteligencji, ale ostatnio nastąpił logarytmiczny wzrost nakładów na ten cel.

Od 2017 do 2020 r. przewidziano w planach dziesięciokrotny wzrost finansowania technologii AI[69]. Cechą charakterystyczną chińskiej strategii jest silne poleganie na krajowych firmach, takich jak Meituan Dianping, DJI, ZTE, OnePlus, Tencent, GearBest, Haier, TCL, Skyworth, Bajdu, Alibaba, Toutiao, Huawei czy iFlyTek, a także wspieranie ich finansowo, jak również stworzenie bazy dla rozwoju własnych technologii i badań.

Chiny również umiejętnie wykorzystują duże ilości danych do rozwoju sztucznej inteligencji, które z kolei są zablokowane do wykorzystywania ich przez firmy i instytucje naukowe z innych państw[70].

Jednocześnie wdrożyły na szczeblu regionalnym i krajowym system poszukiwania i rekrutacji osób ze specjalnymi zdolnościami IT . Największe firmy chińskie otwierają również oddziały zagraniczne w celu poszukiwania i przyciągnięcia najbardziej utalentowanych ludzi do współpracy. Dobrym przykładem tej strategii jest aktywność koncernu Huawei w Europie Środkowej. Koncern ten posiada w Polsce oddział Huawei Consumer Business Group Polska, który zatrudnia tysiąc pracowników. Już w 2008 r. Huawai utworzył w RP swoje europejskie centrum dla obsługi 28 państw tego regionu[71]. Aktywnie też współpracuje z Politechniką Warszawską i Politechniką Poznańską. Stworzona Akademia Huawei działa w wyselekcjonowanych państwach świata. W Polsce dzięki niej koncern może pozyskiwać do współpracy najwybitniejszych studentów kształcących się

---

69 J. Ding, op.cit., s. 31.

70 Ibidem.

71 A. Jadczak, *Huawei zatrudni nawet 500 osób w dziale R&D w Warszawie*, https://itwiz.pl/huawei-zatrudni-nawet-500-osob-dziale-rd-warszawie/ [dostęp: 21.01.2020].

w nowoczesnych technologiach informacyjnych. Wybrani z nich przechodzą szkolenie w centrali firmy w Shenzhen. Ten przykład doskonale ilustruje stosowane metody. Wyselekcjonowanym osobom oferowane są atrakcyjne miejsca pracy w samych Chinach[72]. Raport wskazuje na szczególny nacisk na rozwój robotyki i inteligentnych procesów produkcyjnych, które mają opierać się na krajowych rozwiązaniach i technologiach[73].

Zgodnie z planem, Chiny zamierzają rozwijać swój przemysł sztucznej inteligencji do poziomu najbardziej rozwiniętych państw w tej dziedzinie do 2020 r. W perspektywie 2025 r., chcą zdobyć dominację w niektórych obszarach AI, aby w 2030 r. stać się globalnym centrum badań i innowacji związanych ze sztuczną inteligencją, co ma dać ogromny impuls dla chińskiej gospodarki szacowany na 150,8 mld USD (sektor AI), a uwzględniając inne branże powiązane ze sztuczną inteligencją 1,5 bln USD[74]. Chiny rozwijają też inne obszary technologiczne, które wspierać będą ekspansję sztucznej inteligencji. Poczyniły imponujący skok w budowie superkomputerów. Jeszcze w 2014 r. na globalnej liście Top 500 USA miały 232 takie maszyny (46,4%), a Chiny 76 (15,2%), ale już 3 lata później na tej liście TOP500 w czerwcu 2017 r. ChRL miał już 159 superkomputery (31,8%), a USA 168 systemów (33,6%)[75].

W raporcie wskazano, że Chiny już w 2014 r. wyprzedzało Stany Zjednoczone pod względem zarejestrowanych patentów dotyczących sztucznej inteligencji, a także artykułów naukowych dotyczących procesów *głębokiego uczenia* się. Jednak są one nadal daleko od USA w dziedzinie badań podstawowych[76].

---

[72] J. Ding, op.cit., s. 4–5.

[73] Ibidem, s. 5.

[74] Ibidem, s. 10.

[75] Ibidem, s. 24.

[76] Ibidem, s. 26.

Wielu analityków wskazuje, że potencjał sztucznej inteligencji opracowany przez USA i ChRL może odgrywać kluczową rolę w zdobywaniu przewagi strategicznej nad przeciwnikiem przez jedno z tych państw. Wysoki stopień fuzji cywilno-wojskowej w ChRL budzi uzasadnione obawy dotyczące powszechnego wykorzystania zdolności militarnych sztucznej inteligencji w chińskich siłach zbrojnych[77]. Stworzona narodowa strategia fuzji militarno-cywilnej (*junmin ronghe*) ma doprowadzić do zbudowania armii gotowej do działań w wojnach inteligentnych[78]. Chiny dążą „do synergii między naukami o mózgu, sztuczną inteligencją (AI) i biotechnologią, co ma mieć ogromne konsekwencje dla przyszłej siły militarnej"[79]. Niewiele informacji dociera do ogółu społeczeństwa na temat badań przeprowadzonych w Chinach w tej dziedzinie rozwoju sztucznej inteligencji. Jednak poziom zaawansowania realizowanych projektów potwierdza globalna pozycja wielu przedsiębiorstw chińskich. Megvia i SenseTime dominują w algorytmach rozpoznawania twarzy. Technologia, która ma umożliwić aktywną obserwację obywateli korzystających z kamer CCTV i urządzeń przenośnych, został opracowany przez SenseTime. W listopadzie 2016 r. naukowcy z Shanghai Jiao Tong University w Chinach przedstawili system, który uczy się odróżnić przestępców od innych ludzi na podstawie ich zdjęć[80]. DJI ma 70% udziałów w globalnym rynku dronów. Jego produkty są wyposażone w algorytmy do rozpoznawania obiektów w terenie. Firma Ubtech Robotics ma silną pozycję na rynku robotów humanoidalnych. Cambricon Technologies wyposaża smartfony Huawei w chi-

[77] Ibidem, s. 32–33.

[78] E.B. Kania, *Minds at War. China's Pursuit of Military Advantage through Cognitive Science and Biotechnology*, „PRISM" 2019, vol. 8, nr 3, s. 84.

[79] Ibidem, s. 83.

[80] T. Walsh, *To żyje. Sztuczna inteligencja*..., op.cit., s. 226.

py, które pozwalają im korzystać z algorytmów uczenia głębokiego. iFlytTek specjalizuje się w algorytmach, które pozwalają ludziom rozmawiać z maszyną, a Cloudwalk tworzy technologie sztucznej inteligencji, które zapewniają bezpieczeństwo publiczne[81]. Jakość tych rozwiązań została przetestowana w Chinach w trakcie walki z koronawirusem COVID-19. Dla potrzeb przyszłego pola Chińczycy prowadzą badania umożliwiające połączenie inteligencji ludzkiej z maszynową[82]. Służyć ma temu między innymi China Brain Project, który jest realizowany od 2016 r. w perspektywie do 2030 r. Jak podkreśla *Moo-ming Poo, dyrektor chińskiego Institute of Neuroscience* (ION) i *Centre for Excellence in Brain Science and Intelligence Technology of Chinese Academy of Sciences* (CAS) „W porównaniu z innymi projektami CBP ma bardziej kompleksowy charakter; obejmuje podstawowe badania neuronalnych funkcji poznawczych, badania stosowane w opracowywaniu metod diagnozowania i interwencji zaburzeń mózgu, a także metody i urządzenia komputerowe inspirowane mózgiem"[83].

Chińska Armia Ludowo-Wyzwoleńcza powołana też w 2017 r. Komitet Sterujący Wojskowych Badań Naukowych wzorowany na amerykańskim *Defense Advanced Research Projects Agency* (DARPA). Ma ona ustalać priorytet w prowadzonych badaniach i wyznaczać strategiczne kierunki rozwoju militarnych technologii. Chiński gen. He Fuchu, były prezes Akademii Wojskowej Nauk Medycznych, a następnie wiceprezes Akademii Nauk

---

[81] E. Cieślik, *Chiny zaskakują sztuczną inteligencją*, Obserwatorfinansowy.pl, https://www.obserwatorfinansowy.pl/tematyka/makroekonomia/chiny-zaskakuja-sztuczna-inteligencja/ [dostęp: 12.01.2019].

[82] E.B. Kania, *Minds at War. China's Pursuit...*, op.cit., s. 84.

[83] Ling Wang, *Interview. Moo-ming Poo: China Brain Project and the Future of Chinese neuroscience*, [w:] National Science Review 24 February 2017, https://www.researchgate.net/publication/314070218_Mu-ming_Poo_China_Brain_Project_and_Future_of_Chinese_Neuroscience [dostęp: 12.02.2020].

Wojskowych wskazuje na konieczność militaryzacji biotechnologii i połączenia jej z nanotechnologią i sztuczną inteligencją, aby wykorzystać je w warunkach przyszłego konfliktu zbrojnego. Jego zdaniem Chiny winny uwzględniać, iż przyszła wojna obejmie domenę ludzkiej świadomości, a ludzki mózg stanie się domeną przyszłej walki. Dlatego Chiny powinny wypracować modele integracji ludzkiej i sztucznej inteligencji[84].

Najbardziej niebezpieczny i nieprzewidywalny wyścig w historii ludzkości odbywa się głównie między USA i Chinami. Obie strony są zainteresowane uzyskaniem przewagi strategicznej nad przeciwnikiem. Aplikacje sztucznej inteligencji o największym znaczeniu dla walki i przewagi strategicznej będą również najtrudniejsze do prawnego uregulowania, ponieważ państwa będą zainteresowane inwestowaniem w ich rozwój i nie przestrzeganiem wszelkich ograniczeń związanym z ewentualną skutecznością ich zastosowania. Wyścig zbrojeń będzie w coraz większym stopniu oparty na prognozach przyszłego pola bitwy na którym dominować będą autonomiczne systemy do walki z autonomicznymi systemami przeciwnika.

Z drugiej strony nowoczesne technologie AI zaczęły stwarzać dla KPCh coraz bardziej rozbudowane narzędzia nadzoru społecznego. Mają one jednak dwoistą naturę – mogą być też użyte do eskalacji protestów społecznych. Ten dylemat doskonale ukazuje Lee Kuan Yew. Chińskie społeczeństwo w coraz większym stopniu ma dostęp do nowoczesnych środków informacji. Będą coraz lepiej poinformowani. Jak zauważa Yew „Nie będzie można rządzić nimi w taki sposób, jak rządzi się dzisiaj, kiedy wystarczy udobruchać i nadzorować parę osób. Ponie-

[84] E. Kania, W. VornDick, *China's Military Biotech Frontier: CRISPR, Military-Civil Fusion, and the New Revolution in Military Affairs*, China Brief, październik 2019, vol. 19, nr 18, The Jamestown Fundation, https://jamestown.org/program/chinas-military-biotech-frontier-crispr-military-civil-fusion-and-the-new-revolution-in-military-affairs/ / [dostęp: 12.02.2020].

waż będzie ich do upilnowania bardzo dużo”[85]. Podkreśla, że „Jeśli Chiny zmienią się w sposób pragmatyczny, tak jak czynią to do tej pory, utrzymując przy tym ścisłą kontrolę bezpieczeństwa, nie dopuszczając do zamieszek i rebelii, a jednocześnie łagodząc system... dając więcej uprawnień władzom prowincji, więcej uprawnień miastom, więcej władzy u podstaw... to system jest do utrzymania”[86]. Pogłębi to jednak przepaść między USA a Chinami w rozumieniu wzajemnych strategii i w gotowości szukania konsensusu między dwoma zasadniczo sprzecznymi koncepcjami porządku światowego”[87].

V. Amerykański-chiński wyścig o strategiczną dominację w dziedzinie sztucznej inteligencji może doprowadzić do powstania superinteligencji, która stanie się niezależna od ludzkości

Nick Bostrom wierzy, że „...można rozsądnie przypuszczać, że sztuczna inteligencja dorównująca ludzkiej ma całkiem spore szanse zostać opracowana do połowy tego wieku, a przy tym niezerowe są szanse na to, że pojawi się znacznie szybciej albo znacznie później”[88]. Analiza kilku obszarów, w których opracowywane są technologie sztucznej inteligencji, pokazuje, że tempo ich rozwoju przyspiesza coraz bardziej. Staje się prawdziwym wyzwaniem współczesnego pokolenia spojrzenie w przyszłość i niedokonanie w tym mierze błędu, który radykalnie ograni-

[85] T. Plate, *Conversation with Lee Kuaqn Yew: Citizens Singapore: How to Build a Nation*, Singapore 2010, s. 113, za: A. Graham, R.D. Blackwill, A. Wyne (oprac.), *Chiny, Stany Zjednoczone i świat w oczach wielkiego mistrza Lee Kuan Yewa*, Warszawa 2014, s. 36–37.

[86] Ibidem, s. 37.

[87] G. Allison, *Skazani na wojnę...*, op.cit., s. 180.

[88] N. Bostrom, *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016, s. 44.

czy perspektywę rozwoju ludzkości. Już dziś widać, że sztuczna inteligencja będzie radykalnie zmieniać nasze poznawcze perspektywy i nasze miejsce w świecie. Ray Kurzweil wyraźnie stwierdza: „Inteligencja jaką stworzymy dzięki inżynierii odwrotnej mózgu, będzie miała dostęp do własnego kodu źródłowego i będzie mogła się w szybkim tempie ulepszać w czasie powtarzających się cykli projektowych”[89]. Kluczową kwestią, jaką napotykają w ciągu najbliższych trzydziestu lat, jest dynamika wybuchu sztucznej inteligencji. Nick Bostrom twierdzi, że powolne wyjście – liczone w dziesięcioleciach – to szansa na zbudowanie infrastruktury bezpieczeństwa: „Kraje obawiając się wyścigu zbrojeń w obszarze sztucznej inteligencji będą miały czas, by podjąć próby wynegocjowania stosownych traktatów i opracować mechanizmy ich wyegzekwowania”[90]. Jest to jednak scenariusz, który wydaje się mniej prawdopodobny.

Analiza powinna również uwzględniać opcję, która jest skrajnie niekorzystna dla ludzkości. Jest to sytuacja, gdy dochodzi do gwałtownego wybuchu sztucznej inteligencji. Bostrom zauważa, że: „Do szybkiego odejścia dochodzi w krótkim czasie liczonym w minutach, godzinach lub dniach. Scenariusze szybkiego odejścia nie pozostawiają ludzkości wiele czasu do namysłu. Być może nikt nawet nie zauważy nic nadzwyczajnego dopóki partia nie będzie już przegrana. W scenariuszu szybkiego odejścia los ludzkości zależy zasadniczo od poczynionych wcześniej przygotowań”[91].

Strategiczna perspektywa ludzkości musi uwzględniać pojawienie się sztucznej inteligencji i obejmować również opcję, w której wykracza ona poza punkt krytyczny i osiąga ogromną przewagę nad ludźmi możliwościami we wszystkich dzie-

[89] R. Kurzweil, *Jak stworzyć umysł. Sekrety ludzkich myśli ujawnione*, Białystok 2018, s. 363.

[90] N. Bostrom, *Superintelcja...*, op.cit., s. 103.

[91] Ibidem.

dzinach wiedzy. Generał Robert H. Latiff słusznie wskazuje, że niewielu rozumie, co przyniesie przyszłość, a przerażająco niewielu zdaje się o to troszczyć[92]. Dalsze badania nad AI nie mogą po prostu obejmować strategii jej rozwoju. Należy w coraz większym stopniu uwzględniać nową logikę ryzyka. Czy zmienimy paradygmat nauk bezpieczeństwa i wziąć pod uwagę rzeczywistość scenariusza wybuchu sztucznej inteligencji może określić nie tylko naszą przyszłość, ale nasze istnienie jako ludzkość.

USA i Chiny w realizowanej przez siebie strategii dominacji w obszarze sztucznej inteligencji, który ma pozwolić im na osiągniecie zwycięstwa w globalnej rywalizacji, nie dostrzegają, że zasadnicza strategiczna przepaść, wynikająca z zasadniczo odmiennego podejścia aksjologicznego między obu państwami, stanowi pułapkę, która może utrudnić dostrzeżenie zagrożenia w momencie, gdy w efekcie tej rywalizacji może dojść do gwałtownego wybuchu sztucznej inteligencji.

Wnioski

Różne kultury strategiczne USA i Chin zwiększają prawdopodobieństwo konfrontacji między tymi dwoma państwami. Głównym obszarem walki o dominację będą nowoczesne technologie. Obydwa państwa uważają, że wygranie wyścigu w obszarze sztucznej inteligencji da im strategiczną przewagę nad swoimi przeciwnikami.

Jednak USA i Chiny muszą brać pod uwagę fakt, że ich konkurencja o prymat w dziedzinie sztucznej inteligencji może doprowadzić do powstania superinteligencji, która będzie miała ogromną przewagę nad ludźmi we wszystkich dziedzinach

[92] A.H. Latiff, *Wojna przyszłości. W obliczu nowego globalnego pola bitwy*, Warszawa 2018, s. 23.

wiedzy. Wytworzenie środowiska ludzkiego i rozwój technologii sztucznej inteligencji doprowadzi do rozwoju systemów autonomicznych i zwiększy ich niezależność. Trwający wyścig technologiczny między USA i Chinami ma wymiar wojskowy. Toby Walsh ostrzega, że autonomiczne bronie zdestabilizują obecny system geopolityczny. Zniszczą one delikatną równowagę zbudowaną po II wojnie światowej. Nasza planeta stanie się bardziej niebezpiecznym miejscem[93]. W wyścigu zbrojeń, w którym USA i Chiny wykorzystują technologie sztucznej inteligencji, aby zyskać przewagę strategiczną nad przeciwnikiem, istnieje niezerowe prawdopodobieństwo niekontrolowanej eksplozji superinteligencji i powstaniem radykalnie niekorzystnej sytuacji dla całej ludzkości.

Bibliografia

Ball P., *Masa krytyczna. Jak jedno z drugiego wynika*, Kraków 2007.

Barrow J.D., *Kres możliwości? Granice poznania i poznanie granic*, Opole 2005.

Bostrom N., *Superinteligencja. Scenariusze, strategie, zagrożenia*, Gliwice 2016.

Brożek B., *Granice interpretacji*, Kraków 2018.

Brynjolfsson E., Mcafee A., *Drugi wiek maszyn. Praca, postęp i dobrobyt w czasach genialnych technologii*, Warszawa 2015.

Cabestan J.-P., *Polityka zagraniczna Chin*, Warszawa 2013.

Cambell K.M., Ratner E., *The China Reckoning. How Beijing Defied American* Expectations, „Foreign Affairs", marzec/kwiecień 2018, vol. 97, nr 2.

Christensen Th.J., *The China Challenge: Shaping the Choices of a Rising Power*, New York–London 2015.

[93] T. Walsh, *To żyje...*, opcit., s. 192.

Dikötter F., *Wielki głód. Tragiczne skutki polityki Mao 1958––1962*, Wołowiec 2013.
Fenby J., *Chiny. Upadek i narodziny wielkiej potęgi*, Kraków 2009.
Fitzgerald C.P., *Chiny. Zarys historii kultury*, Warszawa 1974.
Gernet J., *Inteligencja Chin. Społeczeństwo i mentalność*, Warszawa 2008;
Góralczyk B., *Wielki renesans. Chińska transformacja i jej konsekwencje*, Warszawa 2018.
Górka S.P., *Antoine-Henri Jomini – twórca nowoczesnej strategii*, „Kwartalnik Bellona" 2018, nr 1 (692).
Graham A.G., *Skazani na wojnę? Czy Ameryka i Chiny unikną Pułapki Tukidydesa*, Bielsko-Biała 2018.
Graham A., Blackwill R.D., Wyne A. (oprac.), *Chiny, Stany Zjednoczone i świat w oczach wielkiego mistrza Lee Kuan Yewa*, Warszawa 2014.
Granet M., *Cywilizacja chińska*, Warszawa 1973.
Grenda B., Grochmalski P., Świeboda H. (red.), *National Security Forecast. Polish Perspective*, Poznań 2019.
Grochmalski P., *Autorytaryzm centroazjatycki a kwestia transformacji systemowej – próba poszukiwania modelu metodologicznego*, [w:] *Przywództwo, elity i transformacje w krajach WNP. Problemy metodologii badań*, t. 1, red. T. Bodio, Warszawa 2010.
Heginbotham E. et al, *The US–China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996––2017*, Santa Monica 2015.
Heller M., *Filozofia przypadku*, Kraków 2014.
Huntington H., *Zderzenie cywilizacji i nowy kształt ładu światowego*, Warszawa 2000,
Jisi W., *China's Search for Stability with America*, „Foreign Affairs", wrzesień/październik 2005, vol. 84, nr 5.
Kania E.B., *Minds at War. China's Pursuit of Military Advan-*

tage through Cognitive Science and Biotechnology, „PRISM" 2019, vol. 8, nr 3.
Kennedy P., *U progu XXI wieku (przymiarka do przyszłości)*, London 1994.
Kissinger H., *O Chinach*, Wołowiec 2014.
Kurzweil R., *Jak stworzyć umysł. Sekrety ludzkich myśli ujawnione*, Białystok 2018.
Kurzwail R., *Nadchodzi osobliwość. Kiedy człowiek przekroczy granice biologii*, Warszawa 2013.
Latiff R.H., *Wojna przyszłości. W obliczu nowego globalnego pola bitwy*, Warszawa 2018.
Lee Kuan Yew, *Wywiad dla Grahama Alllisona i Roberwa d. Blackilla, 11 maja 2011 r.*, [w:] *Chiny, Stany Zjednoczone i świat w oczach wielkiego mistrza Lee Kuan Yewa*, oprac. A. Graham, R.D. Blackwill, A. Wyne, Warszawa 2014.
Mayor F., Bindé J.(wsp.), *Przyszłość świata*, Warszawa 2001.
McGregor R., *Partia. Sekretny świat komunistycznych władców Chin*, Kraków 2013.
Mearsheimer J., *Tragizm polityki mocarstw*, Kraków 2019.
Miśkiewicz R., *Knowledge transfer in the prospect of Industry 4.0 in terms of developing innovative technologies for electromobility*, [w:] *Urban Electromobility in the context of industry 4.0*, oprac. W. Drożdż, R. Miśkiewicz, F. Elżanowski, J. Pokrzywniak (wsp.), Toruń 2019.
Miśkiewicz R., *Przedsiębiorstwa we współczesnej gospodarce globalnej*, „Organizacja i Zarządzanie" 2018, nr 118.
Nixon R., *Asia After Viet Nam*, „Foreign Affairs", październik 1967, vol. 46, nr 1.
Rodziński R., *Historia Chin*, Wrocław–Warszawa–Kraków––Gdańsk 1974.
Schwartz B.L. *Starożytna myśl chińska*, Kraków 2009
Sun Tzu, Sun Pin, *Sztuka wojny*, Gliwice 2014.
Taleb N.N., *Czarny łabędź*, Warszawa 2015.

Walsh T., *To żyje. Sztuczna inteligencja. Od logicznego fortepianu po zabójcze roboty*, Warszawa 2018.

Westad O.A., *The Souces of Chinese Conduct. Are Washington and Beijing Fighting a New Cold War?*, „Foreign Affairs", Sept/Octob., vol. 98, nr 5.

Whyte A.F., *China and Foreign Powers*, Oxford 1928

Wójcik G.M., *Obliczenia płynowe w modelowaniu mózgu,* [w:] *Neurocybernetyka teoretyczna*, red. R. Tadeusiewicz, Warszawa 2009.

Wyjątki z dzieł przewodniczącego Mao Tse-Tunga (Czerwona książeczka), Wrocław 2005.

Źródła internetowe

Cieślik E., *Chiny zaskakują sztuczną inteligencją*, Obserwator Finansowy, https://www.obserwatorfinansowy.pl/tematyka/makroekonomia/chiny-zaskakuja-sztuczna-inteligencja/.

Ding J., *Deciphering China's AI Dream The context, components, capabilities, and consequences of China's strategy to lead the world in AI*, https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream.pdf.

Jadczak A., *Huawei zatrudni nawet 500 osób w dziale R&D w Warszawie*, https://itwiz.pl/huawei-zatrudni-nawet-500-osob-dziale-rd-warszawie/.

Kania E., VornDick W., *China's Military Biotech Frontier: CRISPR, Military-Civil Fusion, and the New Revolution in Military Affairs*, China Brief, październik 2019, vol. 19, nr 18, *The Jamestown Fundation*, https://jamestown.org/program/chinas-military-biotech-frontier-crispr-military-civil-fusion-and-the-new-revolution-in-military-affairs/.

Nathan A.J., *China: Back to the Future*, „The New York Review of Books", https://www.nybooks.com/articles/2018/05/10/china-back-to-the-future/.

Wang L., *Interview. Moo-ming Poo: China Brain Project and the Future of Chinese neuroscience*, „National Science Review", 24.02.2017, https://www.researchgate.net/publication/314070218_Mu-ming_Poo_China_Brain_Project_and_Future_of_Chinese_Neuroscience.

Abstrakt

Artykuł analizuje rywalizację Chińskiej Republiki Ludowej ze Stanami Zjednoczonymi w badaniach i zastosowaniach sztucznej inteligencji (Artificial Inteligence). Wśród przywództwa Komunistycznej Partii Chin jak i wpływowych elit USA narasta przekonanie, że to państwo, które właściwie wykorzysta technologie sztucznej inteligencji, w tym głównie algorytmy głębokiego uczenia, może uzyskać strategiczną przewagę nad przeciwnikiem. Rosnący wyścig między Stanami Zjednoczonymi i Chinami o dominację w AI jest potencjalnie najbardziej niebezpiecznym konfliktem w historii świata. Nie ma precedensu. Państwo, które wygra, będzie miało ogromną przewagę strategiczną nad swoim przeciwnikiem. Przywódcy USA i ChRL nadal widzą możliwość osiągnięcia konsensusu. Jednak staje się coraz trudniejsze do osiągnięcia. Strategia obecnego chińskiego przywódcy, Xi Jinpinga, jest coraz bardziej konfrontacyjna wobec USA.

Słowa kluczowe: sztuczna inteligencja, Stany Zjednoczone, Republika Chińska, wyścig zbrojeń, strategia USA wobec Chin, strategia Chin wobec USA, strategiczna wyobraźnia

Abstract

The article analyzes the rivalization between the United States and the People's Republic of China in investigating and implementing Artificial Intelligence (AI). Among the PRC leadership and influential US' elites there is a growing conviction that the state which will properly use AI technology, including deep learning algorithms, may gain strategic advantage over its opponents. The increasing pace of race between the US and the PRC for the AI potentially is the most dangerous conflict in the world's history. There is no precedence. The state that wins will have tremendous strategic advantage over its opponent. The US' and PRC's leaders still see a possibility of consensus. However, it is becom-

ing more difficult to achieve. The strategy of the current Chinese leader, Xi Jinping, is confrontational toward the US.

Keywords: artificial intelligence, the United States, the People's Republic of China, armaments race, US' strategy toward the PRC, PRC's strategy toward the US, strategic imagination

Monika Nowikowska
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0001-5166-8375

Światowy Indeks Cyberbezpieczeństwa na przykładzie wybranych państw Azji i Oceanii

Za zapewnienie bezpieczeństwa kraju uważano kiedyś posiadanie wielotysięcznej armii, najnowszej broni oraz innej infrastruktury wojskowej. Wraz z pojawieniem się komputerów bezpieczeństwo ewoluowało w kierunku bezpieczeństwa informacji[1]. Powszechnie uważa się, że jeśli państwo nie może kontrolować swoich zasobów cybernetycznych, nie jest bezpieczny. Ataki w cyberprzestrzeni odbywają się codziennie. Jeśli kraj nie dysponuje bezpiecznymi systemami, nie tylko całe państwo, ale także jego obywatele są narażeni na naruszenie ich podstawowych praw. Instytucje finansowe wspierające gospodarkę są narażone na kradzież danych z powodu niepewnych systemów cybernetycznych. W wyniku ataków w cyberprzestrzeni może być także zagrożona infrastruktura kraju.

Mając na uwadze powyższe, ataki na informacje przechowywane w systemie komputerowym mogą mieć dwojaki charakter: jako chęć podważenia wiarygodności systemu albo kradzież informacji. W pierwszym przypadku cyberterroryści w sieci wprowadzają własne dane bądź manipulują danymi zapisami w systemie. Ataki te mają na celu dezorganizację działania państwa, co

[1] W. Kitler, *Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne*, [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 19.

jest ze szkodą dla całego społeczeństwa. Działania te mogą być skierowane na infrastrukturę krytyczną, zaopatrzenie w wodę i energię, infrastrukturę telekomunikacyjną itp. Wywieranie wpływów na te systemy może także prowadzić do zniszczeń materialnych czy ofiar w ludziach, np. w przypadku spowodowania kolizji w ruchu pociągów. Atak cybernetyczny polegający na podważeniu wiarygodności systemu lub kradzieży informacji może zatem dotyczyć zarówno zasobów krajowych, jak i informacji, których właścicielem jest jednostka – obywatel[2].

Wobec wyżej opisanych zagrożeń powstaje pytanie, które państwa są najbezpieczniejsze? Istnieją raporty i artykuły, które próbują odpowiedzieć na to pytanie. Jednym z nich jest *Global Cybersecurity Index* – Globalny (Światowy) Indeks Cyberbezpieczeństwa (GCI), który publikowany jest przez Międzynarodowy Związek Telekomunikacyjny. Powszechnie przyjmuje się, że Indeks jest najdokładniejszym rankingiem dojrzałości państw w zapewnieniu polityki cyberbezpieczeństwa. Raport analizuje państwa pod względem ich dojrzałości pod względem prawnym, technicznym, organizacyjnym, budowania zdolności i współpracy.

Międzynarodowy Związek Telekomunikacyjny (ang. *International Telecommunication Union* tzw. ITU) jest wyspecjalizowaną agencją Organizacji Narodów Zjednoczonych ds. Technologii Informacyjnych i Komunikacyjnych[3]. Powszechnie przyjmuje się, że podmiot ten angażuje się w „łączenie świata". Praktycznie każdy aspekt współczesnego życia, od biznesu, kultury, po rozrywkę, pracę w domu – uzależniony jest od technologii informacyjnych i komunikacyjnych. W celu ułatwienia międzynarodowej łączności w sieciach komunikacyjnych, organizacja opracowuje standardy techniczne, które zapewniają

[2] B. Hołyst, *Terroryzm*, Warszawa 2011, s. 961.

[3] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx [dostęp: 30.11.2019].

bezproblemowe połączenie sieci i technologii oraz dąży do poprawy dostępu do technologii informacyjno-komunikacyjnych dla społeczności o ograniczonym dostępie na całym świecie. ITU angażuje się także w łączenie wszystkich ludzi na świecie – niezależnie od tego, gdzie mieszkają i bez względu na środki, wspierając prawo każdego do komunikacji.

Współcześnie istnieją miliardy abonentów telefonów komórkowych, blisko pięć miliardów ludzi z dostępem do telewizji i dziesiątki milionów nowych użytkowników Internetu. Globalna międzynarodowa sieć telekomunikacyjna jest największym i najbardziej zaawansowanym osiągnięciem inżynieryjnym, jaki kiedykolwiek powstał. Używamy jej za każdym razem, gdy logujemy się do Internetu, wysyłamy e-mail lub SMS, słuchamy radia, oglądamy telewizję, podróżujemy samolotem[4].

Do podstawowych zadań ITU należy m.in.:

- wspieranie rewolucji mobilnej, poprzez opracowywanie standardów technicznych i ram polityki, które umożliwiają mobilny i szerokopasmowy dostęp do Internetu;
- współpraca z partnerami z sektora publicznego i prywatnego, w celu zapewnienia dostępu i usług technologii informacyjnych i komunikacyjnych (ICT) w sposób przystępny, sprawiedliwy i uniwersalny;
- wspieranie ludzi na całym świecie poprzez edukację i szkolenia technologiczne;
- opracowywanie standardów, protokołów i umów międzynarodowych jako podstawowych elementów leżących u podstaw globalnego systemu telekomunikacyjnego;
- wspieranie komunikacji w następstwie katastrof i nagłych wypadków – poprzez pomoc naziemną, dedykowane kanały komunikacji awaryjnej, standardy techniczne dla

[4] E. Milczarek, *Cyberbezpieczeństwo – wyzwanie XXI wieku*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017, s. 26.

systemów wczesnego ostrzegania oraz praktyczną pomoc w odbudowie po katastrofie;
– współpraca z branżą IT w celu zdefiniowania nowych technologii.

Jednym z zadań ITU jest publikacja Globalnego Indeksu Cyberbezpieczeństwa (*Global Cybersecurity Index* – GCI). Przyjmuje się, że GCI przyczynia się do podnoszenia świadomości w zakresie bezpieczeństwa w cyberprzestrzeni w najsłabiej rozwiniętych państwach świata, dostarczając wskazówek na temat działań w zakresie budowania zdolności, które mogą być podejmowane na poziomie krajowym. ITU podejmuje także inicjatywę uświadamiania państwom potrzeby i znaczeniaustanowienia krajowych zespołów reagowania na incydenty komputerowe tzw. CIRT, a także krajowych strategii bezpieczeństwa cybernetycznego, zapewniając im podstawowe narzędzia do jego ustanowienia[5]. Można uznać, że GCI pozwala na udzielenie odpowiedzi: Jak rządy (państwa) są bezpieczne? Problematyka ta jest bardzo ważna, gdyż technologie informacyjne i komunikacyjne (ICT) zostają włączone w strukturę naszej codziennej pracy i życia. Faktem jest znaczący wzrost ilości danych osobowych, biznesowych i rządowych przepływających przez Internet i między urządzeniami. Naraża to nas na coraz szerszy zakres zagrożeń cybernetycznych[6]. Jak więc rządy chronią siebie i swoich obywateli przed zagrożeniami cybernetycznymi?

---

[5] M. Nowikowska, *Zadania i obowiązki podmiotów wchodzących w skład systemu cyberbezpieczeństwa – zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)*, [w:] J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska *Retencja, migracja i przepływ danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019, s. 153.

[6] K. Chałubińska-Jentkiewicz, *Bezpieczeństwo telekomunikacyjne, jako element bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 70.

Globalny Indeks Cyberbezpieczeństwa ITU ocenia zakres reakcji rządowych i pomaga państwom dowiedzieć się, w jaki sposób mogą zwiększyć swoje zaangażowanie w cyberbezpieczeństwo. Pierwszy Indeks pojawił się w 2014 r. W badaniu wzięło udział 105 krajów. W 2017 r. ITU wydał drugą edycję Indeksu, w ramach której uczestniczyły 134 państwa. W 2018 r. rozpoczęła się trzecia edycja GCI. Globalny Indeks Cyberbezpieczeństwa analizuje w skali globu sposób, w jaki rządy państw zarządzają cyberryzykiem i adresują prawne oraz technologiczne aspekty cyberbezpieczeństwa.

Global Cybersecurity Index to zaufana referencja mierząca zaangażowanie państw w cyberbezpieczeństwo na poziomie globalnym – w celu zwiększenia świadomości znaczenia i różnych wymiarów problemu. Ponieważ cyberbezpieczeństwo ma szeroki zakres zastosowania, obejmujący wiele branż i różnych sektorów, poziom rozwoju lub zaangażowania każdego kraju ocenia się według pięciu filarów – (I) środki prawne; (II) środki techniczne; (III) środki organizacyjne; (IV) budowanie zdolności oraz (V) współpraca – a następnie łączone w ogólny wynik.

Indeks oparty zatem został na pięciu filarach:

– podstawy prawne – w tym ustawodawstwo, regulacja i ograniczenie ustawodawstwa dotyczącego spamu. Każde państwo jest zobowiązane do ustanowienia podstawowych mechanizmów reagowania, poprzez dochodzenie i ściganie przestępstw oraz nakładanie sankcji za nieprzestrzeganie prawa lub naruszenie prawa. Ramy prawne określają minimalne podstawy zachowania, na których można budować dalsze możliwości cyberbezpieczeństwa. Zasadniczo celem jest posiadanie wystarczającego ustawodawstwa w celu zharmonizowania praktyk na poziomie regionalnym oraz międzynarodowym i uproszczenia międzynarodowej walki z cyberprzestępczością. Kontekst prawny ocenia się na podstawie liczby

instytucji prawnych i ram prawnych dotyczących cyberbezpieczeństwa i cyberprzestępczości.

– zdolności operacyjne (techniczne) – technologia jest podstawą obrony przed zagrożeniami w cyberprzestrzeni, w tym wykorzystanie komputerowych zespołów reagowania na awarie lub incydenty[7], wdrażanie standardów, mechanizmów technicznych i możliwości wykorzystywanych w celu zwalczania spamu, ochrony dzieci w Internecie[8] itp. Bez odpowiednich umiejętności technicznych do wykrywania i reagowania na ataki cybernetyczne państwa pozostają podatne na zagrożenia. Efektywny rozwój i wykorzystanie ICT może naprawdę dobrze prosperować tylko w środowisku zaufania i bezpieczeństwa. W związku z tym państwa muszą zbudować i zainstalować zaakceptowane kryteria minimalnego bezpieczeństwa i systemy akredytacji dla aplikacji i systemów. Wysiłkom tym musi towarzyszyć utworzenie organu krajowego w celu reagowania na incydenty cybernetyczne, wiarygodnego podmiotu rządowego oraz krajowych ram monitorowania, ostrzegania i reagowania na incydenty. Elementy techniczne są oceniane na podstawie liczby praktycznych mechanizmów radzenia sobie z cyberbezpieczeństwem.
– środki organizacyjne – w tym strategie krajowe, odpowiedzialne agencje i wskaźniki bezpieczeństwa cybernetycznego, są niezbędne do prawidłowego wdrożenia każdej inicjatywy krajowej. Każde państwo powinno wyznaczyć ogólne cele strategiczne wraz z kompleksowym planem wdrożenia, dostawy i pomiaru. Agencje krajowe

[7] M. Nowikowska, op.cit., s. 156–158.

[8] K. Badźmirowska-Masłowska, *Małoletni użytkownik Internetu a zagrożenia bezpieczeństwa informacji,* [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 318.

muszą być obecne, aby wdrożyć strategię i ocenić wynik. Bez krajowej strategii, modelu zarządzania i organu nadzorczego, wysiłki w różnych sektorach stają się sprzeczne, co uniemożliwia starania o skuteczną harmonizację rozwoju cyberbezpieczeństwa. Struktury organizacyjne są oceniane na podstawie obecności instytucji i strategii obejmujących rozwój cyberbezpieczeństwa na poziomie krajowym[9].

– budowa wydolności państwa – w tym kampanie podnoszenia świadomości publicznej, ramy certyfikacji i akredytacji specjalistów ds. bezpieczeństwa cybernetycznego, profesjonalne szkolenia w zakresie bezpieczeństwa w cyberprzestrzeni, programy edukacyjne lub programy akademickie itp. Ww. elementy stanowią nieodłączny element trzech pierwszych filarów (prawnego, technicznego i organizacyjnego). Cyberbezpieczeństwo jest najczęściej rozpatrywane z technologicznego punktu widzenia, mimo że istnieje wiele implikacji społeczno-ekonomicznych i politycznych. Budowanie zdolności ludzkich i instytucjonalnych jest niezbędne do podnoszenia świadomości, wiedzy i *know-how* w różnych sektorach, do systematycznych i odpowiednich rozwiązań oraz do wspierania rozwoju wykwalifikowanych specjalistów. Budowanie zdolności ocenia się na podstawie liczby programów badawczo-rozwojowych, edukacyjnych i szkoleniowych oraz certyfikowanych specjalistów i agencji sektora publicznego.
– współpraca: cyberprzestępczość jest problemem globalnym i nie ogranicza się do granic krajowych ani po-

[9] F. Radoniewicz, *Wprowadzenie*, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019, s. 4.

działów sektorowych[10]. W związku z tym walka z cyberprzestępczością wymaga podejścia wielostronnego z udziałem wszystkich sektorów i dyscyplin (w tym umów dwustronnych i wielostronnych, udziału w forach, stowarzyszeniach międzynarodowych, partnerstwie publiczno-prywatnym, współpracy między agencjami, najlepsze praktyki itp.). Współpracę krajową i międzynarodową ocenia się na podstawie liczby partnerów, ram współpracy i sieci wymiany informacji[11].

Metoda dla GCI, w przypadku każdego z filarów, oceniana jest na podstawie ankiety internetowej opartej na pytaniach oraz zbieraniu dowodów potwierdzających. Wartość indeksu jest wyliczana z 25 subfilarów (przedstawionych na grafice poniżej) zawierających 50 binarnych (TAK, NIE) pytań. Pytania ankiety są ważone przez grupę ekspertów. Można zatem stwierdzić, że GCI jest złożonym indeksem łączącym 25 wskaźników w jedną miarę porównawczą w celu monitorowania i porównywania poziomu zobowiązań cyberbezpieczeństwa państw członkowskich ITU w odniesieniu do pięciu filarów. Motto badania brzmi: „GCI jest narzędziem budowania zdolności, aby wspierać kraje w poprawie ich krajowego bezpieczeństwa cybernetycznego". Wskaźniki zastosowane do obliczenia GCI zostały wybrane na podstawie następujących kryteriów:

– znaczenie dla pięciu filarów GCA (globalnej agendy bezpieczeństwa cybernetycznego) oraz w przyczynianiu się do głównych celów GCI i ram koncepcyjnych;

---

[10] J. Sobczak, *Cyberprzestrzeń jako obszar ochrony bezpieczeństwa narodowego w optyce dokumentów europejskich*, [w:] *Pozyskiwanie informacji w walce z terroryzmem*, red. P. Herbowski, D. Słapczyńska, D. Jagiełło, Warszawa 2017, s. 42.

[11] P. Milik, *Międzynarodowe uregulowania prawne w obszarze bezpieczeństwa w cyberprzestrzeni*, [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017, s. 115.

– dostępność i jakość danych;
– możliwość wzajemnej weryfikacji poprzez dane wtórne.

Ogólnymi celami GCI jest: pomoc państwom w zidentyfikowaniu obszarów wymagających poprawy, motywacja do poprawy rankingów GCI, podniesienie poziomu cyberbezpieczeństwa na całym świecie, pomoc w identyfikowaniu i promocja najlepszych praktyk, wspieranie globalnej kultury cyberbezpieczeństwa.

Badanie *Global Cybersecurity Index* oparte jest na sześciu fazach: (I) przygotowawczej, (II) początkowej, (III) gromadzenia danych, (IV) weryfikacyjnej (V) analizy, (VI) pisania i publikacji raportu.

Faza przygotowawcza polega na opracowaniu ankiety we współpracy z ekspertami i partnerami. Następuje w niej opracowanie internetowego systemu ankiet, jak również przygotowanie dokumentacji pomocniczej, takiej jak: przewodniki, ramy koncepcyjne, listy itp. Wszystkie dokumenty podlegają ogłoszeniu na stronie internetowej ITU.

Faza początkowa sprowadza się do poinformowania oraz zaproszenia państw członkowskich do badania. W fazie tej następuje także zbieranie danych punktów kontaktowych wyznaczonych przez administrację państw członkowskich. Ważną czynnością jest zapoznanie z programami ramowymi i zapewnienie dostępu do ankiety online wraz ze wszystkimi niezbędnymi dokumentami i instrukcjami, jak również wsparcie techniczne.

Faza gromadzenia danych polega na wypełnianiu kwestionariuszy przez państwa członkowskie.

Kolejną jest faza weryfikacji, która polega na zwrocie kwestionariuszy oraz ich weryfikacji przez specjalistów ITU.

Faza analizy sprowadza się do analizy wszystkich zebranych danych, a następnie przygotowanie rankingu, wykresów porównawczych, map, tabel i innych elementów statystycznych.

Ostatnią jest faza pisania i publikacji raportu, który jest publikowany na stronie internetowej ITU. W tej fazie następuje także oficjalne informowanie państw członkowskich o wynikach badania.

ITU wskazuje w jaki sposób można poprawić wynik i pozycję w rankingu GCI. Po pierwsze, należy zaangażować się w cyberbezpieczeństwo. Robić postępy we wszystkich pięciu filarach. Udostępniać wszystkie odpowiednie dane. Współpracować, jak również aktywnie uczestniczyć w GCI.

Według GCI Wielka Brytania znajduje się na szczycie listy państw najbardziej zaangażowanych w cyberbezpieczeństwo. Na kolejnych miejscach znalazły się Stany Zjednoczone, Francja, Litwa i Estonia, Singapur, Hiszpania, Malezja, Norwegia i Kanada.

Dane GCI pokazują znaczną poprawę cyberbezpieczeństwa na całym świecie. Więcej państw ma krajowe strategie bezpieczeństwa cybernetycznego, plany krajowe, zespoły reagowania i szczegółowe przepisy prawne w celu przeciwdziałania zagrożeniom w cyberprzestrzeni. Niestety między poszczególnymi regionami istnieje znaczna różnica. Ponadto istnieje wyraźna luka między wieloma państwami pod względem wiedzy na temat wdrażania przepisów dotyczących cyberprzestępczości, krajowych strategii bezpieczeństwa cybernetycznego (NCS), komputerowych zespołów reagowania kryzysowego (CERT), świadomości i zdolności do rozpowszechniania strategii oraz zdolności i programów w dziedzinie cyberbezpieczeństwa.

Oprócz rankingu najbardziej zaangażowanego państwa w cyberbezpieczeństwo, raport GCI zawiera również informacje na temat praktyk krajowych, które dają wgląd w osiągnięte postępy. Należy podkreślić, że gromadzenie danych GCI jest wielowymiarowe, nie ma jednego uniwersalnego rozwiązania dostosowanego do cyberbezpieczeństwa. Aby opracować GCI dane zebrane za pomocą ankiety internetowej są wykorzysty-

wane do odzwierciedlenia zaangażowania państw członkowskich w każdym filarze. Wartością dodaną raportu jest także tworzenie globalnej kultury cyberbezpieczeństwa. Inicjatywa ta zachęca państwa do zwiększenia zaangażowania w zakresie bezpieczeństwa w cyberprzestrzeni, podnoszenia świadomości w tej kwestii i umożliwienia większej współpracy na szczeblu krajowym, regionalnym i międzynarodowym.

Wydaje się, że badanie *Global Cybersecurity Index* ma unikalną wartość. Wynika to z faktu, iż GCI jest to zrównoważone połączenie szerokiego zasięg geograficznego, obejmujące wszystkie państwa członkowskie ITU. Badanie cyberbezpieczeństwa następuje w pięciu szerokich obszarach (filary globalnej agendy bezpieczeństwa cybernetycznego). Ponadto posiada mechanizmy oceny i rankingu, ukazując profile państw-uczestników.

Najważniejsze wnioski płynące z raportu:

1. Po pierwsze, ze względu na przyjęcie przez ITU różnej metodologii, porównywanie indeksu z lat 2014, 2017 i 2018 nie ma praktycznego znaczenia.
2. Analiza wyników raportu pokazuje poprawę i wzmocnienie wszystkich pięciu elementów agendy bezpieczeństwa cybernetycznego w różnych państwach we wszystkich regionach. Jest jednak miejsce na dalszą poprawę współpracy na wszystkich poziomach, budowanie zdolności i środki organizacyjne. Różnica w poziomie zaangażowania w cyberbezpieczeństwo między różnymi regionami jest nadal obecna i widoczna. Poziom rozwoju poszczególnych filarów różni się w poszczególnych państwach w regionach. Chociaż zaangażowanie w Europie pozostaje bardzo wysokie, szczególnie w zakresie prawa i techniki, trudna sytuacja w regionach Afryki i obu Ameryk wskazuje na potrzebę dalszego zaangażowania i wsparcie.
3. W raporcie w pierwszej dziesiątce znalazły się państwa ze wszystkich regionów: trzy z Azji i Pacyfiku, dwa z Euro-

py i obu Ameryk oraz jeden z Afryki i państw arabskich. Sugeruje to, że duże zaangażowanie nie jest ściśle związane z lokalizacją geograficzną.

4. W raporcie nie wykazano korelacji między rozwojem infrastruktury telekomunikacyjnej (ICT *for Development Index*) a indeksem cyberbezpieczeństwa. Wynika z tego, że inwestycje w technologie nie zawsze idą w parze z bezpieczeństwem systemów, zarządzaniem ryzykiem, propagowaniem świadomości cybernetycznej, tworzeniem procedur, polityk i strategii. Jako przykład można podać Danię oraz Niemcy, które znalazły się w pierwszej piętnastce indeksu ICT *Development Index*, a niebędące w grupie dwudziestu państw z najwyższym indeksem cyberbezpieczeństwa.
5. Bezpieczeństwo cybernetyczne jest niezbędne dla osób, firm, gospodarek, rządów i narodów jako całości. W rzeczywistości wszyscy starają się dotrzymać kroku najnowszym cyberatakom, ale niektóre państwa bardziej angażują się w cyberbezpieczeństwo. Wśród dziesięciu państw najlepiej przygotowanych do odparcia ataków cybernetycznych znalazły się USA. Stany Zjednoczone są jednym z państw, które każdego roku doświadczają ogromnej liczby cyberataków. Właśnie dlatego znajduje się tam około 58% firm zajmujących się cyberbezpieczeństwem i próbuje znaleźć nowe sposoby walki z najnowszymi atakami. Podobnie Estonia, dobrze znana z usług e-administracji i nauczyła się na podstawie swoich przeszłych doświadczeń w 2007 r., jak radzić sobie z wojnami cybernetycznymi[12].
6. Wysoka świadomość i organizacja cyberbezpieczeństwa państwa nie oznacza współmiernego rozwoju infrastruk-

[12] Ibidem, s. 122.

tury telekomunikacyjnej. Jak przykład wskazuje się Gruzję czy Egipt. Prawdopodobnie dysproporcja indeksowa dla tych państw wynika z ich wysokiego poczucia zagrożenia cybernetycznego.

7. Geograficzne zróżnicowanie indeksu jest dość widoczne. Półkula północna jest o wiele bardziej dojrzała w implementacji procesów cyberbezpieczeństwa. Wśród kontynentów najlepszy wynik osiąga Europa i Ameryka Północna. Bardzo niskie indeksy zanotowały państwa tradycyjnie niezaangażowane w politykę międzynarodową, np. San Marino, Watykan, Andora oraz małe państwa wyspiarskie na Pacyfiku.
8. Nie ma bezpośredniego związku między PKB na osobę w danym państwie a jego indeksem cyberbezpieczeństwa. Powszechnie wydaje się, że rozwój ekonomiczny niesie ze sobą wysokie standardy cyberbezpieczeństwa. Wyniki GCI nie potwierdzają tej tezy. Może wynikać to z faktu, że indeks cyberbezpieczeństwa nie mierzy jak funkcjonuje sektor prywatny i jaki jest poziom zaawansowania samych obywateli. Państwo z niskim indeksem cyberbezpieczeństwa może bardzo dobrze być zorganizowanym i silnym w cyberprzestrzeni pod warunkiem, że sektor prywatny przejmie rolę państwa w wielu płaszczyznach.
9. Państwa, które doświadczyły w przeszłości poważnych ataków na swoje systemy teleinformatyczne Gruzja, Estonia znajdują się obecnie w czołówce indeksu z bardzo dobrze rozwiniętymi instytucjami i prawem w obszarze cyberbezpieczeństwa[13].

[13] M. Kamiński, *Obrona Narodowa Republiki Estonii*, Warszawa 2018; idem, *System cyberbezpieczeństwa Republiki Estonii. Czy warto wzorować się na estońskich rozwiązaniach prawno-organizacyjnych*, [w:] *System bezpieczeństwa w cyberprzestrzeni RP*, red. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018.

10. Analiza danych zawartych w GCI pokazują znaczną poprawę cyberbezpieczeństwa na całym świecie. Więcej państw ma krajowe strategie bezpieczeństwa cybernetycznego, plany krajowe, zespoły reagowania i szczegółowe przepisy prawne w celu przeciwdziałania zagrożeniom. Niestety między poszczególnymi regionami istnieje znaczna różnica.
11. Istnieje wyraźna luka między wieloma państwami pod względem wiedzy na temat wdrażania przepisów dotyczących cyberprzestępczości, krajowych strategii bezpieczeństwa cybernetycznego (NCS), komputerowych zespołów reagowania kryzysowego (CERT), świadomości i zdolności do rozpowszechniania strategii oraz zdolności i programów w dziedzinie cyberbezpieczeństwa.
12. Państwa wg rezultatów podzielono na trzy grupy: początkujące, dojrzewające i przewodzące.

W fazie aktywnego gromadzenia danych w ramach GCI reakcje państw w regionach ITU były zróżnicowane. Spośród 44 państw członkowskich w regionie Afryki 29 odpowiedziało na ankietę. Spośród 38 państw członkowskich w regionie Azji i Pacyfiku 25 odpowiedziało na ankietę. Spośród 43 państw członkowskich w regionie Europy 34 odpowiedziało na ankietę.

Wśród trzech najwyżej uplasowanych państw w regionie Azji i Pacyfiku znalazły się Singapur, Malezja oraz Australia.

Singapur został najwyżej ocenionym krajem w regionie. Państwo wyspiarskie ma długą historię inicjatyw w zakresie cyberbezpieczeństwa. W 2005 r. Singapur uruchomił swój pierwszy plan generalny dotyczący bezpieczeństwa cybernetycznego. Singapurska Agencja ds. Bezpieczeństwa Cybernetycznego została utworzona w 2015 r. jako specjalny podmiot nadzorujący cyberbezpieczeństwo, a kraj wydał kompleksową strategię w 2016 r.

Malezja zajmuje drugie miejsce w regionie Azji i Pacyfiku oraz osiąga doskonałe wyniku w budowaniu zdolności dzięki

szeregowi inicjatyw w tym filarze. *Cybersecurity Malaysia*, jednostka rządowa odpowiedzialna za bezpieczeństwo informacji w tym kraju, oferuje profesjonalne szkolenia za pośrednictwem instytucji szkolnictwa wyższego w Malezji. Prowadzi stronę internetową *Cyberguru*, poświęconą profesjonalnym szkoleniom z zakresu bezpieczeństwa.

Australia zajmuje trzecie miejsce w regionie i jest domem dla AusCERT, jednego z najstarszych zespołów CERT w regionie utworzonego w 1993 r. W Australii i Nowej Zelandii pozytywnie oceniono m.in. procesy akredytacji, certyfikacji, edukacji i szkoleń w zakresie cyberbezpieczeństwa i bezpieczeństwa informacji dla osób fizycznych i korporacyjnych.

Szczegółowa analiza wyników według poszczególnych filarów wykazała dominującą rolę państw azjatyckich w obszarze szkolenia z zakresu cyberbzpieczeństwa. Jako przykład została wskazana Nowa Zelandia. Policja Nowej Zelandii (NZ) wprowadziła 3-poziomowy program szkoleniowy dla specjalistów od cyberprzestępczości, śledczych, a następnie personelu pierwszej linii. Zostało to przedstawione w pierwszej krajowej strategii zapobiegania cyberprzestępczości policji NZ na lata 2014–2017. Policja NZ zapewnia również szkolenia dla wymiaru sprawiedliwości i prokuratorów.

W filarze II – środki techniczne, obszar: ochrona dzieci w Internecie[14], wyróżniony został Singapur. Przyjęto w nim rozwiązania, zgodnie z którymi singapurscy dostawcy treści internetowych (ICP) i dostawcy usług dostępu do Internetu (IASP) zostali objęci licencją na podstawie ustawy o radiofonii

[14] Zob. P. Dubiel-Zielińska, P. Zieliński, *Cyberbezpieczeństwo a odpowiedzialność dzieci i młodzieży*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017, s. 49; U. Kazubowska, *Rodzina jako przestrzeń edukacji ku/dla bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni. Rzeczywistość i wyzwania*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017, s. 162.

i telewizji i zobowiązani do przestrzegania Kodeksu praktyk internetowych w celu ochrony dzieci w Internecie[15]. Od 2012 r. wszyscy usługodawcy zostali prawnie zobowiązani do oferowania usług filtrowania z subskrypcjami internetowymi oraz do informowania o tym konsumentów. Urząd ds. Rozwoju Mediów Informacyjnych również blokuje witryny pornograficzne, ekstremistyczne lub szerzące mowę nienawiści[16].

Wśród innych państw azjatyckich, których przyjęte rozwiązania zostały wskazane jako dobre praktyki znalazła się Korea, w filarze IV – budowa zdolności, obszar: narzędzia motywacyjne. W Korei została utworzona *Korea Internet Security Agency* (KISA), zobowiązana do stworzenia sieciowej podstawy dla użytkowników Internetu i firm internetowych poprzez poprawę konkurencyjności usług internetowych oraz niezawodności informacji i wiedzy w Internecie. KISA wspiera start-upy w komercjalizacji ich modeli biznesowych i zwiększaniu przewagi konkurencyjnej w dziedzinie technologii bezpieczeństwa, poprzez programy mające na celu wspieranie start-upów w branży Internetu rzeczy i bezpieczeństwa. Korea ustanowiła również kompleksową usługę wspierającą start-upy w zdobywaniu pozycji nie tylko na rynku krajowym, ale także na rynku globalnym w celu rozszerzenia ich modeli biznesowych.

Podsumowując przeprowadzone rozważania można stwierdzić, że cyberbezpieczeństwo jest dziś coraz ważniejszą częścią

---

[15] K. Nizioł, *Cyberbezpieczeństwo transakcji i płatności dokonywanych w Internecie przez małoletnich konsumentów*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017, s. 195.

[16] G. Krawiec, *Pornografia jako cyberzagrożenie w zakresie relacji międzyludzkich propozycja profilaktyki*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017, s. 206; L. Putyński, *Pornografia internetowa wśród dzieci i młodzieży – specyficzne i zagrażające uzależnieniem zjawisko*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, M. Górka, Warszawa 2017, s. 219.

naszego życia, a stopień wzajemnych połączeń sieci oznacza, że wszystko może zostać ujawnione, od krajowej infrastruktury krytycznej po nasze prywatne informacje, będąc zagrożeniem zarówno dla poszczególnych obywateli, jak i całych państw.

Mając na uwadze powyższe ITU poprzez swoje działania nawołuje rządy wszystkich państw do rozważenia polityk wspierających dalszy rozwój zaawansowania technologicznego, dostępu i bezpieczeństwa oraz jako kluczowy pierwszy krok do przyjęcia krajowej strategii bezpieczeństwa w cyberprzestrzeni. W edycjach *Global Cybersecurity Index* od 2014 r. mierzy się zaangażowanie państw członkowskich w bezpieczeństwo w cyberprzestrzeni, jak również podkreśla szereg przykładowych praktyk z całego świata. Pozytywnie należy ocenić fakt, że po pierwszej edycji GCI zrealizowanej w 2014 r. państwa członkowskie zmotywowały się do usprawnienia ich pracy związanej z cyberbezpieczeństwem. Działania ITU podnoszą także w państwach świadomość potrzeby rozpoczęcia współpracy dwustronnej, wielostronnej i międzynarodowej oraz zwiększają widoczność tego, co kraje robią, aby poprawić cyberbezpieczeństwo.

Bibliografia

Badźmirowska-Masłowska K., *Małoletni użytkownik Internetu a zagrożenia bezpieczeństwa informacji,* [w:] *Bezpieczeństwo informacyjne, Aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017.

Chałubińska-Jentkiewicz K., *Bezpieczeństwo telekomunikacyjne, jako element bezpieczeństwa informacyjnego*, [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017.

Dubiel-Zielińska P., Zieliński P., *Cyberbezpieczeństwo a odpowiedzialność dzieci i młodzieży*, [w:] *Cyberbezpieczeństwo*

dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa, red. M. Górka, Warszawa 2017.

Hołyst B., *Terroryzm*, Warszawa 2011.

Kamiński M., *Obrona Narodowa Republiki Estonii*, Warszawa 2018.

Kamiński M., *System cyberbezpieczeństwa Republiki Estonii. Czy warto wzorować się na estońskich rozwiązaniach prawno-organizacyjnych*, [w:] *System bezpieczeństwa w cyberprzestrzeni RP*, red. W. Kitler, K. Chałubińska-Jentkiewicz, K. Badźmirowska-Masłowska, Warszawa 2018.

Kazubowska U., *Rodzina jako przestrzeń edukacji ku/dla bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni. Rzeczywistość i wyzwania*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017.

Kitler W., *Pojęcie i zakres bezpieczeństwa informacyjnego państwa, ustalenia systemowe i definicyjne*, [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017.

Krawiec G., *Pornografia jako cyberzagrożenie w zakresie relacji międzyludzkich propozycja profilaktyki*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017.

Milczarek E., *Cyberbezpieczeństwo – wyzwanie XXI wieku*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017.

Milik P., *Międzynarodowe uregulowania prawne w obszarze bezpieczeństwa w cyberprzestrzeni*, [w:] *Bezpieczeństwo informacyjne: aspekty prawno-administracyjne*, red. W. Kitler, J. Taczkowska-Olszewska, Warszawa 2017.

Nizioł K., *Cyberbezpieczeństwo transakcji i płatności dokonywanych w Internecie przez małoletnich konsumentów*, [w:]

Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa, red. M. Górka, Warszawa 2017.

Nowikowska M., *Zadania i obowiązki podmiotów wchodzących w skład systemu cyberbezpieczeństwa – zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT)*, [w:] J. Taczkowska-Olszewska, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Retencja, migracja i przepływ danych w cyberprzestrzeni. Ochrona danych osobowych w systemie bezpieczeństwa państwa*, Warszawa 2019.

Putyński L., *Pornografia internetowa wśród dzieci i młodzieży – specyficzne i zagrażające uzależnieniem zjawisko*, [w:] *Cyberbezpieczeństwo dzieci i młodzieży. Realny i wirtualny problem polityki bezpieczeństwa*, red. M. Górka, Warszawa 2017.

Radoniewicz F., *Wprowadzenie*, [w:] *Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz*, red. W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz, Warszawa 2019.

Sobczak J., *Cyberprzestrzeń jako obszar ochrony bezpieczeństwa narodowego w optyce dokumentów europejskich*, [w:] *Pozyskiwanie informacji w walce z terroryzmem*, red. P. Herbowski, D. Słapczyńska, D. Jagiełło, Warszawa 2017.

Abstrakt

W artykule została omówiona problematyka *Światowego Indeksu Cyberbezpieczeństwa*, publikowanego przez Międzynarodowy Związek Telekomunikacyjny (ITU), który analizuje w skali globu sposób, w jaki rządy państw zarządzają cyberryzykiem i adresują prawne oraz technologiczne aspekty cyberbezpieczeństwa. Badanie oparte jest na pięciu filarach: podstawy prawne, zdolności, środki organizacyjne, budowa wydolności państwa, współpraca. Indeks powstał w 2014 r. w celu ułatwienia budowy globalnej kultury cyberbezpieczeństwa. Ocenia on wysiłki członków Międzynarodowego Związku Telekomunikacyjnego na rzecz poprawy cyberbezpieczeństwa. Metodologia tego badania polega na wysłaniu

pytań do członków ITU dotyczących wszystkich filarów. W artykule analizie poddane zostały wyniki trzech najwyżej uplasowanych państw w regionie Azji i Pacyfiku: Singapuru, Malezji oraz Australii.

Słowa kluczowe: cyberataki, cyberbezpieczeństwo, Globalny Indeks Cyberbezpieczeństwa, Międzynarodowy Związek Telekomunikacyjny, nowe technologie, wskaźnik bezpieczeństwa

Abstract

The article discusses the issues of the *Global Cybersecurity Index*, published by the International Telecommunications Union (ITU), which analyzes globally the way in which governments manage cyber-risk and address the legal and technological aspects of cyber security. The research is based on five pillars: legal bases, capabilities, organizational measures, building state efficiency, cooperation. The index was created in 2014 to facilitate the construction of a global cybersecurity culture. He assesses the efforts of the members of the International Telecommunications Union to improve cyber security. The methodology of this study is to send questions to ITU members regarding all pillars. The article analyzes the results of the three highest placed countries in the Asia-Pacific region: Singapore, Malaysia and Australia.

Keywords: cyber attack, cybersecurity, Global Cybersecurity Index, International Telecommunication Union, new technologies, security indicator

Katarzyna Badźmirowska-Masłowska
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0002-3551-2378

Cyberbezpieczeństwo Australii. Wybrane aspekty strategiczne

Wprowadzenie

Rozważania dotyczące strategicznych i prawnych aspektów cyberbezpieczeństwa Związku Australijskiego (*Commonwealth of Australia*), stanowiącego suwerenne państwo w ramach *Commonwealth realm,* połączonego unią personalną z Wielką Brytanią[1], osadzone są w *continuum* polityki prowadzonej przez Australię po II wojnie światowej. W następstwie rozpadu imperium brytyjskiego, dotychczasowego gwaranta bezpieczeństwa omawianego kontynentu, zwłaszcza w sferze wojskowej, kluczową pozycję w tym zakresie w obszarze Azji i Pacyfiku zajęły Stany Zjednoczone Ameryki Północnej (USA). Bipolarny podział świata[2], proces dekolonizacyjny, dyferencjacja ekonomiczna i ro-

[1] Kwestia uzyskania niepodległości przdez Australię nie jest jednoznacznie postrzegana w literaturze przedmiotu, począwszy od wskazywania daty 1 stycznia 1901 r. (Konstytucja Związku Australijskiego), po okres pomiędzy dwudziestoleciem międzywojennym a końcem II wojny światowej (w tym Statut Westminsterski, z 1931 r., mający cechy zarówno aktu prawa wewnętrznego, jak i umowy międzynarodowej, tworzący *Commonwealth of Nations*), a nawet *Australia Act(s)* z 1986 r. Por. np. S. Bożyk, *System konstytucyjny Australii*, Warszawa 2001; T. Wieciech, *Ustroje federalne Stanów Zjednoczonych, Kanady i Australii*, Kraków 2009.

[2] Por. np. K. Badźmirowska-Masłowska, *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej. Aspekty prawne i polityczne*, Warszawa 2013, s. 21–27 (i cytowana tam literatura).

snąca populacja państw Azji Południowo-Wschodniej[3], rodzące się obawy o niekontrolowaną, nielegalną, obcą kulturowo imigrację nie sprzyjały budowaniu relacji z państwami azjatyckimi, zwłaszcza z wskazywanego regionu[4]. Polityczno-wojskowy pakt ANZUS z 1951 r.[5] usytuował jego strony w strategicznych ramach przeciwdziałania rozprzestrzenianiu się komunizmu i zapewnianiu wzajemnego bezpieczeństwa w rejonie Oceanu Spokojnego. W okresie od lat 60. do 80. ubiegłego wieku polityka bezpieczeństwa Australii koncentrowała się na obszarze jej kontynentu, przedmiotowo odnosząc się przede wszystkim do obrony przed bezpośrednimi atakami militarnymi i uwzględniając w poszczególnych jej etapach przełożenie sytuacji geopolitycznej na jego poziom[6]. Dynamiczny rozwój ekonomiczny i postępujące procesy stabilizacji politycznej i demokratyzacji państw azjatyckich w późnych latach 80.[7] zapoczątkowały zaangażowanie Australii

[3] Por. np. K. Gawlikowski, *Azja Południowo-Wschodnia jako region historyczno-kulturowy* (I), „Azja-Pacyfik" 2002, t. V, s. 9–32.

[4] Por. np. A. Burke, *Fear of Security. Australia's Invasion Anxiety,* Cambridge 2010, DOI: https://doi.org/10.1017/CBO9780511720543; A. Jelonek, M.M. Ishaak, *Kwestie etniczne i aspiracje narodowe, a polityka budowy „zjednoczonego narodu Malezji",* „Azja-Pacyfik" 2002, nr 5, s. 33–50; R. Kamiński, *Wybrane aspekty polityki zagranicznej Australii u progu XXI wieku,* http://dx.doi.org/10.18778/7969-136-4.03 [dostęp: 12.08.2019]; szerzej: S. Firth, *Australia in International Politics: An Introduction to Australian Foreign Policy,* Sydney, 2011.

[5] Powołany 1 września 1951 r.; wszedł w życie 29 kwietnia 1952 r.; por. też traktat o strefie bezatomowej z Rarotonga z 11 grudnia 1986 r.

[6] Por. H. White, *'Four Decades of the Defence of Australia: Reflections on Australian Defence Policy over the Past 40 years'*, [w:] *History as Policy: Framing the debate on the future of Australia's Defence Policy*, red. R. Huisken, M. Thatcher, Canberra 2007, s. 163–171 (163–187), w szczególności doktryna *Forward Defence* (wysuniętej obrony).

[7] Por. np. T. Minh Tuan, *Polityka zagraniczna Wietnamu w okresie „odnowy" (doi moi): źródła i ewolucja,* „Azja-Pacyfik" 2002, nr 5, s. 51–62; J. Smulski, *Indonezja na przełomie XX i XXI w. od systemu autokratycznego ku semidemokracji*, „Azja-Pacyfik" 2005, nr 5, s. 80–88; szerzej por. R.P. Appelbaum, J. Henderson (red.), *States and Development in the Asian Pacific Rim*, London 1992; E.M. Kim (red.), *The four Asian tigers: Economic development and the global political economy*, San Diego 1998.

w instytucjonalizację bilateralnych i multilateralnych gospodarczych stosunków międzynarodowych w rejonie Azji i Pacyfiku[8]. I tak, już w opartym na deklaracjach politycznych układzie integracyjnym APEC (1989), stanowiącym forum ekonomiczne Azja – Pacyfik[9], na rzecz zrównoważonego rozwoju i budowy dynamicznej i harmonijnej społeczności regionu, podniesiono jako jeden z wiodących celów w liberalizacji handlu współpracę technologiczną. Forum Regionalne ASEAN (ARF, 1994), którego Australia była członkiem-założycielem, stanowi obecnie fundamentalną płaszczyznę spotkań w dziedzinie bezpieczeństwa, pomiędzy państwami Azji Południowej i Wschodniej a mocarstwami światowymi (Unia Europejska, USA, Rosja etc.)[10]. Najważniejszym zaś kompleksowym, wielostronnym porozumieniem o wolnym handlu łączącym rynki: australijsko-nowozelandzkie z ASEAN-em jest AANZFTA (2010)[11]. Australia jest też członkiem megaregionalnych stref: wolnego handlu, tj.: Regionalne Kompleksowe Partnerstwo Gospodarcze (RCEP, 2012)[12], Partnerstwo Transpacyficzne (TPP, 2015) oraz jego kontynuacja – Wszechstronne i Progresywne Porozumienie na rzecz Partner-

[8] R. Kamiński, op.cit., s. 29–33; H. White, *Four Decades of the Defence of Australia…*, op.cit., s. 171–176.

[9] https://www.apec.org/About-Us/About-APEC/Mission-Statement, https://www.apec.org/ [dostęp: 19.10.2019].

[10] http://aseanregionalforum.asean.org/about-arf/; http://aseanregionalforum.asean.org/; http://asean.pl/forum-regionalne-asean/ [dostęp: 19.10.2019].

[11] *Agreement establishing the ASEAN–Australia–New Zealand Free Trade Area (AANZFTA),* 27.02.2009, https://dfat.gov.au/trade/agreements/in-force/aanzfta/official-documents/Pages/agreement-establishing-the-asean-australia-new-zealand-free-trade-area-aanzfta.aspx; por. też: https://dfat.gov.au/trade/agreements/in-force/aanzfta/Pages/asean-australia-new-zealand-free-trade-agreement.aspx; https://aanzfta.asean.org/aanzfta-overview; https://aanzfta.asean.org/agreement-establishing-the-aanzfta [dostęp: 19.10.2019].

[12] K. Żołądkiewicz, *Wszechstronne Regionalne Partnerstwo Ekonomiczne (RCEP) jako przykład nowego trendu w regionalizmie,* „Finanse, Rynki, Finansowe, Ubezpieczenia" 2016, nr 3 (81), s. 335–344, https://www.msfaccess.org/spotlight-regional-comprehensive-economic-partnership-rcep [dostęp: 19.10.2019].

stwa Transpacyficznego (CPTPP, 2018 określane mianem TPP-11 lub TPP bez USA)[13]. Podejście Australii do kwestii bezpieczeństwa realizowane jest pod względem politycznym w ramach systemu euro-atlantyckiego[14], a w kwestii ekonomicznej zasadza się na dwu- i wielostronnych umowach wolnego handlu, a w szczególności integracji ekonomicznej w obszarze Azji i Pacyfiku[15].

Australia w wieku Azji[16]. Przesłanki polityki cyberbezpieczeństwa

W *Australia in the Asian Century: White Paper* (29.10.2012)[17],

[13] Umowę CPTPP ratyfikowano dotychczas w Australii, Kanadzie, Japonii, Meksyku, Nowej Zelandii, Wietnamie i Singapurze; ma ona charakter przyszłościowy, jeśli uwzględnić prawdopodobny akces UE, https://businessinsider.com.pl/finanse/makroekonomia/japonia-tworzy-nowy-lad-ekonomiczny-cptpp/tkjs35g [dostęp: 19.10.2019].

[14] Por. w tym kontekście, *Defending Australia Defence White Paper* 1994, https://www.defence.gov.au/Publications/wpaper1994.pdf; *Defence 2000: Our Future Defence Force* (2000 Defence White Paper, *nota bene,* por. też Białe Księgi Obronności z lat 1976, 1987, 1994, 2000 a następnie 2009 r.), https://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/pubs/rp/rp1516/DefendAust/2000 [dostęp: 19.10.2019]; H. White, *Four Decades of the Defence of Australia…*, op.cit., s. 176–184; idem, *Strategic Interests in Australian Defence Policy: Some Historical and Methodological Reflections,* „Security Challenges" 2008, vol. 4, nr 2, s. 63–79.

[15] Por. *Australia's free trade agreements* (FTAs), https://dfat.gov.au/trade/agreements/pages/trade-agreements.aspx [dostęp: 19.10.2019]. W ich ramach zawarto jedenaście umów wielostronnych, wskazywane już: ASEAN-Australia-New Zealand-AANZFTA, 2010 i Comprehensive and Progressive Agreement for Trans-Pacific Partnership-CPTPP, 2018.

[16] Przyjęto ówczesną perspektywę Australii, chociaż poddaje się w wątpliwość dominację państw azjatyckich, por. np.: S. Prokurat, *XXI wiek wiekiem Azji? (Tylko w pierwszej połowie XXI wieku. Technokapitalizm pomoże Zachodowi zdystansować gospodarczo Azję),* CSPA, 27.02.2017, http://www.polska-azja.pl/s-prokurat-xxi-wiek-wiekiem-azji-tylko-w-pierwszej-polowie-xxi-wieku-technokapitalizm-pomoze-zachodowi-zdystansowac-gospodarczo-azje/ [dostęp: 19.10.2019]. Co istotne, autor wskazuje na rozwój nowoczesnych technologii (technokapitalizm) jako czynnik, który pogrąży produkcję w Azji.

[17] *Australia in the Asian Century,* White Paper, październik 2012, https://www.eastasiaforum.org/wp-content/uploads/2014/04/australia-in-

dynamiczny rozwój państw kontynentu azjatyckiego, ujmowany jest w formule szans i wyzwań, jakie niesie on dla wzmocnienia siły australiskiego potencjału i prosperity kraju. Za strategiczne cele (*roadmap*) do 2025 r. przyjęto:

1. osiągnięcie prężnej i odpornej gospodarki – poprzez: a) podtrzymanie wysokiego poziomu wskaźników makrospołecznych i finansowych; b) koncentrację na edukacji, umiejętnościach, kwalifikacjach i nauce, podnoszących poziom kapitalu społecznego, otwartego na kulturę państw azjatyckich; c) wsparcie dla innowacyjnych rozwiązań w biznesie, zwiększających konkurencyjność podmiotów rynkowych i uwzględniające kontekst międzynarodowy (dywersyfikacja sektorowa), związany w szczególności z omawianym kontynentem oraz efektywny i uczciwy system podatkowy oraz skuteczne reformy, w tym regulacje prawne w dziedzinie przedsiębiorczości; d) systemowo-finansowe podejście instytucjonalno-infrastrukturalne, obejmujące zwłaszcza sektor prywatny, ale też podkreślające znaczenie rozwoju technologii informacyjno-komunikacyjnych (TIK) dla rozprzestrzeniania idei i wymiany handlowej, upowszechniania szerokopasmowego Internetu i pokonywania barier w dostępie do niego w omawianym regionie; e) ochronę środowiska[18];
2. budowanie potencjału (zdolności) pod kątem potrzeby profesjonalnego zaangażowania publicznych i prywatnych podmiotów krajowych na kontynencie azjatyckim poprzez: a) stosowne ukierunkowanie systemu edukacyjnego (szkolnictwo wszystkich szczebli, nauka, szkolenia,

the-asian-century-white-paper.pdf, s. 1–5; por. też: R. Kamiński, op.cit., s. 33–35; B. Mascitelli, G. Barry O'Mahony, *Australia in the Asian century – a critique of the white paper,* „Australian Journal of Regional Studies" 2014, vol. 20, nr 3, s. 540–566.

[18] *Australia in the Asian Century…*, op.cit., pkt 1–8.

ekspertyzy etc.); b) wzmacnianie współpracy pomiędzy władzami publicznymi Australii i państw azjatyckich; c) przystosowanie społeczności i regionów do zmian strukturalnych, także w zakresie rozwoju demokratycznego, opartego na liberalnych instytucjach i prawie, multikulturowego, spójnego społeczeństwa[19];

3. funkcjonowanie w ramach wzrastających rynków azjatyckich w obszarze biznesu, przedsiębiorczości, rolnictwa etc., sprzyjające otwartości i większej integralności ekonomicznej z Azją[20]. Poszukiwanie sukcesu ekonomicznego i podnoszenie kapitału społecznego, sprzyja innowacyjności oraz swobodnemu przepływowi inwestycji, technologii i wiedzy.

Natomiast dedykowane bezpieczeństwu są:

1. budowanie stabilnego, zrównoważonego, opartego na kooperacji bezpieczeństwa w regionie poprzez[21]: a) promowanie porozumień z kluczowymi państwami (Japonią, Indonezją, Indiami, Koreą Południową), wraz z uznaniem wiodącej w niniejszym zakresie roli sojuszu z USA i ich obecnością militarną i uwzględnieniem włączania Chin jako aktywnego uczestnika, zaangażowanego w przeciwdziałanie konfliktom[22]; b) podtrzymywanie kompleksowego, wielostronnego podejścia, realizowanego w ramach ONZ, G20, ukierunkowanego na zbu-

[19] Ibidem, pkt 9–16.

[20] Ibidem, pkt 17–19.

[21] Ibidem, pkt 20–21, s. 222–249.

[22] Por. B. Mascitelli, G. Barry O`Mahony, op.cit., s. 560–562. Por. w tym kontekście, umowy dwustronne: Nowa Zelandia–ANZCERTA 1983; Singapur–SAFTA 2003; USA–AUSFTA 2005; Tajlandia-TAFTA 2005; Chile–Acl-FTA 2009; Malezja–MAFTA 2013; Korea–KAFTA 2014 oraz, co szczególnie istotne z perspektywy bezpieczeństwa: Japonia–JAEPA 2015; Chiny–ChAFTA 2015. Nie weszły jeszcze w życie umowy z Hong Kongiem z 2018 r.; Indonezją z 2019 r. i Peru z 2018 r., *Australia's free trade agreements* (FTAs)…, op.cit.

dowanie bezpiecznego otoczenia międzynarodowego[23];
c) rozwój, ważnej z perspektywy społeczeństw, stabilności bazowych rynków (energii, żywności i wody) oraz

2. pogłębienie i poszerzenie relacji dyplomatycznych, biznesowych i więzi międzyludzkich, zdolnych do przezwyciężania różnic polityczno-ekonomicznych i pogłębiania związków kulturowych, na rzecz rozwoju potencjału i promocji interesów Australii na kontynencie azjatyckim[24].

Najważniejszym, uwidaczniającym wzmacniające i dostosowujące do wyzwań współczesnego środowiska międzynarodowego (*From a foundation of strength to a secure future*)[25], dokumentem w obszarze bezpieczeństwa Australii, jest jej pierwsza narodowa strategia z 23 stycznia 2013 r.: *Strong and Secure. A Strategy for Australia's National Security*[26]. Jej celem jest utworzenie jednolitego systemu bezpieczeństwa narodowego (militarnego i pozamilitarnego), antycypującego zagrożenia i ukierunkowanego na ochronę narodu i kształtowanie świata[27] zgodnie z interesami państwa, tj.: 1) ochrona

---

[23] Por. J. Stańczyk, *Środowisko bezpieczeństwa państwa w ujęciu międzynarodowym,* „Rocznik Bezpieczeństwa Międzynarodowego" 2018, vol. 12, nr 2, s. 15–22 (11–24). Australia jest członkiem największych organizacji miedzynarodowych, tj.: OECD, ONZ, WTO etc. i wielu specjalistycznych, https://en.wikipedia.org/wiki/Outline_of_Australia [dostęp: 19.10.2019]. Obecnie np. negocjowana jest umowa ramowa między Unią Europejską i jej państwami członkowskimi z jednej strony a Australią z drugiej, Dz.Urz. UE L237/7 15.09.2017.

[24] *Australia in the Asian Century…*, op.cit., pkt 22–25, s. 250–272.

[25] *Strong and Secure. A Strategy for Australia's National Security,* https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf, s. II [dostęp: 19.10.2019].

[26] Ibidem, s. II–III, 33–35; por. np.: I. Krawczyk, *Od silnych fundamentów ku bezpiecznej przyszłości – pierwsza Strategia Bezpieczeństwa Narodowego Australii,* „Bezpieczeństwo Narodowe" 2013, nr 28, s. 53–72; R. Kamiński, op.cit., s. 35–38.

[27] Por. w tym kontekście środowisko bezpieczeństwa państwa doby

i wzmacnianie suwerenności; 2) zapewnienie, aby ludność była bezpieczna i odporna/wytrzymała na istniejące zagrożenia; 3) zabezpieczenie aktywów (w tym kapitału), infrastruktury i instytucji oraz 4) promowanie sprzyjającego środowiska międzynarodowego. Za kluczowe zagrożenia uznano: 1) szpiegostwo i zagraniczne ingerencje, niestabilność rozwijających się i słabych[28] państw oraz konflikty mogące w znaczący sposób wpływać na interesy narodowe, co szerzej ma szczególne znaczenie w warunkach ogólnoświatowej niepewności politycznej i ekonomicznej; 2) proliferację broni masowego rażenia; 3) terroryzm i nacechowany przemocą ekstremizm oraz poważną, zorganizowaną przestępczość; osobno wyodrębniono ogólną ich kategorię określaną jako szkodliwa/wroga aktywność cybernetyczna[29].

Bezpieczeństwo, definiowane jako wolność od ataku, utrzymanie integralności terytorialnej i politycznej niezależności oraz ochrona podstawowych wolności i zdolności rozwojowych (społecznych, zasobów, infrastruktury i instytucji), osadzone jest w paradygmacie zapobiegania i zwalczania ryzyka i optymalnego wykorzystania szans[30]. Szerokiemu i dynamicznemu podejściu do niego odpowiadają, uwzględniające ocenę poszczególnych zagrożeń, jego filary, które można przedsta-

globalizacji, J. Stańczyk, *Środowisko bezpieczeństwa państwa…*, op.cit., s. 19–22.

[28] W ujęciu *fragile states,* w szerszym kontekście por. np. *Fragile states indexannual report 2019,* https://fundforpeace.org/wp-content/uploads/2019/04/9511904-fragilestatesindex.pdf [dostęp: 19.10.2019].

[29] *Every day, Australian governments, businesses and individuals face a range of cyber-related threats such as state-based and commercial espionage, identity theft, and denial and disruption of services. If left unchecked, cyber-related threats have the potential to undermine confidence in our social and economic stability and our prosperity, Strong and Secure. A Strategy for Australia`s National Security…,* op.cit., s. 11.

[30] Por. *Strong and Secure. A Strategy for Australia's National Security…*, op.cit., s. 9–12; I. Krawczyk, op.cit., s. 59–60.

wić w kategoriach: 1) negatywnych: a) przeciwdziałania terroryzmowi, szpiegostwu i ingerencji zewnętrznej; b) odstraszania i zwalczanie ataków na państwo i jego interesy (wraz z utrzymaniem integralności terytorialnej, w strategicznym sojuszu z USA)[31]; c) profilaktyki (zapobiegania), wykrywania i zakłócania poważnej, zorganizowanej przestępczości; 2) pozytywnych: a) promowania bezpiecznego, międzynarodowego środowiska na rzecz australijskich interesów oraz uzyskania wpływów w polityce światowej, zwłaszcza w regionie Azja – Pacyfik; b) wzmocnienia kapitału społecznego, zasobów, infrastruktury i instytucji[32].

W kontekście tytułowej tematyki szczególnego znaczenia nabiera filar dotyczący przestępczości zorganizowanej, w ramach którego podniesiono problem wykorzystywania w jej ramach nowych technologii, niestabilności światowej gospodarki, implikującej wzrost nielegalnych rynków oraz przemytu i handlu ludźmi, zachodzących zwłaszcza w państwach słabych. Odpowiedzią na niniejsze zagrożenia powinno być m.in. zbudowanie australijskiego systemu cyberobrony, mającego za zadanie przeciwdziałanie (zapobieganie i przede wszystkim zwalczanie) cyberprzestępczości[33]. Podkreślono też, że w ogólności impet rozwojowy technologii informacyjno-komunikacyjnych, określany niekiedy mianem rewolucji informacyjnej/informatycznej, a w szczególności ich upowszechnienie (*increasing online engagement*), implikuje nowy obszar wyzwań, związany zarówno

[31] R. Kamiński, op.cit., s. 36–38; por. też: J. Stańczyk, *Globalne stosunki sił 2017–2018,* „Rocznik Bezpieczeństwa Międzynarodowego" 2018, vol. 12, nr 2, s. 25–38.

[32] *Strong and Secure. A Strategy for Australia's National Security…*, op.cit., s. 60–66; por. zwłaszcza uwagi na temat pojęcia *resilience,* s. 61–62. Strategia miała być uaktualniana co 5 lat, por. np. S. Bashfield, *Australia Needs a New National Security Strategy,* https://thediplomat.com/2019/02/australia-needs-a-new-national-security-strategy/ [dostęp: 19.10.2019].

[33] (…) *Building Australia's cyber defences to become hostile to cyber crime*, ibidem, s. 34.

z pojawieniem się wirtualnej przestrzeni, jak i możliwością ich wykorzystywania w kształtowaniu pozostałych wymienionych w omawianej *Strategii* rodzajów zagrożeń (z uwzględnieniem ich globalnej współzależności i prywatyzowaniem, właściwych do tej pory sektorowi publicznemu podmiotów)[34]; w tym ujęciu można definiować rolę TIK w kontekście ich transsektorowości. Dlatego też zintegrowana polityka cyberprzestrzeni, wraz z operacjami wzmacniającymi obronę cyfrowych sieci, stała się jednym z trzech[35] priorytetów strategicznej perspektywy 5-letniej Australii; *notabene* w ramach jego realizacji Australia ratyfikowała Konwencję Rady Europy o cyberprzestępczości z dnia 23.11.2001 r. (30.11.2012 r., wejście w życie 1.03.2013 r.)[36].

Australijska strategia cyberbezpieczeństwa

Przedmiotowy zakres zagadnień, obejmowany strategią na rzecz bezpieczeństwa narodowego Australii, znajduje odzwierciedlenie w *Australia's Cyber Security Strategy – Enabling innovation, growth & prosperity* (26.04.2016 r., ACSS)[37]. W warunkach globalnej ekonomii, stałej wszechobecności, zwłaszcza mobilnych

[34] I. Krawczyk, op.cit., s. 65. Autorka zauważa, że: „Priorytet ten związany jest z rosnącym zagrożeniem bezpieczeństwa narodowego, związanym z rewolucją informatyczną. Cyberprzestrzeń stwarza możliwość nieprzyjaznej działalności zagranicznych służb wywiadowczych i organizacji przestępczych, ułatwia dalszą radykalizację i koordynację działań ekstremistów, może być wykorzystywana do szerzenia nienawiści i podziałów społecznych". Ibidem, s. 69–70.

[35] Obok zachęcania do regionalnego zaangażowania na rzecz bezpieczeństwa i efektywnego partnerstwa, ukierunkowanego na osiągnięcie innowacyjnych i skutecznych rezultatów w dziedzinie bezpieczeństwa narodowego, *Strong and Secure. A Strategy for Australia`s National Security…*, op.cit., s. 27.

[36] https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185 [dostęp: 19.10.2019].

[37] Wraz z: *Australia's Cyber Security Strategy at Glance,* https://cybersecuritystrategy.homeaffairs.gov.au/ [dostęp: 19.10.2019].

technologii cyfrowych, silne bezpieczeństwo w cyberprzestrzeni jest fundamentalnym czynnikiem wzrostu i prosperity kraju oraz ma żywotne znaczenie dla jego wymiaru narodowego, zwłaszcza w warunkach poszerzania się spektrum celów i zwiększającej się liczby incydentów w cyberprzestrzeni, których ofiarami padło w 2014 r. prawie milion Australijczyków[38], *ergo* wzrastających w skali ogólnej kosztów; ataki na *hardware i software* mają wyrafinowany, często nieuchwytny, niewidoczny, niepozostawiający śladów charakter. Dla przeciwdziałania zagrożeniom, za istotną z perspektywy wspólnotowej, uznano potrzebę współdziałania w sferze cyberbezpieczeństwa wszystkich podmiotów, począwszy od rządu, przez interesariuszy, po pojedyncze jednostki, czyniąc je wszystkie odpowiedzialnymi za uczynienie Australii, najbezpieczniejszym miejscem łączenia się *online*; oparte na badaniach problemów, rozwiązania, wypracowywane są z udziałem środowiska naukowego, ekspertów, przedstawicieli organów ścigania i wymiaru sprawiedliwości etc.[39]

Strategia koncentruje się na pięciu priorytetach, uwzględniających ww. przesłanki[40]. Pierwszym z nich jest narodowe partnerstwo publiczno-prywatne, polegające na ustanowieniu strategicznej agendy, corocznych spotkań rządu z liderami biznesu i środowiska naukowego, na rzecz usprawnienia zarządzania przedmiotowym obszarem, w tym ustalenia kosztów szkodliwej działalności w cyberprzestrzeni, dla australijskiej ekonomii ogółem i poszczególnych podmiotów, wraz z zapew-

[38] *Over 9,500 cyber crimes were reported to the Australian Cybercrime Online Reporting Network in its first three months of operation. The Australian Signals Directorate responded to 37% more government cyber security incidents in 2014 compared to previous years, op.cit., Australia's Cyber Security Strategy…*, op.cit., s. 16 (13–20).

[39] Można to ująć w następujący sposób: *A strategy to secure our prosperity in a connected world*, ibidem, s. 5, 20.

[40] Do każdego z priorytetów dołączono plan działań.

nieniem stosownego systemu informacyjnego dostępnego na szczeblu lokalnym[41]. Podnosi się tu problematykę instytucjonalizacji niniejszych zagadnień, poprzez stworzenie rządowej architektury cyberbezpieczeństwa; zagadnienia polityczne usytuowane są w obszarze uprawnień premiera (specjalny doradca), aspekty międzynarodowego zaangażowania w Ministerstwie Spraw Zagranicznych i Handlu a operacyjne i koordynacyjne w resorcie obrony[42]. Ważną kwestią jest też wzmocnienie czołowego, w niniejszym zakresie, organu, jakim jest Australijskie Centrum Bezpieczeństwa Cybernetycznego (*the Australian Cyber Security Centre*)[43]. Nieustannie monitoruje ono cyberzagrożenia (24 godziny na dobę, 7 dni w tygodniu), informuje i przekazuje porady, podmiotom indywidualnym, biznesowym, organizacjom pozarządowym, środowisku akademickiemu, operatorom infrastruktury krytycznej, władzom krajowym, federalnym i lokalnym etc. Integrujące współdziałanie sektorów publicznego i prywatnego w dzieleniu się informacjami i wiedzą, rola Centrum (*hub*) ukierunkowana jest na zapobieganie oraz zwalczanie zagrożeń i minimalizowanie szkód, wynikających przede wszystkim z cyberprzestępczości;

---

[41] Ibidem, s. 6, 21–25, 58. *More strategic discussions between public and private sector leaders will focus on practical outcomes and elevate cyber security, both as a business risk and as a strategic opportunity rather than just as an operational matter*, ibidem, s. 22.

[42] Ibidem, s. 24–25.

[43] Por. w kontekście ACSC: 1) *the Australian Signals Directorate* (ASD) [which] *is a vital member of Australia's national security community, working across the full spectrum of operations required of contemporary signals intelligence and security agencies: intelligence, cyber security and offensive operations in support of the Australian Government and Australian Defence Forces (ADF)* (od 1 lipca 2018 r. ACSC stała się formalnie częścią ASD), https://www.asd.gov.au/about [dostęp: 19.10.2019]; 2) *Defence Intelligence Organisation,* https://www.defence.gov.au/dio/index.shtml [dostęp: 19.10.2019]; 3) *Computer Emergency Response Team – AUSCERT,* https://www.auscert.org.au/ [dostęp: 19.10.2019] oraz *Australian Federal Police, Australian Crime Commission* i *Australian Criminal Intelligence Commission*. Zagadnienia instytucjonalne wymagają odrębnego opracowania.

zdolności rządowe wpływają pozytywnie na uodpornienie społeczeństwa i wspierają ekonomiczny dobrobyt ery cyfrowej[44].

Silna cyberobrona oparta jest na przygotowaniu ofensywnych i defensywnych rozwiązań, uodparniających australijski system sieciowy na ataki poprzez ich wykrywanie, powstrzymywanie i reakcję, w ramach wymiany w czasie rzeczywistym informacji posiadanych przez sektor rządowy i prywatny[45], zwłaszcza uczestniczący w usługach infrastruktury krytycznej, wspomagany w szczególności przez australijski CERT. Zwiększenie wydolności w zwalczaniu cyberprzestępczości łączy się z podnoszeniem potencjału w sferze organów ścigania i wymiaru sprawiedliwości (*Australian Crime Commission, Australian Federal Police*). Niezbędna świadomość ryzyka i sposobów mierzenia się z nim implikuje przygotowanie – uwzględniających standardy międzynarodowe i funkcjonujących na zasadzie dobrowolności – wytycznych (*co-design*), promujących wprowadzanie przez poszczególne podmioty inicjatyw samoregulacyjnych, w tym tzw. dobrych praktyk[46].

Australia przyjmuje podejście globalnej odpowiedzialności, w ekonomicznym i aksjologicznym paradygmacie szanse – ryzyko; uczestniczy w międzynarodowej współpracy na rzecz otwartego, wolnego i bezpiecznego Internetu, zarządzanego

---

[44] https://www.cyber.gov.au/; https://www.cyber.gov.au/about; https://www.asd.gov.au/cyber [dostęp: 19.10.2019]; por. też: Joint Cyber Security Centre (JCSC) program, https://www.cyber.gov.au/programs/joint-cyber-security-centres [dostęp: 19.10.2019].

[45] Por. instytucjonalno-programowy, model warstwowy obejmujący: *Astralian Cyber Security Centre, Joint Cyber Threat Centres, online cyber threat sharing portal, Australia' s Cyber Security Strategy*…, op.cit., s. 32–33.

[46] Ibidem, s. 6–7, 27–36, 59–63. W niniejszy proces włączają się też: ASD, *the Australian Media and Communications Authority*, https://www.acma.gov.au/; *Council of Registered Ethical Security Testers (CREST) Australia New Zealand,* https://www.crest-approved.org/ [dostęp: 19.10.2019]; por. też w tym kontekście: *Defence White Paper 2016*, https://www.defence.gov.au/WhitePaper/Docs/2016-Defence-White-Paper.pdf [dostęp: 19.10.2019].

wedle wielostronnego modelu partnerskiego, na równych zasadach traktującego sektor rządowy, prywatny i wspólnotowy. Celom tym służy wyznaczenie ambasadora cyberbezpieczeństwa, zapewniającego w praktyce skoordynowaną, spójną i ukierunkowaną na uzyskiwanie wpływu i pozycji światowego gospodarczego, lidera, współpracę zwłaszcza poprzez wspieranie właściwego stosowania, przewidzianych dla cyberprzestrzeni, norm prawa międzynarodowego i redykcji ryzyka konfilktów[47]. Z uwagi na fakt, że źródła pochodzenia większości czynów kryminalnych są pozakrajowe, niezbędne jest współdziałanie na poziomie międzynarodowym z organami ścigania i wymiaru sprawiedliwości, agencjami wywiadowczymi i innymi komputerowymi zespołami szybkiego reagowania, zwłaszcza w kwestiach powstrzymywania cyberataków oraz śledzenia ich sprawców. Z jednej strony zapobieganie i ograniczanie – z perspektywy sprawców przestępstw i innych szkodliwych graczy – bezpiecznych przestrzeni, a szerzej przeciwdziałanie cybewrprzestępczości, z drugiej wyrównywanie cyfrowych i ekonomicznych poziomów różnych państw, wymaga także wspomagania rozwoju zdolności partnerów z obszaru Indo-Pacyfiku, *ergo* strategicznego cyberzaangażowania Australii na szczeblu bilateralnym i regionalnym[48].

Priorytet, dotyczący wzrostu i innowacji, ujmuje Internet jako szerokie narzędzie zróżnicowania i rozwoju (R&D), nowych inwestycji i możliwości rynkowych w wymiarze regionalnym (Azja-Pacyfik) i globalnym, a w ogólności zwiększenia przekonania do australijskiego biznesu online i zapewnienia mu prosperity. Implikuje to też rządowe wsparcie dla usług i badań w obszarze cyberbezpieczeństwa, odpowiadających wyzwaniom przemysłu i potrzebom władz publicznych, ukierunkowanych

[47] *Australia's Cyber Security Strategy...*, op.cit., s. 7, 39–44, 63.

[48] Ibidem, s. 39–43. W 2014 r. Australia otworzyła *formal multi-agency cyber policy dialogues* z Chinami, Indiami, Koreą Południową i Japonią.

na konkurencyjne w skali światowej rozwiązania. Australia pozycjonuje się jako centrum innowacji w omawianym zakresie, realizujące poprzez *Cyber Security Growth Centre* (*AustCyber*) wysoki poziom bezpieczeństwa w cyberprzestrzeni. Ma ono na celu usprawnienie: zaangażowania pomiędzy badaniami a biznesem, zarządzania i umiejętności siły roboczej (zatrudnionych), dostępu do rynków międzynarodowych oraz przyjęcie reform regulacyjnych[49].

Prezentowane w niniejszej strategii podejścia łączą się z ostatnim z priorytetów, kładącym nacisk na zwiększanie umiejętności i zdolności ludzkich (*a cyber smart nation*), stanowiących warunek urzeczywistnienia przyjętych w niej zobowiązań. Podtrzymanie sukcesu zależy od przełamania krytycznych niedoborów kadrowych, poprzez stworzenie systemu edukacyjnego i naukowego, sprzyjającego przygotowaniu wykwalifikowanych osób, profesjonalistów cyberbezpieczeństwa, rekrutujących się z różnych dziedzin (zwłaszcza nauk inżynieryjno-technicznych, ale też społecznych, w tym prawnych)[50]. Ponadto społeczeństwo powinno być świadome ryzyka i szans online oraz możliwych do zastosowania regulacyjnych i alternatywnych metod ochrony, czemu służyć mają publiczno-prywatne inicjatywy i kampanie edukacyjne[51].

---

[49] *Australia's cyber Security Strategy*..., op.cit., s. 8–9, 45–49, 64. Por. też np.: https://www.industry.gov.au/data-and-publications/industry-growth-centres-initiative-progress-and-impact/growth-centre-achievements/cyber-security-growth-centre-austcyber (*The CCGC was announced in December 2015 as part of the Government's National Innovation and Science Agenda*); *Australian Cyber Security Growth Network*), *The Commonwealth Scientific and Industrial research Organisation (CSIRO),* https://www.austcyber.com/; https://www.csiro.au/ [dostęp: 19.10.2019].

[50] *The most urgent need is for highly-skilled cyber security professionals. Academic centres of excellence will enhance the quality of cyber security courses, teachers and professionals in Australia, Australia's cyber Security Strategy*..., op.cit., s. 53.

[51] Ibidem, s. 9, 51–55, 65.

W tytułowym kontekście szczególnego znaczenia nabiera też dokument o wymiarze ponadkrajowym, wskazujący na strategiczną rolę „cyberspraw" dla relacji międzynarodowych: *Australia's International Cyber Engagement Strategy* (4.10.2017, AICES)[52]. Jako światowy lider otwartej, wolnej i bezpiecznej cyberprzestrzeni, maksymalizujący, wpisane w nią szanse, dla rozwoju ekonomicznego (zwłaszcza handlu cyfrowego) i prosperity, Australia ukierunkowuje swoją politykę na redukcję ryzyka, a zarazem na promowanie pokoju i stabilności cyberprzestrzeni; przyjmuje wielostronny model zarządzania Internetem, oparty na poszanowaniu praw człowieka, zasadach demokratycznych i popieraniu dobrych praktyk w zakresie cyberbezpieczeństwa. Współpraca międzynarodowa i kreatywne partnerstwo przełamuje trudności w przeciwdziałaniu (zapobieganiu i zwalczaniu) szeroko rozumianym, wykraczającym poza granicę państw, *ergo* ich jurysdykcji, cyberzagrożeń. Postępująca złożoność środowiska międzynarodowego implikuje zwiększanie liczby graczy, realizujących strategiczne cele domeny cyfrowej, co wymaga zastosowania międzynarodowych regulacji prawnych w cyberprzestrzeni, kompleksowości i skoordynowanego podejścia[53]. W praktycznym aspekcie AICES obejmuje szerokie spektrum zagadnień, ukierunkowanych na następujące cele[54]:

1. maksymalizację handlu cyfrowego – poprzez ukształtowanie właściwego środowiska, harmonizację standardów, zawieranie umów handlowych, podejmowanie inwestycji

---

[52] *Australia's International Cyber Engagement Strategy*, https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html; https://australiansecuritymagazine.com.au/australias-international-cyber-engagement-strategy-launched/ [dostęp: 19.10.2019].

[53] Ibidem, s. 10–11, 82–88.

[54] Ibidem, s. 8–9.

oraz wdrażanie środków ułatwiających jego prowadzenie[55];

2. wzmacnianie cyberbezpieczeństwa – na poziomie wewnętrznym, poprzez partnerskie relacje globalne i podnoszące stosowne zdolności w regionie Indo-Pacyfiku oraz rozprzestrzenianie innowacyjnych rozwiązań i promowanie australisjkiego przemysłu[56];
3. przeciwdziałanie cyberprzestępczości – poprzez zapobieganie jej, zwalczanie przez organy ścigania i wymiaru sprawiedliwości, z położeniem nacisku na region Indo-Pacyfiku, w którym niezbędna jest też pomoc w podniesieniu świadomości niniejszej problematyki oraz wzmocnieniu regulacji prawnych i struktury instytucjonalnej; ponadto istotny jest dialog dyplomatyczny i międzynarodowa wymiana informacji[57];
4. ukształtowanie międzynarodowego, stabilnego i pokojowego środowiska cyberprzestrzeni – poprzez ustanowienie jasnych oczekiwań względem zachowań państw, powstrzymywanie i reagowanie na nieakceptowane ich rodzaje oraz implementowanie praktycznych środków zapobiegania konfliktom[58];
5. przyjęcie wielostronnego, kooperatywnego, inkluzywnego, opartego na konsensusie, transparentnego i odpowiedzialnego podejścia do zarządzania otwartym, wolnym, niezależnym od rządowej kontroli i bezpiecznym Internetem oraz upowszechnienie go w regionie Indo-Pacyfiku[59];
6. promowanie i zastosowanie standardów praw człowieka i zasad demokratycznych w sferze online analogicznie do

[55] Ibidem, s. 12–21.
[56] Ibidem, s. 22–31.
[57] Ibidem, s. 32–43.
[58] Ibidem, s. 44–55.
[59] Ibidem, s. 56–63.

ich wymiaru offline oraz zapewnienie ich poszanowania i ochrony we wszystkich australijskich projektach, łączących się technologią cyfrową[60];

7. wykorzystanie technologii na rzecz zrównoważonego rozwoju oraz inkluzywnego wzrostu ekonomicznego w regionie Indo-Pacyfiku, w interesie którego należy też prowadzić szeroką współpracę (z organizacjami międzynarodowymi, regionalnymi rządami i sektorem prywatnym), ukierunkowaną na ulepszenie zdolności przyłączeniowych i dostępu do Internetu oraz w rządzeniu, cyfrowym dostarczaniu usług, przedsiębiorczości, integracji na globalnym rynku i kształtowaniu umiejętności cyfrowych[61].

Strategie dotyczące cyberbezpieczeństwa Australii są dokumentami nowymi, pochodzącymi z lat 2016–2017, wyznaczającymi kierunki polityki związanej z cyberprzestrzenią. Powstające raporty wskazują na rysujące się wyzwania, stojące przed realizacją ich założeń; dlatego wymagają one zasygnalizowania.

Wyzwania dla cyberbezpieczeństwa Australii

W raporcie *Australia's Cyber Security Strategy. Enabling innovation, growth & prosperity,* First Annual Update, 2017[62] podniesiono, że pierwszy rok realizacji strategii przynosi perspektywę usprawnienia bezpieczeństwa w środowisku online, także w zakresie innowacji, wzrostu ekonomicznego i prosperity, które to obszary, w coraz większym stopniu postrzega się właśnie przez pryzmat uzyskania globalnej konkurencyjności w cyber-

[60] Ibidem, s. 64–69.

[61] Ibidem, s. 70–81.

[62] https://cybersecuritystrategy.homeaffairs.gov.au/Documents/cybersecurity-strategy-first-annual-update-2017.pdf, s. 6–28 [dostęp: 19.10.2019].

przestrzeni. Co więcej, wygenerowała ona platformę partnerskich, bardziej bezpośrednich i pogłębionych rozmów między rządami, biznesem (w tym pełniącym centralną rolę zwłaszcza w zakresie infrastruktury, prywatnym sektorem), środowiskiem naukowo-badawczym i społeczeństwem, dla którego przygotowano podstawy pod realizację celu *cyber smart nation*; nastąpiło wzmocnienie instytucjonalne ACSS. Upowszechnił się paradygmat równoważący szanse i ryzyko, w ramach którego incydenty mogą być traktowane jako okoliczność sprzyjająca uczeniu się. W perspektywie międzynarodowej za istotny krok uznano przyjęcie AICES.

Analizując *the 2019 Progress Report sets out Australia's achievements under each of the 61 actions highlighted in the inaugural International Cyber Engagement Strategy*[63] należy podkreślić wielość praktycznych działań podejmowanych dla realizacji celów, przewidzianych w AICES. W szczególności, odnośnie handlu cyfrowego można przykładowo wymienić kształtujące środowisko cyfrowe: wejście w życie *Comprehensive and Progressive Trans-Pacific Partnership* (CPTPP), podjęcie inicjatywy WTO *E-commerce*; ponadto inne na forum APEC, OECD, G20 oraz promujące australisjki handel i inwestycje cyfrowe. W zakresie cyberbezpieczeństwa prowadzono działania regionalne (Indo-Pacyfik) oraz globalne, dotyczące m.in. wspierania międzynarodowych standardów i promowania australijskiego przemysłu w niniejszym obszarze. Współpraca międzynarodowa opierała się zwłaszcza na programach i kursach ukierunkowanych na ustanowienie jasnych oczekiwań względem zachowań państw w cyberprzestrzeni, reakcje na nieakceptowalne z nich i przeciwdziałania konfliktom. W wielostronnym podejściu do zarządzania In-

[63] https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/2019_progress_report.html [dostęp: 19.10.2019].

ternetem uściślono m.in. kryteria uczciwej i efektywnej konkurencji, a promocja aplikacji praw człowieka i zasad demokracji w cyberprzestrzeni odbywała się w formie krajowych i międzynarodowych konferencji i sporządzenia wytycznych do ich przyjmowania online; podobnie w ramach organizacji dedykowanych poszczególnym obszarom technologicznym (np. *Transport Network Strategic Investment Tool, TraNSIT*), w tym nowym zagadnieniom, tj. np. blockchain.

Podsumowując prezentowany w niniejszym opracowaniu przegląd zagadnień strategicznych związanych z cyberbezpieczeństwem Australii można wysnuć wnioski ogólniejszej natury. Problematyka niniejsza jest nowa i wymaga pogłębionych badań i analiz. W szczególności odrębnemu opracowaniu powinny podlegać zagadnienia prawno-instytucjonalne, zwłaszcza związane ze współpracą w przeciwdziałaniu cyberprzestępczości w regionie Indo-Pacyfiku. Inicjatywy legislacyjne, tj. uczestnictwo w negocjacjach dodatkowego protokołu do budapesztańskiej konwencji o cyberprzestępczości powinny być uzupełniane alternatywnymi metodami, związanymi zwłaszcza z uświadamianiem społeczeństwa w zakresie ochrony przed cyberzagrożeniami, w tym przestępstwami (programy, warsztaty etc.); *last but not least,* niezbędny jest też dialog dyplomatyczny i międzynarodowa wymiana informacji dotycząca cyberprzestępczości[64].

[64] Australia ma szerokie doświadczenie w zwalczaniu cyberprzestępczości, podobnie jak i w badaniu jej kryminologicznych aspektów, por. np. *McAfee Virtual Criminology Report Cybercrime Versus Cyberlaw. The annual McAfee global study on organized crime and the Internet in collaboration with leading international security experts,* https://www.ifap.ru/pr/2008/n081212b.pdf [dostęp: 19.10.2019]; R. Brewer, J. Cale, A. Goldsmith, T. Holt, *Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents*, „International Journal of Cyber Criminology", styczeń–czerwiec 2018, vol 12 nr 1, s. 115–132.

Bibliografia

Badźmirowska-Masłowska K., *Wspólna polityka zagraniczna i bezpieczeństwa Unii Europejskiej. Aspekty prawne i polityczne*, Warszawa 2013.

Brewer R., Cale J., Goldsmith A., Holt T., *Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents*, „International Journal of Cyber Criminology", styczeń–czerwiec 2018, vol 12, nr 1.

Burke A., *Fear of Security. Australia`s Invasion Anxiety,* Cambridge 2010.

Bożyk S., *System konstytucyjny Australii*, Warszawa, 2001.

Firth S., *Australia in International Politics: An Introduction to Australian Foreign Policy,* Sydney 2011.

Gawlikowski K., *Azja Południowo-Wschodnia jako region historyczno-kulturowy* (I) „Azja Pacyfik" 2002, t. V.

Jelonek A., Ishaak M.M., *Kwestie etniczne i aspiracje narodowe, a polityka budowy „zjednoczonego narodu Malezji"*, „Azja-Pacyfik" 2002, t. V.

Kamiński R., *Wybrane aspekty polityki zagranicznej Australii u progu XXI wieku,* http://dx.doi.org/10.18778/7969-136-4.03.

Mascitelli B., Barry O`Mahony G., *Australia in the Asian century – a critique of the white paper,* „Australian Journal of Regional Studies" 2014, vol. 20, nr 3.

McAfee Virtual Criminology Report Cybercrime Versus Cyberlaw. The annual McAfee global study on organized crime and the Internet in collaboration with leading international security experts, https://www.ifap.ru/pr/2008/n081212b.pdf.

Minh Tuan T., *Polityka zagraniczna Wietnamu w okresie „odnowy" (doi moi): źródła i ewolucja,* „Azja-Pacyfik" 2002, nr 5.

Smulski J., *Indonezja na przełomie XX i XXI w. od systemu autokratycznego ku semidemokracji*, Toruń 2002.

Stańczyk J., *Globalne stosunki sił 2017–2018,* „Rocznik Bezpieczeństwa Międzynarodowego" 2018, vol. 12, nr 2.
Stańczyk J., *Środowisko bezpieczeństwa państwa w ujęciu międzynarodowym,* „Rocznik Bezpieczeństwa Międzynarodowego" 2018, vol. 12, nr 2.
Appelbaum R.P., Henderson J. (red.), *States and Development in the Asian Pacific Rim*, London 1992.
Kim E.M. (red.), *The four Asian tigers: Economic development and the global political economy*, San Diego 1998.
White H., *'Four Decades of the Defence of Australia: Reflections on Australian Defence Policy over the Past 40 years'*, [w:] *History as Policy: Framing the debate on the future of Australia's Defence Policy*, red. R. Huisken, M. Thatcher, Canberra 2007.
White H., *Strategic Interests in Australian Defence Policy: Some Historical and Methodological Reflections,* „Security Challenges" 2008, vol. 4, nr 2.
Wieciech T., *Ustroje federalne Stanów Zjednoczonych, Kanady i Australii*, Kraków 2009
Żołądkiewicz K., *Wszechstronne Regionalne Partnerstwo Ekonomiczne (RCE P) jako przykład nowego trendu w regionalizmie,* „Finanse, Rynki, Finansowe, Ubezpieczenia" 2016, nr 3 (81).

Źródła internetowe

Australia

https://www.acma.gov.au/.
https://www.asd.gov.au/about.
https://www.auscert.org.au/.
https://www.austcyber.com/.
https://www.crest-approved.org/.
https://www.csiro.au/.
https://www.cyber.gov.au/.
https://www.cyber.gov.au/about.

https://www.cyber.gov.au/programs/joint-cyber-security-centres.
https://cybersecuritystrategy.homeaffairs.gov.au/
https://cybersecuritystrategy.homeaffairs.gov.au/Documents/cyber-security-strategy-first-annual-update-2017.pdf.
https://www.defence.gov.au/dio/index.shtml.
https://www.defence.gov.au/WhitePaper/Docs/2016-Defence--White-Paper.pdf.
https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/index.html.
https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/chapters/2019_progress_report.html.
https://www.industry.gov.au/data-and-publications/industry-growth-centres-initiative-progress-and-impact/growth-centre-achievements/cyber-security-growth-centre-austcyber.

Organizacje międzynarodowe

https://aanzfta.asean.org/aanzfta-overview.
https://aanzfta.asean.org/agreement-establishing-the-aanzfta.
https://www.apec.org/About-Us/About-APEC/Mission-Statement.
https://www.apec.org/.
http://aseanregionalforum.asean.org/about-arf/.
http://aseanregionalforum.asean.org/.
http://asean.pl/forum-regionalne-asean/.
https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185.
https://dfat.gov.au/trade/agreements/pages/trade-agreements.aspx.
https://dfat.gov.au/trade/agreements/in-force/aanzfta/official-documents/Pages/agreement-establishing-the-asean--australia-new-zealand-free-trade-area-aanzfta.aspx.

https://www.eastasiaforum.org/wp-content/uploads/2014/04/australia-in-the-asian-century-white-paper.pdf.
https://www.msfaccess.org/spotlight-regional-comprehensive-economic-partnership-rcep.

Inne

Bashfield S., *Australia Needs a New National Security Strategy,* https://thediplomat.com/2019/02/australia-needs-a-new-national-security-strategy/.
https://australiansecuritymagazine.com.au/australias-international-cyber-engagement-strategy-launched/.
https://businessinsider.com.pl/finanse/makroekonomia/japonia-tworzy-nowy-lad-ekonomiczny-cptpp/tkjs35g.
https://en.wikipedia.org/wiki/Outline_of_Australia.
Prokurat S., *XXI wiek wiekiem Azji? (Tylko w pierwszej połowie XXI wieku. Technokapitalizm pomoże Zachodowi zdystansować gospodarczo Azję),* CSPA, 27.02.2017, http://www.polska-azja.pl/s-prokurat-xxi-wiek-wiekiem-azji-tylko-w-pierwszej-polowie-xxi-wieku-technokapitalizm-pomoze-zachodowi-zdystansowac-gospodarczo-azje/.

Abstrakt

Artykuł odnosi się do kwestii wybranych strategicznych aspektów cyberbezpieczeństwa Australii; ma charakter wprowadzający do niniejszej problematyki. Osadzony jest w ogólnie zarysowanych realiach polityki bezpieczeństwa prowadzonej przez nią od czasów zakończenia II wojny światowej, zwłaszcza w kontekście regionu Azji Południowo-Wschodniej; wymienia najważniejsze wydarzenia z okresu do końca lat 80. i aktywność Australii wobec instytucjonalizacji stosunków międzynarodowych w Azji. Następnie ukazuje, w kontekście istotnych z perspektywy tytułowej tematyki, zagadnień związanych z rozwojem technologii informacyjno-komunikacyjnych, pierwszą w historii *Strong and Secure. A Strategy for Australia's Nartional Security* (2013), implikowaną dokumentem *Australia in the Asian Century White Paper* (2012). W dalszej, zasadniczej części omawia cele, kierunki strategiczne, najważniejsze

aspekty przedmiotowe, instytucjonalne i prawne cyberbezpieczeństwa w oparciu o: *Australia's Cyber Security Strategy* (2016) i *Australia's International cyber Engagement Strtategy* (2017), z uwzględnieniem cyberprzestępczości jako szczególnego wyzwania dla ochrony.

Słowa kluczowe: Australia, bezpieczeństwo, cyberprzestrzeń, strategia, wyzwania

Abstract

The article concerns the chosen strategic aspectcs of Australia`s cyber security; it is of the introductory character. They are presented within the scope of the secure policy which the State has led since the end of the second World War. In particular, in the context of changes which have occurred in the South-East Asia region the basic agreements, such as APEC, ASEAN, AANZFTA etc. are listed as examples of way to institutionalize the Australia's international relations. Then the following documents are depicted (aims, scope etc.), taking into consideration the cyber security strategic approach: *Australia in the Asian Century White Paper* (2012); *Strong and Secure. A Strategy for Australia`s Nartional Security* (2013) *Australia's Cyber Security Strategy* (2016) and *Australia's International cyber Engagement Strtategy* (2017). Finally, the cybercrime as the special security threat is mentioned.

Keywords: Australia, security, cyberspace, strategy, challenges

Katarzyna Chałubińska-Jentkiewicz
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0003-0188-5704

System prawny cyberbezpieczeństwa w Rosji – charakterystyka

Dynamiczne zmiany cywilizacyjne, obserwowane w ostatnich latach na całym świecie są skutkiem gwałtownego rozwoju informacji oraz wspomagających ją technologii informacyjno-komunikacyjnych. Nową sferą oddziaływania tych procesów jest cyberprzestrzeń. Wraz z rozwojem cyberprzestrzeni ewoluują zagrożenia w niej występujące. Obecnie żadne państwo nie ma całkowicie bezpiecznej cyberprzestrzeni, dlatego konieczne jest podejmowanie nowych działań w celu minimalizacji strat spowodowanych atakami. Nie jest to jednak proste, gdyż cyberzagrożenia cechują się nieprzewidywalnością oraz globalnym zasięgiem. Cyberprzestrzeń to współcześnie symbol rozwoju, ale także wolności i prywatności, a każda ingerencja w jej funkcjonowanie kojarzona jest z atakiem na te wartości. W państwach zaangażowanych w budowę społeczeństwa informacyjnego bezpieczeństwo cyberprzestrzeni uznawane jest za jedno z najpoważniejszych wyzwań. Odpowiedzialność za zapewnienie cyberbezpieczeństwa spoczywa na wszystkich użytkownikach sieci, ale znaczącą rolę odgrywają określone organy administracji publicznej, której jednym z podstawowych zadań są działania na rzecz zapewnienia bezpieczeństwa i porządku publicznego. Realizacja zadań publicznych na rzecz cyberbezpieczeństwa wiąże się ściśle z przyjętą strategią i opartymi na niej regulacjami, które ostatecznie kształtują system cyberbezpieczeństwa wskazując kierunki i obszary działania,

którego sfera ta dotyczy (zarówno w sensie przedmiotowym, podmiotowym, organizacyjnym, jak i funkcjonalnym). Każda analiza rozwiązań prawnych dotyczących danego obszaru regulacji wymaga uprzedniego ustalenia rozwiązań systemowych na poziomie strategicznym. Kolejnym istotnym elementem jest sfera ingerencji w działania użytkowników sieci. To regulacje prawne, odnoszące się do kwestii prywatności i zakresu wkraczania władz publicznych w sferę prywatną jednostek – obywateli, określają charakter danego systemu prawnego obowiązującego w cyberprzestrzeni.

Strategie i akty prawne

W Federacji Rosyjskiej podstawowymi dokumentami strategicznymi są: doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej zatwierdzona dekretem Prezydenta Federacji Rosyjskiej z dnia 5 grudnia 2016 r. nr 646 oraz strategia rozwoku społeczeństwa informacyjnego Federacji Rosyjskiej na 2017–2030. W pierwszym z powyższych dokumentów wprowadzono pojęcie sfery informacyjnej, która obejmuje zbiór informacji, obiekty informatyzacji, systemy informacyjne, strony w sieci informatycznej i telekomunikacyjnej „Internet", sieci komunikacyjne, technologie informacyjne, a także podmioty, których działania związane są z tworzeniem i przetwarzaniem informacji, rozwój i wykorzystanie technologii informacyjnych, zapewnienie bezpieczeństwa informacji, a także zestaw mechanizmów regulujących public relations.

Zgodnie z doktryną narodowe interesy Federacji Rosyjskiej w sferze informacyjnej obejmują istotne potrzeby jednostki, społeczeństwa i państwa w zapewnieniu ich bezpieczeństwa i zrównoważonego rozwoju w sferze informacyjnej. Z kolei zagrożenie dla bezpieczeństwa informacji Federacji Rosyj-

skiej stanowi zbiór działań i czynników, które stwarzają niebezpieczeństwo szkodzenia wskazanym powyżej interesom narodowym w sferze informacyjnej. Bezpieczeństwo informacji definiuje się jako stan ochrony jednostki, społeczeństwa i państwa przed zagrożeniami informacyjnymi wewnętrznymi i zewnętrznymi, co zapewnia realizację konstytucyjnych praw i wolności człowieka i obywatela, godną jakość oraz standard życia obywateli, suwerenność, integralność terytorialną i zrównoważony rozwój społeczno-gospodarczy Federacji Rosyjskiej oraz obronność i bezpieczeństwo państwa. W celu zapewnienia bezpieczeństwa informacji jednym z kluczowych działań jest wdrożenie wzajemnie połączonych środków prawnych, organizacyjnych, operacyjnych, śledczych, wywiadowczych, kontrwywiadowczych, naukowych, technicznych, informacyjnych, analitycznych, kadrowych, ekonomicznych i innych środków do przewidywania, wykrywania, powstrzymywania, zapobiegania incydentom i eliminowania ich konsekwencji. Narzędzia bezpieczeństwa informacji to prawne, organizacyjne, techniczne i inne środki wykorzystywane przez siły bezpieczeństwa informacji, które tworzą organy państwowe, a także oddziały i urzędnicy organów państwowych, organy samorządu lokalnego i organizacji upoważnionych do wykonywania zadań w zakresie bezpieczeństwa informacji.

Doktryna wymienia główne zagrożenia informacyjne i do nich można zaliczyć wykorzystywanie możliwości transgranicznego obiegu informacji do osiągania geopolitycznych celów wojskowo-politycznych, a także terrorystycznych, ekstremistycznych, kryminalnych i innych niezgodnych z prawem, sprzecznych z prawem międzynarodowym kosztem bezpieczeństwa międzynarodowego i stabilności strategicznej. W doktrynie podkreśla się, iż różne organizacje terrorystyczne i ekstremistyczne szeroko wykorzystują mechanizmy informacyjne dotyczące świadomości indywidualnej, grupo-

wej i publicznej w celu wywołania napięć etnicznych i społecznych, pobudzenia nienawiści, w tym nienawiści etnicznej i religijnej, propagowania ideologii ekstremistycznej i przyciągania nowych zwolenników do działań terrorystycznych. Takie organizacje do celów nielegalnych aktywnie tworzą środki destrukcyjnego wpływu na obiekty krytycznej infrastruktury informatycznej. Jednym z głównych negatywnych czynników wpływających na stan bezpieczeństwa informacji jest rozbudowa przez wiele innych państw możliwości technologii informatycznych wykorzystywanych do wpływania na infrastrukturę informacyjną do celów wojskowych, wywiad techniczny w stosunku do rosyjskich organów państwowych, organizacji naukowych i przedsiębiorstw kompleksu wojskowo-przemysłowego, wykorzystywanie przez służby specjalne poszczególnych stanów informacji i wpływów psychologicznych mających na celu destabilizację wewnętrznej sytuacji politycznej i społecznej w różnych regionach świata, prowadzące do podważania suwerenności i naruszania integralności terytorialnej innych państw. W doktrynie wskazuje się, że w działalność taką zaangażowane są organizacje religijne, etniczne i inne organizacje i grupy. W Doktrynie podkreśla się, że istnieje tendencja w środkach masowego przekazu prezentowania negatywnej oceny polityki państwa Federacji Rosyjskiej. Z kolei rosyjskie media są narażane na jawną dyskryminację za granicą, a rosyjskim dziennikarzom utrudnia się prowadzenie działalności zawodowej. Kluczowym zagrożeniem jest wpływ informacji na ludność Rosji, przede wszystkim na młodzież, w celu osłabienia tradycyjnych rosyjskich wartości duchowych i moralnych.

W doktrynie wskazuje się także na sytuację w sferze gospodarczej, którą charakteryzuje niewystarczający poziom rozwoju konkurencyjnych technologii informacyjnych i ich wykorzystaniem do produkcji oraz usług. Wynika to z uzależnienia przemysłu krajowego od zagranicznych technologii informa-

cyjnych w zakresie bazy komponentów elektronicznych, oprogramowania, komputerów i komunikacji. W dziedzinie nauki, technologii i edukacji dostrzega się niewystarczającą wydajność badań naukowych mających na celu tworzenie obiecujących technologii informacyjnych, niski poziom realizacji rozwoju krajowego i niedostateczną obsadę w dziedzinie bezpieczeństwa informacji, a także niską świadomość obywateli w zakresie zapewnienia bezpieczeństwa danych osobowych. Tu doktryna podkreśla problem przestępczości komputerowej, zwłaszcza w sferze kredytowej i finansowej, przestępstw związanych z naruszaniem konstytucyjnych praw i wolności człowieka i obywatela, w tym w części dotyczącej prywatności, intymności i sfery rodzinnej, w przetwarzaniu danych osobowych z wykorzystaniem technologii informacyjnej.

Zgodnie z polityką wojskową Federacji Rosyjskiej głównymi kierunkami zapewnienia bezpieczeństwa informacji w dziedzinie obrony kraju są:

a) strategiczne odstraszanie i zapobieganie konfliktom zbrojnym, które mogą powstać w wyniku wykorzystania technologii informacyjnych;
b) usprawnienie systemu bezpieczeństwa informacji Sił Zbrojnych Federacji Rosyjskiej, innych wojsk, formacji i ciał wojskowych, w tym sił oraz środków konfrontacji informacyjnej;
c) prognozowanie, wykrywanie i ocena zagrożeń informacyjnych, w tym zagrożeń dla Sił Zbrojnych Federacji Rosyjskiej w sferze informacyjnej;
d) pomoc w zapewnieniu ochrony interesów sojuszników Federacji Rosyjskiej w sferze informacyjnej;
e) neutralizacja informacji i oddziaływanie psychologiczne, w tym mające na celu podważenie historycznych podstaw i tradycji patriotycznych związanych z obroną FR.

Głównymi kierunkami zapewnienia bezpieczeństwa informacji w dziedzinie bezpieczeństwa państwa i publicznego są:

a) przeciwdziałanie wykorzystaniu technologii informacyjnych do propagowania ideologii ekstremistycznej, szerzenie ksenofobii, idei wyłączności narodowej w celu podważania suwerenności, stabilności politycznej i społecznej, przymusowej zmiany porządku konstytucyjnego, naruszenia integralności terytorialnej Federacji Rosyjskiej;
b) zniesienie działań szkodliwych dla bezpieczeństwa narodowego Federacji Rosyjskiej, przeprowadzanych za pomocą środków technicznych i technologii informacyjnych przez służby specjalne i organizacje państw obcych, a także przez osoby fizyczne;
c) poprawa bezpieczeństwa krytycznej infrastruktury informacyjnej i trwałości jej działania, rozwijanie mechanizmów wykrywania i zapobiegania zagrożeniom informacyjnym oraz eliminowanie konsekwencji ich występowania, zwiększanie bezpieczeństwa obywateli i terytoriów przed skutkami sytuacji awaryjnych spowodowanych informacją i wpływem technicznym na obiekty krytycznej infrastruktury informacyjnej;
d) poprawa bezpieczeństwa funkcjonowania infrastruktury informatycznej, w tym w celu zapewnienia trwałej interakcji organów państwowych, zapobieganie zagranicznej kontroli nad funkcjonowaniem takich obiektów, zapewnienie integralności, trwałości funkcjonowania i bezpieczeństwa zunifikowanej sieci telekomunikacyjnej Federacji Rosyjskiej, a także zapewnienie bezpieczeństwa informacji przesyłanych za jej pośrednictwem i przetwarzane w systemach informatycznych na terytorium Federacji Rosyjskiej;
e) poprawa bezpieczeństwa funkcjonowania broni, sprzę-

tu wojskowego i specjalnego oraz zautomatyzowanych systemów kontroli;

e) zwiększenie skuteczności zapobiegania przestępstwom popełnianym przy użyciu technologii informacyjnych i przeciwdziałania takim przestępstwom;

g) zapewnienie ochrony informacji zawierających informacje stanowiące tajemnice państwowe, innych informacji o ograniczonym dostępie i dystrybucji, w tym poprzez zwiększenie bezpieczeństwa odpowiednich technologii informacyjnych;

h) doskonalenie metod i metod produkcji oraz bezpiecznego użytkowania produktów, świadczenie usług opartych na technologiach informacyjnych z wykorzystaniem krajowych rozwiązań spełniających wymogi bezpieczeństwa informacji;

i) poprawa skuteczności wsparcia informacyjnego dla realizacji polityki państwa;

j) neutralizacja wpływów informacyjnych mających na celu erozję tradycyjnych rosyjskich wartości duchowych i moralnych.

Podstawą organizacyjną systemu bezpieczeństwa informacji są: Rada Federacji Zgromadzenia Federalnego Federacji Rosyjskiej, Duma Państwowa Zgromadzenia Federalnego Federacji Rosyjskiej, rząd Federacji Rosyjskiej, Rada Bezpieczeństwa Federacji Rosyjskiej, federalne organy wykonawcze, Bank Centralny Federacji Rosyjskiej, Komisja Wojskowo-Przemysłowa Federacji Rosyjskiej, organy międzyresortowe ustanowione przez prezydenta Federacji Rosyjskiej i Rząd Federacji Rosyjskiej, a także władze lokalne oraz organy sądowe podejmowane zgodnie z ustawodawstwem Federacji Rosyjskiej uczestnictwa w rozwiązywaniu problemów związanych z bezpieczeństwem informacji.

Uczestnikami systemu bezpieczeństwa informacji są: właściciele krytycznych obiektów infrastruktury informatycznej i orga-

nizacji obsługujących takie obiekty, środki masowego przekazu i komunikacji masowej, organizacje monetarne, walutowe, bankowe i inne obszary rynku finansowego, operatorzy telekomunikacyjni, operatorzy systemów informatycznych, organizacje wdrażające działania w zakresie tworzenia i działania systemów informacyjnych i sieci komunikacyjnych, rozwoju, produkcji i działania środków dostarczania bezpieczeństwa informacji, w celu zapewnienia w zakresie usług ochrony informacji, organizacje zaangażowane w działania edukacyjne w tym zakresie, stowarzyszeń, innych organizacji publicznych i osób fizycznych.

Do zadań organów państwowych w ramach bezpieczeństwa informacji należą:

a) zapewnienie ochrony praw i uzasadnionych interesów obywateli i organizacji w sferze informacyjnej;
b) ocena stanu bezpieczeństwa informacji, prognozowanie i wykrywanie zagrożeń informacyjnych, identyfikacja obszarów priorytetowych dla ich zapobiegania i eliminacja konsekwencji ich manifestacji;
c) planowanie, wdrażanie i ocena skuteczności zestawu środków zapewniających bezpieczeństwo informacji;
d) organizacja działań i koordynacja interakcji sił bezpieczeństwa informacji, poprawa ich prawnych, organizacyjnych, operacyjnych-dochodzeniowych, wywiadowczych, kontrwywiadowczych, naukowo-technicznych, informacyjnych-analitycznych, personelu i wsparcia gospodarczego;
e) opracowywanie i wdrażanie środków wsparcia państwa dla organizacji zajmujących się rozwojem, produkcją i obsługą narzędzi bezpieczeństwa informacji, świadczeniem usług bezpieczeństwa informacji, a także organizacji prowadzących działania edukacyjne w tej dziedzinie.

Do zadań organów państwowych w ramach działań mających na celu rozwój i poprawę systemu bezpieczeństwa informacji należą:

a) wzmocnienie zarządzania pionowego i centralizacja sił bezpieczeństwa informacji na poziomie federalnym, międzyregionalnym, regionalnym, gminnym, a także na poziomie obiektów informatyzacji, operatorów systemów informatycznych i sieci komunikacyjne;
b) poprawa form i metod interakcji między siłami bezpieczeństwa informacji w celu zwiększenia ich gotowości do zwalczania zagrożeń informacyjnych, w tym poprzez regularne szkolenia (ćwiczenia);
c) poprawa analitycznych informacji i naukowo-technicznych aspektów funkcjonowania systemu bezpieczeństwa informacji;
d) zwiększenie skuteczności interakcji między organami państwowymi, organami samorządu lokalnego, organizacjami i obywatelami w rozwiązywaniu problemów zapewnienia bezpieczeństwa informacji.

W drugim istotnym w strategii FR dokumencie pt. Rozwój społeczeństwa informacyjnego w Federacji Rosyjskiej na lata 2017–2030 określono cele w realizacji polityki wewnętrznej i zagranicznej Federacji Rosyjskiej w zakresie technologii informacyjnych i komunikacyjnych, mające na celu rozwój społeczeństwa informacyjnego, budowaniu krajowej gospodarki cyfrowej. Główne zasady tej strategii to: a) zapewnienie praw obywateli do dostępu do informacji; b) zapewnienie swobody wyboru środków pozyskiwania wiedzy; c) zachowanie tradycyjnych i zwyczajowych dla obywateli (doskonałe z cyfrowych) form odbioru towarów i usług; d) priorytet tradycyjnych rosyjskich duchowych oraz moralnych wartości i poszanowanie norm zachowania opartych na tych wartościach, korzystanie z technologii informacyjnych i komunikacyjnych; e) zapewnienie legalności i rozsądnej wystarczalności w gromadzeniu, gromadzenie i rozpowszechnianie informacji o obywatelach i organizacjach; e) zapewnienie państwowej ochrony interesów

rosyjskich obywateli w sferze informacji; f) obiekty krytycznej infrastruktury informacyjnej – systemy informacyjne i sieci informacyjne i telekomunikacyjne agencje rządowe, a także systemy informacyjne, sieci informacyjne i telekomunikacyjne oraz zautomatyzowane systemy sterowania procesami działającymi w przemyśle obronnym, w opiece zdrowotnej, transporcie, komunikacji w sferze kredytowej i finansowej, energia, paliwo, energia jądrowa, rakieta i kosmos, górnictwo, metalurgia i chemia przemysł; m) sieci komunikacyjne nowej generacji – systemy technologiczne, przeznaczone do podłączenia do Internetu piątej generacji do użytku w urządzeniach Internet of Things, problem intensyfikacji wykorzystania samej technologii. Technologia zgodnie ze strategią to stworzony zespół na podstawie zaawansowanej wiedzy nano- i biotechnologia, technologia optyczna, sztuczna inteligencja, alternatywne źródła energii. Rozwój technologii gromadzenia i analizy danych, ich wymiana, kontrola procesu odbywa się na podstawie wprowadzenia technologii poznawczych, ich zbieżność z nano- i biotechnologią. Zgodnie ze strategią powszechne stosowanie powyższych technologii przyczynia się do rozwoju nowego etapu gospodarki – cyfrowego zapewnienia jedności sieci telekomunikacyjnych. Wskazana powyżej strategia obejmuje takie zadania, jak:

a) tworzenie rosyjskiego oprogramowania systemowego i stosowanie zaopatrzenia, sprzętu telekomunikacyjnego i niestandardowego urządzenia do powszechnego użytku przez obywateli;
b) tworzenie narzędzi bezpieczeństwa informacji dla aplikacji w rosyjskiej informacji i komunikacji technologicznej;
c) zapewnienie wykorzystania rosyjskich technologii w komunikacji w rządzie Federacji Rosyjskiej i w przedsiębiorstwach państwowych oraz w samorządzie lokalnym;
d) tworzenie uczciwego działania środowiska biznesowego dla rosyjskich deweloperów.

W celu ochrony danych w Federacji Rosyjskiej istotnym celem stała się poprawa ram regulacyjnych[1] w dziedzinie opra-

[1] Ustawodawstwo federalne dotyczące cyberbezpieczeństwa obejmuje ustawę federalną z dnia 29 czerwca 2015 r., nr 188-ФЗ „W sprawie zmian w ustawie federalnej »Informacje, technologie informacyjne i ochrona informacji«" oraz art. 14 ustawy federalnej „W sprawie systemu umownego w dziedzinie zamówień na towary, roboty i usługi i potrzeby komunalne". ustawę federalną z dnia 5 kwietnia 2013 r., nr 44-ФЗ (ze zmianami z dnia 31 grudnia 2014 r.) „W sprawie systemu kontraktów w dziedzinie zamówień na towary, roboty budowlane, usługi dla potrzeb państwowych i miejskich". Do podstawowych aktów prawnych związanych z kwestiami cyberbezpieczeństwa zaliczyć także można następujące akty prawne: ustawa federalna z 4 maja 2011 r., nr 99-ФЗ „O licencjonowaniu niektórych rodzajów działalności"; ustawa federalna z dnia 6 kwietnia 2011 r., nr 63-ФЗ „O podpisie elektronicznym"; ustawa federalna z dnia 28 grudnia 2010 r., nr 390-ФЗ „O bezpieczeństwie"; ustawa federalna z dnia 27 lipca 2006 r., nr 149-ФЗ „Informacje, technologie informacyjne i ochrona informacji"; ustawa federalna z 27 lipca 2006 r., nr 152-ФЗ „O danych osobowych"; ustawa federalna z 19 grudnia 2005 r., nr 160-ФЗ „O ratyfikacji Konwencji Rady Europy o ochronie osób zautomatyzowanym przetwarzaniem danych osobowych"; ustawa federalna z 29 lipca 2004 r., nr 98-FZ „On Commercial Secrets"; ustawa federalna z dnia 7 lipca 2003 r., nr 126-FZ „On Communications"; ustawa federalna z 27 grudnia 2002 r., nr 184-ФЗ „W sprawie przepisów technicznych"; Kodeks pracy Federacji Rosyjskiej. Rozdział 14 „Ochrona danych osobowych pracowników". 4 dekrety i zarządzenia Prezydenta Federacji Rosyjskiej: dekret Prezydenta Federacji Rosyjskiej nr 260 z dnia 22 maja 2015 r. „W sprawie niektórych kwestii bezpieczeństwa informacji Federacji Rosyjskiej"; dekret prezydencki nr 537 z dnia 12 maja 2009 r. „W sprawie strategii bezpieczeństwa narodowego Federacji Rosyjskiej do 2020 r."; dekret Prezydenta Federacji Rosyjskiej nr 351 z dnia 17 marca 2008 r. „W sprawie środków zapewniających bezpieczeństwo informacji Federacji Rosyjskiej podczas korzystania z sieci informacyjnych i telekomunikacyjnych międzynarodowej wymiany informacji"; dekret Prezydenta Federacji Rosyjskiej nr 1576 z dnia 1 listopada 2008 r. „O Radzie pod przewodnictwem Federacji Rosyjskiej w sprawie rozwoju społeczeństwa informacyjnego w Federacji Rosyjskiej"; dekret Prezydenta Federacji Rosyjskiej nr 1085 z 16 sierpnia 2004 r. „Pytania Federalnej Służby Kontroli Technicznej i Eksportowej" (zmieniony dekretem prezydenckim z dnia 22.03.2005 r., nr 330 z 20.07.2005 r., nr 846 z 30.11.2006 r., nr 1321 z 23.10.2008 r., nr 1517 z 11.17.2008 r., nr 1625); dekret Prezydenta Federacji Rosyjskiej nr 960 z 11 sierpnia 2003 r. „Pytania Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej"(zmieniony dekretem prezydenckim z 11 lipca 2004 r., nr 870 z dnia 31 sierpnia 2005 r., nr 1007 z dnia 1 grudnia 2005 r., nr 1383 z dnia 12 czerwca 2004 r., nr 602 z dnia 27.07.2006 r., nr 799 z 28.12.2006 r., nr 1476 z dnia 28.11.2007 r., nr 1594 z dnia 28.12.2007 r., nr 1765 z dnia 1.09.2008 r., nr 1278 z dnia

cowania norm międzynarodowych regulacji prawnych, do-

23.10.2008 r., nr 1517 z 11.11.2008 r., nr 1625 z dnia 4.12.2010 r., nr 499, z dnia 5.14.2010 r., nr 589); zarządzenie Prezydenta Federacji Rosyjskiej nr 366-rp z dnia 10 lipca 2001 r. „W sprawie podpisania Konwencji o ochronie osób w automatycznym przetwarzaniu danych osobowych"; doktryna bezpieczeństwa informacyjnego Federacji Rosyjskiej z 9 września 2000 r., nr Pr-1895; dekret Prezydenta Federacji Rosyjskiej nr 188 z dnia 6 marca 1997 r. „O zatwierdzeniu listy informacji o charakterze poufnym" (zmieniony dekretem prezydenckim z 23 września 2005 r., nr 1111 z 13 lipca 2015 r., nr 357); dekret Prezydenta Federacji Rosyjskiej nr 170 z dnia 20 stycznia 1994 r. „O podstawach polityki państwa w dziedzinie informatyzacji"(zmieniony dekretem prezydenckim z 7 lipca 1995 r., nr 764; nr 13 z dnia 17 stycznia 1997 r., nr 710 z 9 lipca 1997 r.); dekret Prezydenta Federacji Rosyjskiej nr 2334 z 31 grudnia 1993 r. „O dodatkowych gwarancjach praw obywateli do informacji"(zmieniony dekretem prezydenckim z 17 stycznia 1997 r., nr 13 z 1 września 2000 r., nr 1606); decyzje rządu Federacji Rosyjskiej; dekret Rządu Federacji Rosyjskiej z dnia 16 listopada 2015 r., nr 1236 „W sprawie ustanowienia zakazu przyjmowania oprogramowania pochodzącego z zagranicy w celu zaopatrzenia dla potrzeb państwowych i miejskich"; dekret rządu Federacji Rosyjskiej z dnia 21 marca 2012 r., nr 211 „O zatwierdzeniu wykazu środków mających na celu zapewnienie spełnienia zobowiązań przewidzianych w ustawie federalnej". „O danych osobowych „i przyjęte zgodnie z nim regulacyjne akty prawne, podmioty będące organami państwowymi lub gminnymi"; dekret rządu Federacji Rosyjskiej z dnia 3 lutego 2012 r., nr 9 „W sprawie działalności licencyjnej dotyczącej technicznej ochrony informacji poufnych"; Lista dokumentów wymaganych do uzyskania licencji na ochronę techniczną informacji poufnych; Wykaz dokumentacji technicznej, norm krajowych i dokumentów metodologicznych niezbędnych do wykonywania pracy i świadczenia usług ustanowionych w Regulaminie dotyczącym licencjonowania działalności w celu technicznej ochrony informacji poufnych; dekret rządu Federacji Rosyjskiej z dnia 3 lutego 2012 r., nr 171 „W sprawie działalności licencyjnej na rzecz rozwoju i produkcji narzędzi ochrony informacji poufnych"; Lista dokumentów wymaganych do uzyskania licencji na opracowanie i produkcję narzędzi bezpieczeństwa informacji poufnych; Wykaz dokumentacji technicznej i technologicznej, norm krajowych i dokumentów metodologicznych wymaganych do wykonywania rodzajów prac ustanowionych w rozporządzeniach dotyczących udzielania licencji na opracowanie i produkcję środków ochrony informacji poufnych; dekret rządu Federacji Rosyjskiej z dnia 1 listopada 2012 r., nr 1119 „O zatwierdzeniu wymogów dotyczących ochrony danych osobowych, gdy są one przetwarzane w systemach informacji o danych osobowych"; dekret rządu Federacji Rosyjskiej z dnia 21 listopada 2011 r., nr 957 „O organizacji udzielania licencji na niektóre rodzaje działalności"; dekret rządu Federacji Rosyjskiej z dnia 6 października 2011 r., nr 826 „O zatwierdzeniu standardowego formularza licencyjnego"; dekret Rządu Federacji Rosyjskiej z dnia 23 stycznia 2006 r., nr 32 „W sprawie zatwierdzenia zasad świadczenia usług

tyczących bezpiecznego i zrównoważonego funkcjonowania i rozwoju Internetu, w tym kwestii jurysdykcyjnych, a także tworzenie nowych mechanizmów partnerstw gwarantujących poufność i bezpieczeństwo osobiste użytkowników, poufność ich informacji i wykluczenie, anonimowość, nieodpowiedzialność użytkowników i bezkarność przestępcy w Internecie[2]. Główne kierunki rozwoju informacji rosyjskiej i technologii komunikacyjnych, których lista może zostać zmieniona w miarę pojawiania się nowych technologii obejmują takie działania, jak: a) konwergencja sieci komunikacyjnych i tworzenie nowych sieci komunikacyjnych pokolenia; b) przetwarzanie dużych ilości danych; c) sztuczna inteligencja; d) zaufana technologia identyfikacji elektronicznej i uwierzytelnianie, w tym w sferze kredytowej i finansowej; e) przetwarzanie w chmurze i mgle; e) Internet przedmiotów i Internet przemysłowy; g) robotyka i biotechnologia; h) inżynieria radiowa i podstawa elementów elektronicznych; i) bezpieczeństwo informacji[3].

komunikacyjnych dla transmisji danych"; uchwała rządu Federacji Rosyjskiej z dnia 2 marca 2005 r., nr 110 „w sprawie zatwierdzenia procedury nadzoru państwowego nad działalnością w dziedzinie komunikacji"; dekret rządu Federacji Rosyjskiej z dnia 30 czerwca 2004 r., nr 320 „w sprawie zatwierdzenia postanowienia w Federalnej Agencji Łączności"; dekret rządu Federacji Rosyjskiej z dnia 26 czerwca 1995 r., nr 608 „O certyfikacji środków bezpieczeństwa informacji"; dekret rządu Federacji Rosyjskiej z 3 listopada 1994 r. nr 1233 „O zatwierdzeniu rozporządzenia w sprawie procedury postępowania z oficjalnymi informacjami o ograniczonej dystrybucji w federalnych organach wykonawczych".

[2] Wdrożenie tej strategii jest zapewnione poprzez skoordynowane działania następujących organów państwowych, samorządy i organizacje lokalne: a) Rząd Federacji Rosyjskiej; b) Administracja Prezydenta Federacji Rosyjskiej; c) aparat Rady Bezpieczeństwa Federacji Rosyjskiej; d) federalne organy wykonawcze; e) Bank Centralny Federacji Rosyjskiej; f) władze wykonawcze podmiotów Federacji; g) samorządy lokalne; h) państwowe fundusze pozabudżetowe; i) fundusze i instytucje rozwoju (zgodnie z planem wdrożenie tej strategii); k) korporacje publiczne, firmy z państwowym udziałem i firmy prywatne (zgodnie z planem wdrożenia tej strategii).

[3] Inne strategie: Konceptualne wglądy do aktywności sił zbrojnych Federacji Rosyjskiej w przestrzeni informacyjnej, 2011; Концептуальные

Zgodnie z przyjętymi celami wspomnianych regulacji działania w zakresie bezpieczeństwa obejmują: 1) prognozowanie, identyfikacja, analiza i ocena zagrożeń bezpieczeństwa; 2) określenie głównych kierunków polityki państwa i planowania strategicznego w dziedzinie bezpieczeństwa; 3) regulacje prawne w dziedzinie bezpieczeństwa; 4) opracowanie i zastosowanie zestawu środków operacyjnych i długoterminowych w celu identyfikacji, zapobiegania i eliminowania zagrożenia dla bezpieczeństwa, powstrzymywania i neutralizowania ich konsekwencji; 5) stosowanie specjalnych środków ekonomicznych w celu zapewnienia bezpieczeństwa; 6) rozwój, produkcja i wprowadzanie nowoczesnych rodzajów broni, sprzętu wojskowego i specjalnego, a także sprzętu podwójnego i cywilnego do celów bezpieczeństwa; 7) organizacja działalności naukowej w dziedzinie bezpieczeństwa; 8) koordynacja działań organów rządu federalnego władz państwowych, podmiotów Federacji Rosyjskiej, władz lokalnych w dziedzinie zapewnienie bezpieczeństwa; 9) finansowanie kosztów bezpieczeństwa, kontrola wydatków docelowych przydzielonych środków; 10) współpraca międzynarodowa dla celów bezpieczeństwa; 11) realizacja innych działań w dziedzinie bezpieczeństwa zgodnie z ustawodawstwem Federacji Rosyjskiej.

Strategia Federacji Rosyjskiej zakłada także generalne cele związane z funkcjonowaniem Rosji na arenie międzynarodowej. Główne cele współpracy międzynarodowej w dziedzinie bezpieczeństwa to: 1) ochrona suwerenności i integralności

взгляды на деятельность Вооруженных Сил Российской Федерации в информационном пространстве. Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 r., 2013 Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года. Rosyjska koncepcja Konwencji ONZ „O międzynarodowym bezpieczeństwie informacyjnym" 2012; Российская концепция конвенции ООН «Об обеспечении международной информационной безопасности».

terytorialnej Federacji Rosyjskiej; 2) ochrona praw i uzasadnionych interesów obywateli rosyjskich za granicą; 3) wzmocnienie stosunków ze strategicznymi partnerami Federacji Rosyjskiej; 4) udział w działaniach organizacji międzynarodowych zainteresowanych dostarczaniem bezpieczeństwo; 5) rozwój stosunków dwustronnych i wielostronnych w celu wypełnienia zadań zapewniających bezpieczeństwo; 6) ułatwianie rozwiązywania konfliktów, w tym udział w działaniach pokojowych.

Prezydent Federacji Rosyjskiej określa główne kierunki polityki państwa w zakresie bezpieczeństwa; zatwierdza strategię bezpieczeństwa narodowego Federacji Rosyjskiej, inne dokumenty koncepcyjne i doktrynalne w dziedzinie bezpieczeństwa; tworzy i kieruje Radą Bezpieczeństwa, ustala kompetencje federalnych organów wykonawczych w dziedzinie bezpieczeństwa, którego zarządzanie prowadzi; zgodnie z procedurą ustanowioną przez federalną ustawę konstytucyjną z 30 maja 2001 r., nr 3-FKZ „w sytuacji stanu wyjątkowego" wprowadza na terytorium Federacji Rosyjskiej lub w jej kraju obszary zagrożenia, sprawuje władzę w sytuacji stanu wyjątkowego; akceptuje, zgodnie z ustawodawstwem Federacji Rosyjskiej: a) zastosowanie specjalnych środków ekonomicznych w celu zapewnienia bezpieczeństwa; b) środki mające na celu ochronę obywateli przed kryminalnymi i innymi bezprawnymi działaniami w celu przeciwdziałania terroryzmowi i ekstremizmowi; decyduje, zgodnie z ustawodawstwem Federacji Rosyjskiej, co do kwestii związanych z zapewnieniem ochrony: a) informacji i tajemnic państwowych; b) ludności i terytorium z sytuacji nadzwyczajnych. Rada Zgromadzenia Federalnego Federacji Rosyjskiej zatwierdza przyjęte przez Dumę Państwową federalne prawo w dziedzinie bezpieczeństwa oraz dekrety Prezydenta Federacji Rosyjskiej o wprowadzeniu stanu wyjątkowego. Z kolei Duma Państwowa przyjmuje federalne przepisy bezpieczeństwa. Uprawnienia rządu Fede-

racji Rosyjskiej w dziedzinie bezpieczeństwa to: 1) określanie głównych kierunków polityki państwa w zakresie zapewnienie bezpieczeństwa; 2) tworzenie federalnych programów docelowych w dziedzinie bezpieczeństwa i zapewnia ich wdrożenie; 3) ustanawianie kompetencji federalnych organów wykonawczych w dziedzinie bezpieczeństwa, którego zarządzanie prowadzi;) organizacja federalnych organów wykonawczych.

Nowe sankcje w dziedzinie cyberbezpieczeństwa

Jedną z najistotniejszych zmian w ustawie federalnej w sprawie zwalczania terroryzmu i niektórych aktów ustawodawczych Federacji Rosyjskiej w sprawie ustanowienia dodatkowych środków w celu zwalczania terroryzmu i zapewnienia bezpieczeństwa publicznego" z 7.07.2016, nr 374-Ф3 była regulacja związana z nowymi sankcjami dotyczącymi funkcjonowania środków społecznego przekazu. Federalny organ wykonawczy w dziedzinie bezpieczeństwa ma prawo do bezpłatnego otrzymywania od organów państwowych i państwowych funduszy pozabudżetowych systemów informacyjnych i/lub baz danych niezbędnych do wypełnienia powierzonych mu obowiązków, w tym poprzez uzyskanie możliwości zdalnego dostępu do nich, z wyjątkiem przypadków, w których ustawy federalne zabraniają transferu takich systemów i/lub baz danych Zmiany do ustawy federalnej nr 40–3 z dnia 3 kwietnia 1995 r. „O federalnej służbie bezpieczeństwa" (ustawa zbiorowa Federacji Rosyjskiej, 1995, nr 15, art. 1269; 2000, nr 1, art. 9; 2003, nr 27, art. 2700; 2006, r 17, art. 1779; 2016, nr 1, art. 88) wprowadziły kolejne rozwiązania, m.in. w art. 15, zgodnie z którym „publiczne wezwania do działań terrorystycznych, publiczne uzasadnienie terroryzmu lub propaganda terroryzmu – (zmienione ustawą federalną z dnia 29 grudnia 2017 r., nr 445-Ф3) podlegają karze grzywny w wysokości od stu tysięcy do pię-

ciuset tysięcy rubli lub w wysokości wynagrodzenia lub innego dochodu osoby skazanej na okres do trzech lat lub pozbawienia wolności na okres od dwóch do pięciu lat (zmienione ustawą federalną z dnia 12 września 2010 r., nr 352-ФЗ, z dnia 7.12.2011 r. nr 420-ФЗ, z dnia 7.06.2016 r., nr 375-ФЗ). Te same czyny popełnione za pomocą środków masowego przekazu lub elektronicznych lub teleinformatycznych sieci, w tym Internetu, podlegają karze grzywny w wysokości od trzystu tysięcy do miliona rubli lub wysokości wynagrodzenia lub innego dochodu osoby skazanej na okres od trzech do pięciu lat lub pozbawienia wolności na okres od pięciu do siedmiu lat z pozbawieniem prawa do zajmowania pewnych stanowisk lub podejmowania określonych czynności przez pięć lat (część 2 zmieniona ustawą federalną z dnia 6.07.2016, nr 375-ФЗ). Przy czym „propaganda terroryzmu jest rozumiana jako działalność polegająca na rozpowszechnianiu materiałów i (lub) informacji mających na celu stworzenie ideologii terroryzmu danej osoby, przekonanie o jej atrakcyjności lub postrzeganie dopuszczalności działań terrorystycznych”[4] (klauzula 1.1 została wprowadzona przez ustawę federalną z 29 grudnia 2017 r., nr 445-ФЗ).

Nowe zasady nadzoru elektronicznego – retencja danych

Dnia 6 lipca 2016 r. prezydent Federacji Rosyjskiej podpisał ustawę federalną nr 374 o zmianie federalnej ustawy o zwalczaniu terroryzmu i wybranych aktach prawnych Federacji Rosyjskiej w sprawie stworzenia dodatkowych środków mających na celu przeciwdziałanie terroryzmowi i ochrona bezpieczeństwa publicznego (ustawa federalna nr 374, PRAVO.GOV.RU z 7 lipca 2014 r., oficjalna publikacja w języku rosyjskim). Ustawa

[4] Obowiązuje od 20 lipca 2016 r. – Prawo federalne z dnia 6.07.2016 r., nr 375-ФЗ.

zawiera szereg przepisów rozszerzających prawa służb wywiadowczych i tajnych służb w zakresie monitorowania prywatnej komunikacji elektronicznej i tworzy podstawy prawne dla organów ścigania do przechwytywania „indywidualnych informacji komputerowych" (Id. art. 3). Ustawa zawiera nowe wymagania dla operatorów sieci telekomunikacyjnych dotyczące identyfikacji użytkowników i zachowania metadanych przesyłanych przez sieci. Ustawa dodaje do federalnej ustawy o komunikacji i ustawie o technologii informacyjnej i informatycznej wymóg, aby wszyscy operatorzy sieci „utrzymywali metadane dotyczące wszystkich połączeń, transmisji i odbioru informacji głosowych, tekstów pisanych, obrazów, dźwięków, wideo i innych wiadomości przesyłane za pośrednictwem sieci komunikacyjnych" przez okres trzech lat (Id. art. 13 § 2.) Te same metadane dla wiadomości przesyłanych online muszą być zachowane przez dostawców Internetu lub organizacje obsługujące usługi wymiany wiadomości przez jeden rok (Id. art. 15 § 1). Dokładny tekst przesyłanych wiadomości, zapisy połączeń telefonicznych („informacje głosowe") oraz treść innych komunikatów muszą być zachowane przez operatorów sieci telekomunikacyjnych przez okres sześciu miesięcy. Zgodnie z postanowieniem obowiązującym od 1 lipca 2018 r. informacje te muszą zostać przekazane służbom bezpieczeństwa na ich wniosek. Wprowadzono także nowe wymagania dla urządzeń szyfrujących stosowanych przez dostawców Internetu. Wymagania certyfikacyjne dotyczące kluczy szyfrowania i sprzętu szyfrującego zostały ustanowione na mocy wcześniejszych przepisów. Ustawa 374 zmienia Kodeks naruszeń administracyjnych, ustanawiając grzywnę za dodatkowe szyfrowanie lub za używanie wcześniej niecertyfikowanego sprzętu szyfrującego do 40 tys. RUB (około 700 USD) i zezwolić na konfiskatę sprzętu do kodowania (Id. art. 11, § 3).

Prawo Yarovaya wymaga zatem od operatorów telekomunikacyjnych przechowywania treści połączeń głosowych,

danych, obrazów i wiadomości tekstowych przez 6 miesięcy, a metadanych na nich (np. czasu, lokalizacji, nadawcy i odbiorców wiadomości) przez 3 lata. Usługi online, takie jak usługi przesyłania wiadomości, poczta elektroniczna i sieci społecznościowe, które wykorzystują zaszyfrowane dane, są wymagane, aby umożliwić Federalnej Służbie Bezpieczeństwa (FSB) dostęp do ich zaszyfrowanej komunikacji i ich odczytywanie. Firmy internetowe i telekomunikacyjne są zobowiązane do ujawnienia tych komunikatów i metadanych, a także „wszystkich innych niezbędnych informacji" organom na żądanie i bez nakazu sądowego.

Ponadto ustawa nakłada na dystrybutorów informacji za pośrednictwem Internetu obowiązek zgłaszania do Federalnej Służby Bezpieczeństwa „wszystkich informacji wymaganych do opisu otrzymanych, przekazanych lub dostarczonych wiadomości elektronicznych". Odmowa dostarczenia takich informacji będzie karana grzywna w wysokości 1 mln rubli (około 16 tys. USD) (Id. art. 11 § 5–6). Według rosyjskiej krajowej agencji prasowej TASS, jednocześnie z podpisaniem tej ustawy, prezydent Rosji wydał szereg zaleceń rządowi i niektórym agencjom rządowym, nakazując im sporządzenie do 1 listopada 2016 r. aktów prawnych mających na celu obniżenie ryzyka związanego z wdrożeniem ustawy. Zadania przewidują opracowanie wymagań technicznych dla krajowego oprogramowania i sprzętu, które będą potrzebne do gromadzenia, przechowywania i pobierania wszystkich informacji przesyłanych za pośrednictwem rosyjskiego Internetu oraz informacji o rosyjskich użytkownikach Internetu. Federalna Służba Bezpieczeństwa ma za zadanie zdefiniować procedury certyfikacji szyfrowania i protokół transferu kluczy szyfrowania, wraz z odpowiedzialnością za stworzenie listy urządzeń podlegających certyfikacji. Dodatkowo zmiany w prawie Yarovaya obejmują wydłużenie okresu więzienia za szereg działań przestępczych, wprowadzenie nowych powodów

odmowy wjazdu lub wyjazdu do i z Rosji oraz wprowadzenie odpowiedzialności karnej za niezgłoszenie organom ścigania faktu planowania „działalności terrorystycznej".

Częstym sposobem naruszania prywatności usługobiorców usług elektronicznych jest wykorzystywanie danych eksploatacyjnych, czyli *traffic data* – to danych pozwalających na śledzenie użytkowników w sieci. Dane te są niezbędne do ustanowienia i utrzymania łączności elektronicznej; zaliczają się do nich informacje dotyczące stron, z jakimi łączył się użytkownik i czasu nawiązania tego połączenia oraz jego trwania. Dane eksploatacyjne to dane o rozpoczęciu, zakończeniu i zakresie świadczonej usługi, czyli informacje o połączeniach między komputerami, w tym także ich adresach IP, rodzaju połączenia, dacie i czasie jego trwania. Charakterystyczną cechą danych eksploatacyjnych jest to, że na ich podstawie możliwe jest śledzenie i ocena aktywności usługobiorcy w sieci. Takie informacje dają usługodawcy możliwość ustalenia, z jakiej usługi świadczonej drogą elektroniczną skorzystał usługobiorca. Zalicza się do nich również adresy przeglądanych przez usługobiorcę stron, zapisy wiadomości wysyłanych pocztą elektroniczną czy też za pomocą SMS. Wszystkie te dane są zapisywane w logach systemowych serwerów usługodawcy[5]. Dzięki takim informacjom usługodawca jest w stanie określić, jakie strony interesują usługobiorcę, jakie reklamy przyciągają jego uwagę oraz z kim się kontaktował, co narusza tajemnicę korespondencji usługobiorcy. Ponadto należy zaznaczyć, że usługobiorca często nie jest świadomy, że informacje, które go dotyczą są przetwarzane.

Wskazane powyżej zasady dotykają kwestii tzw. retencji danych. Widoczną tendencją w różnych ustawodawstwach na

[5] K. Klafkowska-Waśniowska, *Art. 18, Przesłanki legalności*, [w:[*Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustawy*, red. D. Lubasz, M. Namysłowska, Warszawa 2011, s. 276.

świecie jest rozszerzanie zakresu uprawnień służb w zakresie korzystania z informacji na temat ruchu w sieci teleinformatycznej. Częstym uzasadnieniem jest walka z cyberterroryzmem. Prawo Yarovaya jest przykładem tego typu tendencji.

Bibliografia

Klafkowska-Waśniowska K., *Art. 18, Przesłanki legalności*, [w:] *Świadczenie usług drogą elektroniczną oraz dostęp warunkowy. Komentarz do ustawy*, red. D. Lubasz, M. Namysłowska, Warszawa 2011.

Milik P., *International legal regulations in the area of cybersecurity*, „Cybersecurity and Law" 2019, nr 1 (1).

Podstawy polityki Federacji Rosyjskiej w dziedzinie międzynarodowego bezpieczeństwa informacyjnego na okres do 2020 roku, 2013, http://www.scrf.gov.ru/security/information/document114/.

Rosyjska koncepcja Konwencji ONZ „O międzynarodowym bezpieczeństwie informacyjnym" 2012, https://digital.gov.ru/ru/events/36739/.

Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года.

Российская концепция конвенции ООН «Об обеспечении международной информационной безопасности».

Abstrakt

Każda analiza rozwiązań prawnych dotyczących danego obszaru regulacji wymaga uprzedniego ustalenia rozwiązań systemowych na poziomie strategicznym. Kolejnym istotnym elementem jest sfera ingerencji w działania użytkowników Internetu. To regulacje prawne odnoszące się do kwestii prywatności i zakresu wkraczania władz publicznych w sferę prywatną jednostek – obywateli określają charakter danego sys-

temu prawnego obowiązującego w cyberprzestrzeni. Bezpieczeństwo coraz częściej staje się podstawą ograniczeń praw i wolności jednostki. W artykule podjęto temat regulacji związanej z cyberbezpieczeństwem na poziomie strategicznym w Rosji.

Słowa kluczowe: cyberbezpieczeństwo, wolność słowa, regulacja, strategia

Abstract

Any analysis of legal solutions related to a given area of regulation requires prior determination of systemic solutions at the strategic level. Another important element is the sphere of interference in the activities of Internet users. It is the legal regulations relating to the issue of privacy and the scope of the entry of public authorities into the private sphere of individuals – citizens, determine the nature of a given legal system in force in cyberspace. Security is increasingly becoming the basis for restrictions on the rights and freedoms of the individual. The article deals with the topic of regulation related to cyber security at the strategic level in Russia.

Keywords: cybersecurity, freedom of speech, regulation, strategy

Malwina Ewa Kołodziejczak
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0002-2624-4009

Uwarunkowania prawne cyberbezpieczeństwa w Republice Chińskiej (Tajwan)[1]

Od kilkunastu już lat wzrasta poziom cyfryzacji w państwach Azji Wschodniej. Należy tu wyszczególnić nie tylko ogólnodostępne połączenie z Internetem czy zmiany w zakresie działania e-administracji, ale także poziom zabezpieczeń przed cyberzagrożeniami. Dobrym przykładem ukazania rozwoju w tym zakresie jest Tajwan.

Artykuł ma na celu wskazanie i charakterystykę rozwiązań prawnych dotyczących cyberbezpieczeństwa, które wdrożone zostały w Republice Chińskiej (Tajwan). Wybór tego obszaru nie jest przypadkowy z racji zarówno częstotliwości ataków w cyberprzestrzeni, jak i zdiagnozowania występujących i przyszłych zagrożeń. Toteż problem główny zawarty został w pytaniu: jakie są uregulowania prawne w zakresie cyberbezpieczeństwa na Tajwanie? W ostatnich latach przyjęto nowe przepisy, w tym ustawę dotyczącą cyberbezpieczeństwa wraz z regulacjami związanymi z zabezpieczeniem infrastruktury krytycznej, a także sześć aktów wykonawczych w tym zakresie[2]. Toteż wstępne badania wskazują, że regulacje prawne sta-

[1] Biorąc pod uwagę istotę zagadnienia, autorce trudno byłoby opracować niniejszy tekst bez przeprowadzenia badań wstępnych podczas pobytu na Tajwanie w ramach grantu Taiwan Fellowship 2018 – programu Ministerstwa Spraw Zagranicznych Tajwanu, a także dzięki pobytowi badawczemu w kwietniu 2019 r. zrealizowanemu w ramach badań statutowych Akademii Sztuki Wojennej.

[2] Autorka w tej części przedstawia wyniki badań i analizę aktów praw-

nowią interesujące rozwiązania, warte dalszej analizy przedmiotowej i podmiotowej.

Decydenci i politycy na Tajwanie na przestrzeni ostatnich kilku lat starali się przeprowadzać reformy i dbać o rozwój gospodarczo-społeczny, uwzględniając zmiany technologiczne i potrzebę cyfryzacji. Należy pamiętać, że kraj dopiero na początku lat 90. względnie ustabilizował się politycznie, wprowadzając w życie zasady państwa demokratycznego. Miało to wpływ na znaczący rozwój, który odnotowany został w światowych wskaźnikach postępu gospodarczego czy innowacyjnego[3].

Jeszcze ważniejszy jest ranking Global Information Technology Report, w którym przedstawia się wynik analizy zdolności państw do wykorzystywania technologii ICT (*Information and Communications Technology*) w związku z zaawansowaniem technologicznym, poziomem gospodarki, ze stanem otoczenia prawno-instytucjonalnego czy możliwością wykorzystania technologii informacyjnych i komunikacyjnych. Tajwan od kilku już lat zajmuje w nim wysokie miejsce. W ostatnim raporcie z 2016 r.[4] Tajwan w ogólnym rankingu uplasował się na 19 miejscu, ale w kategorii Infrastruktura i treści cyfrowe zajął pierwszą pozycję[5] i co istotne – 9 pozycję w podkategorii Bezpieczeństwo serwerów

nych, z kolei charakterystyka aspektów organizacyjnych i analiza dokumentów strategicznych zawarta jest m.in. w ekspertyzie dotyczącej umów międzynarodowych i bilateralnych Tajwanu i USA, opracowanej w ramach projektu w programie wsparcia badań podstawowych w uczelniach wojskowych pod nazwą „Grant badawczy pt.: *System cyberbezpieczeństwa RP – model rozwiązań prawnych,* kier. K. Chałubińska-Jentkiewicz, MON (GB/4/2018/208/2018/DA)".

[3] Zob. *Profil terytorialny Tajwanu,* Warszawskie Biuro Handlowe, Tajpej 2016, https://poland.tw/resource/0bee84ac-aaca-44f6-b6fe-20b3ed9f1114:JCR [dostęp: 10.09.2019].

[4] *Global Information Technology Report,* zob. http://reports.weforum.org/global-information-technology-report-2016/economies/#indexId=NRI&economy=TWN [dostęp: 21.12.2019].

[5] Podobnie jak w dwóch podkategoriach *Indeks konkurencji sektorów Internetu i telefonii komórkowej* oraz *Zasięg sieci komórkowej,* Zob. ibidem.

internetowych. Równie wysoką – 11 pozycję zajął w podkategorii *Znaczenie ICT w przyszłych rządowych założeniach.*

W istocie zwrócenie się Tajwanu w kierunku szeroko pojętego cyberbezpieczeństwa wynika z kilku powodów. Niewątpliwie jest to jeden z elementów strategii budowanej na zasadzie *public diplomacy*, a wynikającej z problemu uznania Tajwanu w świetle prawa międzynarodowego publicznego. Z racji braku uznania przez społeczność międzynarodową Tajwanu jako pełnoprawnego państwa, konieczne jest podejmowanie działań *soft power*[6]. Oprócz budowania sieci kontaktów i lobbingu, kreowania pozytywnego wizerunku własnego kraju, wspierania wartości i norm międzynarodowych, występują tu także instrumenty związane z technologią i cyfryzacją wraz z umiejętnością komunikacji cyfrowej.

Drugim powodem, dla którego względy cyberbezpieczeństwa są tak istotne dla Tajwanu, są liczne próby podejmowania ataków hackerskich przeprowadzanych z zewnątrz, m.in. za pośrednictwem innych podmiotów międzynarodowych. Kwestie te łączyć należy z występującymi elementami dezinformacji czy nawet tzw. „wojny informacyjnej". Co więcej, często wskazuje się, że ataki cybernetyczne, ale także *fake newsy*, zainfekowane aplikacje etc. są częstym elementem tego procederu. Toteż cyberbezpieczeństwo ma na Tajwanie szczególne znaczenie i rozpatruje się je także w kontekście bezpieczeństwa militarnego.

Z tego też względu coraz większe znaczenie w polityce, strategii i działaniach rządu ma cyberbezpieczeństwo ujęte w różnym wymiarze. Stąd nic dziwnego, że podjęto próby umoco-

[6] Soft power: the ability "to affect others though the cooptive means of framing the agenda, persuading and eliciting positive attraction in order to obtain preferred outcomes". Zob. J. Nye, *Soft Power – The Means to Success in World Politics*, New York 2004 oraz idem, *The Future of Power,* New York 2011.

wania regulacji w tym zakresie na poziomie ustawowym. Nowa ustawa z dnia 6 czerwca 2018 r. o zarządzaniu cyberbezpieczeństwem wraz z sześcioma aktami wykonawczymi[7] tworzą kompletne przepisy w tym zakresie. Warto w tym kontekście dodatkowo wspomnieć o regulacjach w prawie karnym w związku z przestępstwami popełnionymi w systemie informatycznym i telekomunikacyjnym. W znowelizowanym 19 czerwca 2019 r. kodeksie karnym[8] ostatni rozdział poświęcono cyberprzestępstwom zaliczając do nich m.in. *hacking*[9], *phishing*[10], wytwarzanie szkodliwych programów[11], zainfekowanie sprzętu (malware,

---

[7] Są to rozporządzenia z 2018 r.: *Regulations on the Notification and Response of Cyber Security Incident*, *Regulations on Classification of Cyber Security Responsibility Levels, Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency*, *Regulations of Special Non-official Agencies' Cyber Security Management by National Communications Commission*, *Enforcement Rules of Cyber Security Management Act, Cyber Security Information Sharing Regulations,* które dostępne są w języku angielskim w tajwańskim interentowym systemie aktów prawnych pod adresem: https://law.moj.gov.tw/ENG/Law/LawSearchResult.aspx?ty=ONEBAR&kw=cyber [dostęp: 20.12.2019].

[8] *Criminal Code of the Republic of China* z 19 czerwca 2019 r., https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=C0000001 [dostęp: 29.12.2019].

[9] Zgodnie z art. 358 k.k. osoba, która włamuje się do cudzego komputera/systemu albo go uszkadza zostanie skazana na karę pozbawienia wolności na okres nie dłuższy niż trzy lata lub zamiast tego albo dodatkowo może zapłacić grzywnę nie większą niż 100 tys. juanów (w obecnej walucie 300 tys. NTD).

[10] Zgodnie z art. 359 k.k .osoba, która bez zgody uzyskuje, usuwa lub zmienia zapis magnetyczny komputera innej osoby lub związanego z nią sprzętu, co powoduje szkodę publiczną lub pojedynczej osobie zostanie skazana na karę pozbawienia wolności nie dłuższy niż pięć lat lub zamiast tego albo dodatkowo, może zapłacić grzywnę w wysokości nie większą niż 200 tys. juanów (600 tys. NTD).

[11] Zgodnie z art. 362 k.k. osoba, która wytwarza dla siebie bądź innej osoby szkodliwe programy komputerowe w celu popełnienia przestępstwa, wyrządzając szkodę publiczną lub pojedynczej osobie zostanie skazana na karę pozbawienia wolności nie dłuższy niż pięć lat lub zamiast tego albo dodatkowo, może zapłacić grzywnę w wysokości nie większą niż 200 tys. juanów (600 tys. NTD).

randsomware, trojany, wirusy). Co ważne, jeśli przestępstwa te zostaną popełnione w związku z pełnieniem służby publicznej (atak na komputery, systemy organów i instytucji publicznych) kary są zwiększane o połowę[12].

W 2018 r. tajwańska władza wykonawcza rządu (Juan Wykonawczy)[13] zdecydowała o przyjęciu ustawy o zarządzaniu cyberbezpieczeństwem[14], która została podpisana przez prezydent 6 czerwca 2018 r. i obowiązuje od 1 stycznia 2019 r.

Właściwym organem odpowiedzialnym za regulacje zawarte w ustawie i przygotowanie właściwych aktów wykonawczych ustanowiono Juan Wykonawczy[15]. Wyznaczenie jednego regulatora nastąpiło stosunkowo późno w procesie legislacyjnym z powodu obaw, że rozproszenie regulacji dotyczących różnych sektorów i wskazanie kilku odpowiedzialnych za ich przygoto-

[12] Dla porównania, w polskim Kodeksie karnym przestępstwa przeciwko danym komputerowym i systemom informatycznym reguluje m.in. art. 267 – § 1 nieuprawniony dostęp do informacji, § 2 nieuprawniony dostęp do systemu informatycznego, § 3 nielegalny podsłuch i inwigilacja za pomocą urządzeń technicznych i programów komputerowych, § 4 ujawnienie informacji uzyskanej nielegalnie; art. 268 – § 2 i 3 naruszenie integralności zapisu informacji na informatycznym nośniku danych; art. 268a – naruszenie integralności danych, utrudnianie dostępu do danych oraz zakłócanie ich przetwarzania; art. 269 – sabotaż komputerowy; art. 269a – zakłócenie pracy systemu komputerowego lub sieci teleinformatycznej; 269b – tzw. bezprawne wykorzystanie urządzeń, programów i danych. Szerzej na ten temat zob.: F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym,* Warszawa 2016, s. 285–336.

[13] W przeciwieństwie do powszechnej w państwach zachodnich zasady monteskiuszowskiego trójpodziału władzy, na Tajwanie obowiązuje podział odmienny. Władza podzielona jest pomiędzy Juany (izby/rady). Zgodnie z Konstytucją występuje zatem: Juan Wykonawczy, Juan Legislacyjny, Juan Sądowniczy, Juan Kontrolny i Juan Egzaminacyjny. Jest to o tyle istotne, że wzmianka ta pozwala wskazać na zakres działań poszczególnych organów w kontekście cyberbezpieczeństwa.

[14] *Cyber Security Management Act*, https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030297 [dostęp: 16.12.2019].

[15] *Cyber Security Management Act,* art. 2.

wanie organów, byłyby nieskuteczne. W praktyce Departament Cyberbezpieczeństwa Juana Wykonawczego poprowadził działania regulacyjne przedstawiając dodatkowe rozporządzenia[16].

W art. 1 omówiono istotę ustawy i wskazano jej cel, którym jest wdrożenie krajowej polityki bezpieczeństwa informacji i zbudowanie bezpiecznego środowiska informatycznego w celu ochrony bezpieczeństwa narodowego i dobrobytu społeczeństwa.

Art. 3 przedstawia najważniejsze definicje, z których przytoczyć należy te odnoszące się do systemów informatycznych, bezpieczeństwa informacji, incydentów związanych z bezpieczeństwem informacji oraz infrastruktury krytycznej.

Ustawa definiuje system informatyczny i telekomunikacyjny jako system, który ma być wykorzystywany do gromadzenia, kontroli, przesyłania, przechowywania, rozpowszechniania, usuwania informacji lub innego przetwarzania, wykorzystywania i udostępniania takich informacji[17].

Bezpieczeństwo informacji (cyberbezpieczeństwo) przedstawione jest w rozumieniu działań mających zapobiec nieautoryzowanemu dostępowi, wykorzystaniu, kontroli, ujawnieniu, uszkodzeniu, zmianie, zniszczeniu lub innym naruszeniom systemów informatycznych i telekomunikacyjnych w celu zapewnienia poufności, integralności i dostępności systemów informatycznych[18].

Ustawa wyszczególnia także dwa rodzaje agencji – rządową oraz pozarządową. Agencja rządowa to centralna lub lokalna agencja rządowa (instytucji), która wykonuje władzę publicz-

---

16 M.R. Fahey, *Taiwan enacts Cyber Security Management Act*, [17.07.2018], artykuł dostępny na stronie Winkler Partners pod adresem: http://www.winklerpartners.com/?p=8933?utm_source=Mondaq&utm_medium=syndication&utm_campaign=View-Original [dostęp: 12.12.2019].

17 *Cyber Security Management Act,* art. 3 par. 1.

18 Ibidem, art. 3 par. 3.

ną zgodnie z prawem, z wyłączeniem agencji wojskowej i wywiadowczej. Z kolei przez wyrażenie „specjalna agencja pozarządowa" rozumie się dostawców infrastruktury krytycznej, przedsiębiorstwa państwowe i fundacje rządowe[19].

Ustawa definiuje także infrastrukturę krytyczną jako zasoby systemu lub sieci, fizyczne bądź wirtualne, których brak działania lub zmniejszenie efektywności działania doprowadziłoby do znacznego negatywnego wpływu na bezpieczeństwo narodowe, interesy publiczne, poziom życia obywateli i działalność gospodarczą[20].

Należy również przytoczyć definicję incydentu, który określony został jako zdarzenie, w którym stan systemu, usługi lub sieci najprawdopodobniej wskazuje na naruszenie polityki bezpieczeństwa cybernetycznego lub naruszenie środków bezpieczeństwa, a zatem negatywnie wpływa na wydajność systemów informatycznego i telekomunikacji, stanowiąc zagrożenie dla polityki cyberbezpieczeństwa[21].

Co więcej, w oddzielnych uregulowaniach uchwalono poziomy incydentów uderzających w zasoby systemów informatycznych[22]. Zgodnie z art. 2 rozporządzenia wyróżnia się cztery poziomy cyberincydentów[23]. Warto wspomnieć, że według Ju-

---

[19] Ibidem, art. 3 par. 5–6.

[20] Ibidem, art. 3 par. 7.

[21] Ibidem, art. 3 par. 4.

[22] *Regulations on the Notification and Response of Cyber Security Incident* z 21 listopada 2018 r., https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030305 [dostęp: 13.12.2019].

[23] Poziom pierwszy powinien zostać ustanowiony, gdy wykryto niewielkie naruszenie nieistotnych informacji biznesowych lub drobne zmiany w niepodstawowych informacjach biznesowych czy w innych systemach informatycznych i telekomunikacji albo zaistniałego działania, które miało wpływ na działalność podstawową systemu lub spowodowało przerwanie działalności innej niż podstawowa, którą jednak można naprawić w dopuszczalnym czasie przerwy, powodując wpływ na codzienne funkcjonowanie danej agencji. Poziom drugi dotyczy poważnych naruszeń informacji niezwiązanych jednak z infrastrukturą krytyczną albo działanie, które miało

ana Wykonawczego tylko w 2017 r. w tajwańskich instytucjach publicznych doszło do zdiagnozowanych 360 incydentów bezpieczeństwa. Podczas gdy większość była mniej poważnymi incydentami na poziomie pierwszym i drugim, to dwanaście z nich sklasyfikowano jako incydenty na poziomie trzecim[24]. Co jednak istotne, samych udanych ataków jedynie na Mini-

wpływ na działalność systemu (łącznie z przerwaniem funkcjonowania) niezwiązaną z podstawową działalnością gospodarczą. Poziom trzeci obejmuje poważne naruszenie podstawowych informacji biznesowych niezwiązanych z utrzymaniem i eksploatacją infrastruktury krytycznej lub niewielkie naruszenie poufnych, wrażliwych informacji dotyczących ogólnych spraw urzędowych czy też niewielkie naruszenie podstawowych informacji biznesowych obejmujących utrzymanie i eksploatację infrastruktury krytycznej albo działanie, które miało wpływ na działanie systemu informatycznego i telekomunikacyjnego, którego nie może naprawić w dopuszczalnym czasie lub działanie, które może mieć wpływ na działalność operacyjną lub podstawowy system informatyczny i telekomunikacyjny obejmujący utrzymanie i eksploatację infrastruktury krytycznej, którą jednak można naprawić w dopuszczalnym czasie przerwy. Natomiast poziom czwarty obejmuje poważne naruszenie poufnych, wrażliwych informacji dotyczących ogólnych spraw urzędowych lub podstawowych informacji biznesowych, obejmujących utrzymanie i eksploatację infrastruktury krytycznej lub naruszenie niejawnych informacji dotyczących bezpieczeństwa narodowego albo poważną zmianę poufnych, wrażliwych informacji dotyczących ogólnych spraw urzędowych lub podstawowych informacji biznesowych lub podstawowych informacji obejmujących utrzymanie i eksploatację infrastruktury krytycznej lub zmianę niejawnych informacji o bezpieczeństwie narodowym, a także wpływ na (przerwanie) podstawowe działanie systemu informatycznego i telekomunikacyjnego obejmujące utrzymanie i eksploatację infrastruktury krytycznej, którego nie można odzyskać w dopuszczalnym czasie przerwy, *Regulations on the Notification and Response of Cyber Security Incident,* art. 2. Warto dodać, że zgodnie z art. 6 powyższego rozporządzenia, po zapoznaniu się z incydentem związanym z cyberbezpieczeństwem agencja rządowa przekazuje powiadomienie właściwemu organowi albo w ciągu siedemdziesięciu dwóch godzin od zdarzenia incydentu bezpieczeństwa cybernetycznego, jeśli było to zdarzenie na poziomie pierwszym lub drugim, albo ciągu trzydziestu sześciu godzin od rozpoznania incydentu cybernetycznego na poziomie trzecim lub czwartek. Po zakończeniu kontroli szkód agencja rządowa kontynuuje dochodzenie w sprawie zaistniałego incydentu związanego z bezpieczeństwem cybernetycznym oraz przedkłada raport z dochodzenia, przebiegu zdarzenia i naprawy systemu w ciągu jednego miesiąca w sposób wyznaczony przez właściwy organ.

[24] M.R. Fahey, op.cit.

sterstwo Obrony Narodowej Tajwanu było znacznie więcej, gdyż blisko 750 tys. w 2017 r. i 680 tys. w 2018 r.[25] Oznacza to, że zdecydowana większość z nich była nieznaczącymi zabiegami, które jednak nie wypełniły znamion incydentów. Dodać należy, że nieudanych prób naruszenia systemu było zdecydowanie więcej.

Z kolei w rozporządzeniu Juana Wykonawczego z 21 listopada 2018 r. w sprawie udostępniania informacji z zakresu cyberbezpieczeństwa[26] wskazano, że udostępnianie informacji dotyczy zaistniałych sytuacji związanych z: wykrywaniem lub gromadzeniem danych w systemie informatycznym i telekomunikacyjnym; lukami w zabezpieczeniach systemu informatycznego i telekomunikacyjnego; metodami unieważniającymi kontrolę bezpieczeństwa systemów teleinformatycznych lub wykorzystującymi lukę w zabezpieczeniach; informacjami na temat szkodliwych programów; rzeczywistą szkodą lub możliwym negatywnym wpływem incydentu bezpieczeństwa cybernetycznego, jak również odpowiednimi środkami podejmowanymi w celu wykrycia okoliczności określonych w poprzednich pięciu przypadkach, zapobiegania im lub reagowania na nie lub w celu złagodzenia powstałej szkody oraz innymi informacjami technicznymi związanymi z incydentami w zakresie bezpieczeństwa cybernetycznego[27]. Co więcej, w regulacjach tego rozporządzenia zawarto, że w odniesieniu do otrzymanych informacji na temat bezpieczeństwa cybernetycznego każda agencja podejmuje odpowiednie środki bezpieczeństwa, aby zapobiec naruszeniu treści informacji na temat bezpieczeństwa cyberne-

[25] Ying-han Ma, *Military Cyber Threats andResponses*, „Defence Security Brief", grudzień 2018, vol. 7, nr 2, s. 6.

[26] *Cyber Security Information Sharing Regulations* z 21 listopada 2018 r., https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=A0030307 [dostęp: 13.12.2019].

[27] *Cyber Security Information Sharing Regulations,* art. 2 par. 1–7.

tycznego, danych osobowych[28] lub innych ważnych informacji, które nie mogą być udostępniane na mocy przepisów prawa lub aby chronić przed nieuprawnionym dostępem, który mógłby spowodować wyciek danych lub manipulowanie nimi[29].

Wskazać także należy, że rozdział II omawianej ustawy określa obowiązki agencji rządowych w zakresie utrzymania bezpieczeństwa ich systemów informatycznych. Agencje rządowe muszą spełniać wymogi poziomu odpowiedzialności w zakresie utrzymania bezpieczeństwa cybernetycznego, przy czym należy wziąć pod uwagę kategorię, ilość i istotę informacji przechowywanych lub przetwarzanych, a także skalę i zasięg systemów informatycznego oraz telekomunikacyjnego, aby określić, zmienić i wdrożyć plan utrzymania bezpieczeństwa cybernetycznego. Ponadto agencje te muszą wprowadzić politykę bezpieczeństwa informacji i wyznaczyć szefów ds. bezpieczeństwa informacji, którzy są również zobowiązani do zgłaszania incydentów związanych z naruszeniem bezpieczeństwem informacji m.in. do Juana Wykonawczego[30].

W zakresie bezpieczeństwa informacji sektora prywatnego istotną rolę odgrywają wyznaczeni operatorzy infrastruktury krytycznej. W omawianej ustawie w rozdziale III wskazano, że to organ centralny (np. właściwe ministerstwo) odpowiedzialny za odpowiedni sektor powinien po konsultacji z odpowiednią

---

[28] Odnośnie do ochrony danych osobowych istnieją szczegółowe oddzielne przepisy zawarte w ustawie z dnia 30 grudnia 2015 r. o ochronie danych osobowych (*Personal Data Protection Act*, zob. https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050021 [dostęp: 12.01.2020] oraz w przepisach wykonawczych z dnia 2 marca 2016 r. (*Enforcement Rules of the Personal Data Protection Act*, zob. https://law.moj.gov.tw/ENG/LawClass/LawAll.aspx?pcode=I0050022 [dostęp: 12.01.2020]). W ustawie uregulowano kwestie gromadzenia, przetwarzania i wykorzystywania danych osobowych, aby zapobiec naruszeniu praw osobistych i ułatwić prawidłowe wykorzystanie danych osobowych.

[29] Ibidem, art. 8.

[30] *Cyber Security Management Act,* art. 10–11.

agencją rządową, stowarzyszeniami obywatelskimi, naukowcami i ekspertami, wyznaczyć dostawcę (operatora) infrastruktury krytycznej i przedłożyć decyzję właściwemu organowi do zatwierdzenia, powiadamiając o tym zatwierdzonego dostawcę na piśmie[31]. Podobnie jak agencje rządowe, wyznaczeni operatorzy infrastruktury krytycznej będą zobowiązani do wdrożenia polityki bezpieczeństwa informacji oraz planu utrzymania bezpieczeństwa cybernetycznego, a informacje z tego zakresu zobowiązani są do przekazywania odpowiedniemu organowi centralnemu, który to jest zobowiązany do przeprowadzania audytu realizacji planu[32]. Wymóg przeprowadzania kontroli w takiej formie – przez organ centralny – został wprowadzony podczas procesu legislacyjnego w odpowiedzi na pierwotny projekt Juana Wykonawczego, w którym to agencje rządowe zyskałyby uprawnienia do przeprowadzania kontroli[33].

Ponadto dostawcy infrastruktury krytycznej muszą powiadamiać właściwe organy o wszelkich incydentach związanych z cyberbezpieczeństwem[34], co jest analogiczne z postanowieniami dyrektywy NIS[35]. Niedopełnienie tego obowiązku, jak

---

[31] Ibidem, art. 16.

[32] Ibidem.

[33] M.R. Fahey, op.cit.

[34] *Cyber Security Management Act,* art. 18.

[35] Dyrektywa 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 Unii (Dz.Urz. UE L 194/1), https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=CELEX%3A32016L1148 [dostęp: 12.01.2020]. Projekt dyrektywy w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej został przedstawiony w 2013 r. jako jeden z głównych elementów strategii cyberbezpieczeństwa. Dyrektywa NIS zarówno na operatorów usług kluczowych (art. 14), jak i dostawców usług cyfrowych (art. 16) przewiduje nałożenie obowiązków w zakresie bezpieczeństwa i zgłaszanie incydentów, zob. A. Savin, *EU Internet Law*, Northampton 2017, s. 347–348.

wynika z art. 21 przedmiotowej ustawy, obwarowane jest karą grzywny w wysokości od 300 tys. NTD do 5 mln NTD[36].

Z kolei w odniesieniu do agencji pozarządowych, które zajmują się systemami informatycznymi, ale nie zostały określone jako dostawcy (operatorzy) infrastruktury krytycznej także istnieje obowiązek wdrażania polityki oraz planu z zakresu bezpieczeństwa informacyjnego. Właściwy organ może zwrócić się o sprawozdanie z działalności i realizacji planu oraz ma możliwość przeprowadzenia audytu[37]. Nie jest on jednak obowiązkowy.

Wspomniany wyżej plan utrzymania cyberbezpieczeństwa zgodnie z art. 6 przepisów wykonawczych do ustawy o zarządzaniu cyberbezpieczeństwem[38], powinien zawierać następujące m.in. punkty: charakterystyka głównej działalności i jej znaczenie; polityka i cele bezpieczeństwa cybernetycznego, informacje o szefie ds. bezpieczeństwa cybernetycznego; stan systemów informatycznych systemów łączności; ocenę ryzyka cyberbezpieczeństwa; środki ochrony i kontroli w zakresie bezpieczeństwa cybernetycznego; mechanizmy zgłaszania, reagowania związane z incydentami w systemie czy też wytyczne dotyczące ciągłego doskonalenia i zarządzania wydajnością planu utrzymania bezpieczeństwa cybernetycznego i status jego wdrożenia.

Zgodnie z omawianą ustawą operator infrastruktury krytycznej może podlegać karze w wysokości od 100 tys. NTD do 1 mln NTD także w przypadku, jeżeli nie określi, nie zmieni lub nie wdroży planu utrzymania bezpieczeństwa cybernetycznego albo jeżeli nie przekaże sprawozdania z realizacji planu

---

[36] Co równa się kwocie od 35 tys. PLN do 600 tys. PLN.

[37] *Cyber Security Management Act,* art. 17.

[38] *Enforcement Rules of Cyber Security Management Act* z dnia 21 listopada 2018 r., art. 6.

utrzymania bezpieczeństwa cybernetycznego organowi centralnemu odpowiedzialnemu za odpowiedni sektor lub nie spełni wymagań związanych z przedłożeniem i wdrożeniem planu utrzymania bezpieczeństwa cybernetycznego, a także – jeśli zachodzi konieczność poprawienia planu, poprawki nie zostaną wdrożone oraz w przypadku braku zachowania procedury mechanizmu zgłaszania i reagowania na incydenty z zakresu cyberbezpieczeństwa[39]. Natomiast, jak wspomniano wyżej, w przypadku braku przedstawienia właściwemu organowi raportu ze zdarzenia w systemie informatycznym kara jest znacznie wyższa.

* * *

Należy wskazać, że dzięki wprowadzeniu nowej ustawy i regulacjom angażującym centralne organy, agencje rządowe oraz przedsiębiorców z sektora prywatnego, a nawet włączających w procedurę ośrodki naukowe i badaczy, może nastąpić realna poprawa zabezpieczenia środowiska cyberbezpieczeństwa. Wydaje się, że istotą jest tu odpowiednie monitorowanie i reagowanie na zdarzenia oraz incydenty w systemie informatycznym i zachowanie odpowiednich procedur raportowania, a w związku z tym dzielenie się wielowymiarowymi informacjami z zakresu bezpieczeństwa cybernetycznego i aktualizacja systemów informatycznych i telekomunikacyjnych.

Co więcej, Tajwan z racji skomplikowanego statusu prawnomiędzynarodowego i relacji geopolitycznych, narażony jest na częstsze i – jak się zdaje – poważne zagrożenia cyberbezpieczeństwa. W związku z tym konieczne jest ciągłe wdrażanie i ulepszanie wszystkich elementów zapewniających ochronę i poprawę funkcjonowania systemu cyberbezpieczeństwa.

[39] *Cyber Security Management Act,* art. 20.

Bibliografia

Akty prawne

Criminal Code of the Republic of China z dnia 19 czerwca 2019 r.
Cyber Security Information Sharing Regulations z dnia 21 listopada 2018 r.
Cyber Security Management Act z dnia 6 czerwca 2018 r.
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 (Dz.Urz. UE L 194/1).
Enforcement Rules of Cyber Security Management Act z dnia 21 listopada 2018 r.
Enforcement Rules of the Personal Data Protection Act z dnia 2 marca 2016 r.
Personal Data Protection Act z dnia 30 grudnia 2015 r.
Regulations on Audit of Implementation of Cyber Security Maintenance Plan of Specific Non-Government Agency z dnia 21 listopada 2018 r.
Regulations on Classification of Cyber Security Responsibility Levels z dnia 21 listopada 2018 r.
Regulations on the Notification and Response of Cyber Security Incident z dnia 21 listopada 2018 r.
Regulations of Special Non-official Agencies' Cyber Security Management by National Communications Commission z dnia 21 listopada 2018 r.

Publikacje zwarte, artykuły naukowe, raporty

Nye J., *Soft Power – The Means to Success in World Politics*, New York 2004.
Profil terytorialny Tajwanu, Warszawskie Biuro Handlowe, Tajpej 2016.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.
Savin A., *EU Internet Law*, Northampton 2017.
Ying-han Ma, *Military Cyber Threats and Responses*, „Defence Security Brief", grudzień 2018, vol. 7, nr 2.

Źródła internetowe

https://eur-lex.europa.eu.
https://law.moj.gov.tw.
http://reports.weforum.org.
http://www.winklerpartners.com.

Abstrakt

Celem artykułu jest charakterystyka rozwiązań prawnych w zakresie cyberbezpieczeństwa, które wdrożone zostały w Republice Chińskiej (Tajwan) w ostatnich kilku latach. Szczególnej analizie autorka poddała tajwańską ustawę z 2018 r. o zarządzaniu cyberbezpieczeństwem. Wybór tego obszaru nie jest przypadkowy. Doświadczenia Tajwanu stanowią przykład warty szerszej analizy, przede wszystkim z racji częstotliwości ataków w cyberprzestrzeni, jak i zdiagnozowaniu występujących i przyszłych zagrożeń. Warto jednak zwrócić uwagę na umiejętne prowadzenie polityki *soft power* i rokrocznie zajmowane wysokie miejsca w rankingach rozwoju w zakresie zdolności państw do wykorzystywania technologii cyfrowej oraz wprowadzone procedury i zabezpieczenia przed cyberzagrożeniami.

Słowa kluczowe: cyberbezpieczeństwo, technologia cyfrowa, incydent, infrastruktura krytyczna, Tajwan

Abstract

The aim of the article is to characterize new legal solutions in the field of cybersecurity that have been implemented in the Republic of China (Taiwan) in the last few years. The author analyzed the Taiwanese Act

of 2018 on cyber security management, which is the most important legal act about this branch.

Taiwan's experience is an interesting example, worth a broader analysis, due to the frequency of attacks in cyberspace and, as well as, the legal regulations and ability of diagnosis existing and future threats. The important role plays the skilful implementation the *soft power* policy in international relations.

All those treatments and tools allow to hold the high positions in the development rankings regarding the ability of countries to use digital technology as well as the procedures and safeguards against cyber threats.

Keywords: cybersecurity, digital technology, incident, critical infrastructure, Taiwan

Agnieszka Brzostek
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0002-7444-0186

Prawno-administracyjne podstawy cyberbezpieczeństwa Japonii

I. Wstęp

W powszechnej opinii Japonia uchodzi za państwo o wysokim stopniu rozwoju informatycznego i cywilizacyjnego, które od lat jest potęgą w świecie informatycznym i nowych technologii. Tym bardziej zaskakujące jest to, że dopiero w ostatnim dwudziestoleciu Japonia stworzyła cały system cyberbezpieczeństwa. Liczne ataki hakerskie, których adresatem stała się Japonia lub też wykorzystanie japońskich domen do tych ataków, zmusił japoński rząd do podjęcia działań w zakresie ochrony cyberprzestrzeni. Brak regulacji prawnych, instytucji zwalczających zagrożenia pochodzące z sieci oraz niedobór wyspecjalizowanych kadr, które zdolne byłyby ochronić sektor państwowy i prywatny, stał się problem kolejnych gabinetów. Zauważyć można zwiększoną aktywność legislacyjną rządów, która miała stanowić odpowiedź i jednocześnie rozwiązanie po kolejnych najczęściej spektakularnych atakach na instytucje państwowe czy przedsiębiorstwa. Cały proces zmian legislacyjnych i organizacyjnych ma obecnie swoją kulminację. Przygotowania do zbliżających się igrzysk olimpijskich w Tokio w 2020 r. zdeterminowały budowę całego systemu cyberbezpieczeństwa Japonii[1].

[1] P. Soja, *Cyberbezpieczeństwo Japonii w XXI w.,* „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1, s. 288.

Należy także podkreślić, że działania rządu japońskiego podejmowane są wspólnie z innymi państwami i podmiotami międzynarodowymi na podstawie umów międzynarodowych, których Japonia jest stroną[2]. Zintegrowana polityka międzynarodowa w zakresie cyberbezpieczeństwa jest najlepszą gwarancją ochrony przed atakami. Niemniej niniejsze opracowanie będzie dotyczyło tylko działań rządu japońskiego na zagrożenia zewnętrzne, przede wszystkim analizę rozwiązań prawnych i organizacyjnych w zakresie cyberbezpieczeństwa.

II. Polityka rządu Japonii w zakresie cyberbezpieństwa w latach 2010–2014

Zanim omówione zostaną regulacje prawne i rozwiązania administracyjne w zakresie cyberbezpieczństwa należy odnieść się do postanowień Konstytucji Japonii. Mają one fundamentalne znaczenie dla procesu zrozumienia polityki rządu Japonii. W art. 9 Konstytucji[3] Japonia wyrzeka się na zawsze wojny jako suwerennego prawa narodu, jak również użycia lub groźby użycia siły jako środka rozwiązywania sporów międzynarodowych. Nie będą nigdy utrzymywać sił zbrojnych lądowych, morskich i powietrznych i innych środków, które mogą służyć wojnie. Nie uznaje się prawa państwa do prowadzenia wojny. Pomimo tak jednoznacznej demilitaryzacji, Japonia od po-

[2] Obecnie Japonia prowadzi dwustronne dialogi na temat cyberprzestrzeni z 11 krajami (USA, Australia, Wielka Brytania, Francja, Niemcy, Rosja, Indie, ROK, Izrael, Estonia i Ukraina). Japonia prowadzi również dialog na temat cyberprzestrzeni z UE i ASEAN, a także w jej ramach trójstronne ramy Japonia–Chiny–ROK i Japonia–USA–ROK. Zob. JAPAN'S CYBER DIPLOMACY, https://www.mofa.go.jp/files/000412327.pdf [dostęp: 17.12.2019].

[3] Konstytucja Japonii z 3 listopada 1946 r., tłum. T. Suzuki, https://www.pl.emb-japan.go.jp/relations/konstytucja.htm [dostęp: 17.12.2019].

czątku przystąpiła do odbudowy Sił Zbrojnych[4]. Ograniczenia w zakresie posiadania Sił Zbrojnych wpływały też na rozwój polityki rządu w zakresie cyberbezpieczeństwa.

Początkowo podstawy prawne w zakresie cyberbezpieczeństwa były ogólne i pobieżne. Wydawana przez Ministerstwo Obrony Japonii Biała Księga do 2010 r. nie zawierała żadnych pojęć definiujących cyberbezpieczeństwo. W Narodowym Programie Obronnym w 2011 r. wskazano nowe zagrożenia i wyzwania związane z przestrzenią kosmiczną i cyberbezpieczeństwem[5].

Pierwsze regulacje prawne dotyczące cyberbezpieczeństwa powstały w 2000 r. (*e-Japan Strategy i Information Technology Basic*)[6]. Obecne ustalenia instytucjonalne sięgają 2005 r., kiedy powstało Narodowe Centrum Bezpieczeństwa Informacji (NISC)[7] i Rada Bezpieczeństwa ds. Cyberbezpieczenstwa (ISPC) decyduje o podstawowej strategii Japonii w zakresie bezpieczeństwa cybernetycznego w ramach strategicznej centrali IT[8]. NISC, podległe bezpośrednio premierowi Japonii, stało się centralną instytucją przeciw działaniom cybernetycznym, orga-

---

[4] Szerzej na temat strategii obronnych Japonii W. Jakubczak, A. Konopka, *Strategie bezpieczeństwa w globalizujący się świecie*, Gdańsk 2012, s. 102–122.

[5] Więcej na ten temat: ibidem, s. 116–122. W każdym następnym programie obrony Japonii opracowano strategię w zakresie zagrożeń w cyberprzestrzeni. Przyjęty w 2019 r. program obrony Ministerstwa Obrony Japonii poświęcił zagadnieniom odrębny rozdział. Zob. *Defense of Japan 2019*, https://www.mod.go.jp/e/publ/w_paper/pdf/2019/DOJ2019_Full.pdf [dostęp: 17.12.2019].

[6] P. Soja, op.cit., s. 293.

[7] Obecna nazwa to: *National center of Incident readiness and Strategy for Cybersecurity.*

[8] P. Kallender, Ch.W. Hughes, *Japan's Emerging Trajectory as a "Cyber Power": From securitization to Militarization at Cyberspace*, „Journal of Strategic Studies" 2017, Vol. 40, Issue 1–2, s. 8. Zob. Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th ed.), https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5.pdf [dostęp: 17.12.2019].

nem nadzorczym mającym uprawnienia legislacyjne i techniczne[9].

Następnie IPSC wydało w lutym 2006 r. „Pierwszą krajową strategię bezpieczeństwa informacji"[10]. Na jej mocy podziałowi uległy zadania: NPA (ang. *National Police Agency* – Narodowa Agencja Policji) ścigała cyberataki, które mogły zostać zakwalifikowane jako przestępstwa; JMOD (Ministerstwo Obrony) był w większości odpowiedzialny za sieci; kwestie wywiadowcze zostały podzielone między Biuro Bezpieczeństwa Narodowego NPA i Dowództwo Wywiadu Obronnego (DIH) JMOD, oba oddzielone od NISC. Wydarzenia w 2009 r. oraz uznanie znaczenia cyberbezpieczeństwa jako dziedziny bezpieczeństwa same w sobie przyspieszyły kolejne reformy Japonii[11].

Następna strategia, wydana w lutym 2009 r., wskazała organy właściwe w zakresie bezpieczeństwa cybernetyczego. Rząd utworzył Centrum Zarządzania Kryzysowego, które podlegało Głównemu Sekretarzowi Gabinetu Japonii[12], Biuro Badań Wywiadu Gabinetu, podległe Dyrektorowi Wywiadu Gabinetu i Głównego Sekretarza Gabinetu, a NISC kontrolowało ogólny monitoring systemów rządowych. Stworzenie tego systemu zapoczątkowało kontrolę polityczną nad bezpieczeństwem cybernetycznym[13]. Premier przyjął rolę dyrektora generalnego strategicznej centrali IT, a funkcję zastępcy dyrektora generalnego przyjęli sekretarz naczelny gabinetu, minister stanu ds. nauki i technologii, minister spraw wewnętrznych, minister ekonomii,

---

[9] P. Soja, op.cit., s. 293.

[10] T*he Second National Strategy on Information Security,* https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf [dostęp: 17.12.2019].

[11] Ataki hakerskie, jakie dotknęły agencje rządowe i ambasady państw azjatyckich. Zob. P. Soja, op.cit., s. 293.

[12] Minister stanu koordynujący politykę ministerstw i agencji rządowych. Cabinet Act, Article 12, Paragraph 2, Item 4 and 5.

[13] P. Kallender, Ch.W. Hughes, op.cit., s. 9.

handlu i przemysłu oraz 10 innych ministrów stanu. Sekretarz Głównego Gabinetu został przewodniczącym Rady ds. Polityki Bezpieczeństwa Informacji (ang. ISPC), a zastępcą minister stanu ds. polityki nauki i technologii. Ministrowie z NPA, MIC, ekonomii i obrony zasiadali jako członkowie Rady. Głównym zadaniem NISC w ramach scentralizowanej polityki bezpieczeństwa cybernetycznego była tylko koordynacja, a nie sprawowanie kontroli politycznej nad ministrami[14].

Rok 2011 był przełomowy w zakresie realizacji polityki ochrony przed atakami cybernetycznymi. Kiedy w sierpniu 2011 r. *Mitsubishi Heavy Industries* (MHI), największy japoński wykonawca w dziedzinie obronności, odkrył wirusy w swoim systemie w jedenastu lokalizacjach w całej Japonii: czterdzieści pięć serwerów i trzydzieści osiem komputerów zostało zainfekowanych przez co najmniej osiem rodzajów wirusów, gdy pracownicy nieświadomie otworzyli wiadomości e-mail zawierające APT. Niedługo potem dwóch innych dużych wykonawców kosmicznych, obronnych i inżynieryjnych – IHI Corporation i *Kawasaki Heavy Industries* (KHI) – potwierdziło, że byli atakowani. Wiadomości te stworzyły lawinę zainteresowania mediów kwestią cyberataków, ponieważ w kolejnych miesiącach szereg ministerstw i znanych organizacji również publicznie przyznało, że zostały celem wyrafinowanych cyberataków[15]. Jak zauważył P. Kallendar, reakcja JMoD na ataki z 2011 r. jest pouczająca. JMoD dowiedział się o problemach MHI tylko za pośrednictwem mediów, czego skutkiem było szybka zmiana postanowień umów z dostawcami, w których zobowiązywał wykonawców do:

– niezwłocznego poinformowania JMoD o wszelkich naruszeniach bezpieczeństwa;

[14] Ibidem.

[15] P. Kallender, *Japan, the Ministry of Defense and Cyber-Security: Progress and Pitfalls*, „The RUSI Journal" 2014, Vol. 159, Issue 1, s. 94.

– sporządzenia schematów komunikacji, aby wyjaśnić, kto jest odpowiedzialny i z kim należy się skontaktować w przypadku naruszenia bezpieczeństwa;
– wdrażać „pełne skany" za pomocą oprogramowania antywirusowego co tydzień;
– upoważnić ciągłe monitorowanie przez cały rok;
– w celu zachowania dokumentacji dostępu przez co najmniej trzy miesiące;
– do kontroli statusu szkolenia personelu w zakresie bezpieczeństwa cybernetycznego[16].

W latach 2010–2011 Ministerstwo Obrony opublikowało kolejne Białe Księgi obronności, w których po raz pierwszy w tak szerokim ujęciu wskazano zagrożenia wynikające z przekształcenia Internetu w nowoczesną broń. Zwrócono przy tym uwagę na międzynarodowy aspekt problemu, powtarzając amerykańskie rozwiązania instytucjonalno-prawne w charakterze możliwych do zaadaptowania i godnych naśladowania, np. potrzebę utworzenia odpowiednika Cyberdowództwa Stanów Zjednoczonych. W efekcie wewnątrz ministerstwa powstał dodatkowy pion pod postacią Jednostki Cyberbezpieczeństwa (CDU). Dysponując budżetem w wysokości ponad 140 mln dolarów komórka uzyskała pełną zdolność operacyjną w 2014 r. i jest wykorzystywana przez japońską armię jako główny organ udaremniający ataki na wszystkie systemy ministerialne[17]. W Strategii Cyberbezpieczeństwa wydanej w 2013 r. nastąpiła nowa definicja pojęcia „bezpieczeństwo cybernetyczne", uznano za element bezpieczeństwa narodowego i dziedzinę strategiczną wraz z lądem, morzem, powietrzem i przestrzenią kosmiczną[18].

---

[16] Ibidem, s. 95.

[17] P. Soja, op.cit., s. 293, Zob. P. Kallender, Ch.W. Hughes, op.cit., s. 11.

[18] *Cybersecurity Strategy. Towards a world-leading, resilient and vigorous cyberspace*, s. 3, https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf. Zob. też: P. Kallender, Ch.W. Hughes, op.cit., s. 10.

Istotne znaczenie w procesie tworzenia systemu cyberbezpieczństwa odegrało uchwalenie 13 grudnia 2013 r. ustawy o ochronie specjalnie wyznaczonych tajemnic[19], a następnie w listopadzie 2014 r. ustawy podstawowej o cyberbezpieczeństwie. Pierwsze z nich usystematyzował oznaczanie niektórych rodzajów informacji, w tym informacji operacyjnych związanych z JSDF, sygnałów lub danych zdjęciowych, sieci łączności obronnej i kryptografii oraz danych dotyczących wydajności broni i sprzętu wykorzystywanego w obronie, jako tajemnice bezpieczeństwa narodowego podlegające ograniczeniom i karom za naruszenia[20].

III. Ustawa podstawowa o cyberbezpieczeństwie z 2014 r.

Głównym celem uchwalonej w dniu 11 listopada 2014 r. ustawy podstawowej o cyberbezpieczeństwie[21] było przeciwdziałanie poważniejszym zagrożeniom bezpieczeństwa cybernetycznego oraz innym zmianom w sytuacjach wewnętrznych i zewnętrznych, które pojawiły się w skali globalnej wraz z rozwojem Internetu i innych zaawansowanych sieci informatycznych i telekomunikacyjnych oraz postępem w wykorzystaniu technologii informatycznych i telekomunikacyjnych. Ustawa wprowadziła pojęcie „podstawowej filozofii cyberbezpieczeństwa". Zakres regulacji uzasadniono wskazując, że zadaniem rządu jest zapew-

[19] Act on the Protection of Specially Designated Secrets, No. 108, http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=2&dn=1&x-=42&y=6&co=01&ia=03&ja=04&ky=protection+of+specially+designated+secrets&page=16 [dostęp: 17.12.2019].

[20] P. Kallender, Ch.W. Hughes, op.cit., s. 10.

[21] The Basic Act on Cybersecurity, Act No. 104, 12.11.2014, http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=2&dn=1&x-=0&y=0&co=01&ia=03&ja=04&ky=cyber+security&page=3 [dostęp: 17.12.2019].

nienie bezpieczeństwa cybernetycznego przy jednoczesnym zapewnieniu swobodnego przepływu informacji. Oprócz wyjaśnienia obowiązków, ustalenia podstaw strategii bezpieczeństwa cybernetycznego i innych środków związanych z bezpieczeństwem cybernetycznym zdecydowano o tworzeniu zaawansowanej sieci informacyjno-komunikacyjnej[22]. Ustawa nałożyła obowiązki na rząd, wskazując jego odpowiedzialność za sformułowanie i wdrożenie kompleksowych środków związanych z bezpieczeństwem cybernetycznym zgodnie z podstawową filozofią cyberbezpieczeństwa i przy współpracy samorządu lokalnego[23]. Zadaniem rządu jest podjęcie wszystkich niezbędnych środków: prawnych, finansowych i podatkowych, koniecznych do wdrożenia środków bezpieczeństwa cybernetycznego[24]. Jednocześnie ustawa delegowała rząd do przygotowania i uchwalenia planu bezpieczeństwa cybernetycznego w formie Strategii bezpieczeństwa cybernetycznego[25].

Zgodnie z założeniami ustawy strategia bezpieczeństwa cybernetycznego miała określać następujące kwestie: podstawowe zasady dotyczące środków bezpieczeństwa cybernetycznego, sprawy związane z zapewnieniem bezpieczeństwa cybernetycznego w agencjach administracyjnych, sprawy dotyczące promowania zapewnienia bezpieczeństwa cybernetycznego przez ważnych dostawców infrastruktury społecznej, ich organizacje organizujące oraz lokalne podmioty publiczne oraz rozwiązania niezbędne do kompleksowego i skutecznego promowania środków bezpieczeństwa cybernetycznego[26]. Ustawa określiła sposób procedowania Strategii: premier wraz z członkami rządu

[22] Ibidem, art. 1.

[23] Ibidem, art. 4.

[24] Ibidem, art. 10.

[25] Ibidem, art. 12.

[26] Ibidem, art. 12 pkt 1 i 2.

przygotowuje projekt Strategii, który bezzwłocznie przedstawia Izbie Reprezentantów, a po jej przyjęciu, niezwłocznie ją ogłosić we wszystkich przewidzianych prawem formach ogłaszania aktów normatywnych[27]. W celu zabezpieczenia niezbędnych środków na koszty wymagane do wdrożenia strategii bezpieczeństwa cybernetycznego, rząd umieszcza ją w budżecie każdego roku budżetowego[28].

Podstawowa ustawa w zakresie cyberbezpieczeństwa nakreśliła też schemat systemu cyberbezpieczeństwa. Państwo oznaczy organ administracyjny państwa lub inkorporowaną agencję administracyjną. Do ustanowienia jednolitych standardów bezpieczeństwa cybernetycznego przez krajowe agencje rządowe i niezależne agencje administracyjne oraz systemy informacyjne przez krajowe agencje rządowe. Monitorowanie i analiza nielegalnych działań w systemach informacyjnych rządów krajowych za pośrednictwem sieci informacyjnych i komunikacyjnych lub elektromagnetycznych nośników zapisu oraz bezpieczeństwo cybernetyczne w rządach krajowych. Reagowanie na zagrożenia cybernetyczne poprzez ćwiczenia i szkolenia, koordynacja z powiązanymi organizacjami w Japonii i poza nią, dzielenie się informacjami na temat bezpieczeństwa cybernetycznego między krajowymi agencjami rządowymi, niezależnymi agencjami administracyjnymi, specjalnymi korporacjami itp.[29]

Powołano Kwaterę Główną Strategii Bezpieczeństwa Cybernetycznego, której kierownikiem został główny sekretarz gabinetu Japonii[30.] W ramach przydzielonych mu uprawnień może wezwać szefa odpowiedniego organu administracyjnego do złożenia sprawozdania na temat środków podjętych na podstawie tego zalecenia, a także, jeżeli dyrektor generalny stwierdzi, że istnieje

[27] Ibidem, art. 12 pkt 3 i 4.

[28] Ibidem, art. 12 pkt 4–6.

[29] Ibidem, art. 13.

[30] Ibidem, art. 27.

szczególna potrzeba w sprawach zalecanych zgodnie z przepisami ust. 3, poinstruuje on premiera o takich sprawach zgodnie z art. 6 ustawy o rządzie (ustawa nr 5 z 1947 r.). Mogą zostać przedstawione opinie w celu podjęcia określonych działań[31].

W skład Kwatery Głównej, oprócz szefa i jego zastępcy[32], wchodzą: przewodniczący Krajowej Komisji Bezpieczeństwa Publicznego, minister spraw wewnętrznych i komunikacji, minister spraw zagranicznych, minister gospodarki, handlu i przemysłu, Minister obrony, a także, wśród ministrów stanu innych niż szef dywizji i zastępca szefa dywizji, osoby wyznaczone przez premiera jako uznane za szczególnie niezbędne do prowadzenia spraw Kwatery Głównej oraz eksperci do spraw cyberbezpieczeństwa mianowani przez premiera[33.] Kierownik odpowiedniego organu administracyjnego, zgodnie ze sztabem głównym, przekazuje Kwaterze Głównej Bezpieczeństwa Cybernetycznego w odpowiednim czasie materiały lub informacje dotyczące bezpieczeństwa cybernetycznego, które przyczyniają się do wykonywania jurysdykcji centrali[34].

Zgodnie z zaleceniami NISC, w listopadzie 2014 r. IPSC przyjęła „Politykę poprawy bezpieczeństwa cybernetycznego Japonii" i przekształciła się w siedzibę głównej strategii bezpieczeństwa cybernetycznego (CSSH), odpowiedzialną za stworzenie nowej japońskiej „całościowej rządowej" strategii bezpieczeństwa cybernetycznego z września 2015 r.[35]

---

[31] Ibidem, art. 27 pkt 4 i 5.

[32] Ibidem, art. 28.

[33] Ibidem, art. 29 pkt 2. *Ang. – The Chairperson of the National Public Safety Commission; The Minister for Internal Affairs and Communications, The Minister for Foreign Affairs; The Minister of Economy, Trade and Industry; The Minister of Defense;* http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=2&dn=1&x=0&y=0&co=01&ia=03&ja=04&ky=cyber+security&page=3 [dostęp: 17.12.2019].

[34] Ibidem, art. 30.

[35] Ibidem, s. 11.

Na podstawie ustawy wydano już nową strategię cyberbezpieczeństwa. Dużą wagę zaczęto już poświęcać przygotowaniomdo olimpiady w Tokio w 2020 r. Strategia podkreśliła, że cyberprzestrzeń jest obecnie kluczowym elementem ogólnego bezpieczeństwa narodowego Japonii i że będzie ona dążyć do stabilnego korzystania z cyberprzestrzeni zgodnie z szerszą strategią bezpieczeństwa administracji dotyczącą „proaktywnego wkładu w pokój międzynarodowy". JSDF jest zobligowany do obrony przed cyberatakami poprzez jakościowe i ilościowe wzmocnienie swoich zdolności, które obejmują obronę nie tylko własnych sieci i infrastruktury, pogłębienie relacji z podmiotami prywatnymi. Stategia wskazała na szerszą militaryzację cyberobrony i jej potencjał rozciągający się na uprzednio wyłączne domeny cywilne w japońskim społeczeństwie[36].

Rozwiązania prawne stworzyły system cyberbezpieczeństwa, w którym można wyodrębnić trzypoziomową strukturę reagowania na przypadki cyberataków. Pierwszy poziom obejmuje aktywność służb policyjnych (NAP), którym przyznaje się prawo do zatrzymania i przesłuchania osób podejrzanych o postępowanie niezgodne z przepisami. Jeżeli czyn zostaje przyporządkowany do kategorii zagrożeń godzących w bezpieczeństwo narodowe, wtedy organizacją wskazaną do przeciwdziałania są siły zbrojne, czyli Japońskie Siły Samoobrony. Istnieje także wywiad, którego zadaniem jest prewencja i przewidywanie ataków, zanim dojdzie do ich ucieleśnienia. Działania tych służb wzajemnie się przenikają, a nadzorujące ich pracę NAP, Ministerstwo Obrony oraz NISC tworzą ten system[37].

[36] P. Kallendar, Ch.W. Hughes, op.cit., s. 11–12. Zob. *Cybersecurtity Strategy* 4.09.2015, https://www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf [dostęp: 17.12.2019].

[37] P. Soja, op.cit., s. 295.

IV. Strategia Cyberbezpieczeństwa Japonii 2018 r.

W dniu 27 lutego 2018 r. uchwalono nową strategię cyberbezpieczeństwa[38]. Celem przewodnim strategii jest budowa wielopoziomowego bezpieczeństwa cybernetycznego poprzez koordynację działania wielu stron, wśród których można wyróżnić organy rządowe, samorządy lokalne, przedsiębiorstwa informatyczne, operatorzy infrastruktury krytycznej, instytucje edukacyjne i badawcze oraz społeczeństwo[39]. Biorąc pod uwagę zrozumienie, że niemożliwe jest całkowite wyeliminowanie ryzyka cyberbezpieczeństwa rząd założył, że będzie promować inicjatywy w ramach podstawowej wizji bezpieczeństwa cybernetycznego w celu zmniejszenia ryzyka do akceptowalnego poziomu i zapewnienia, że te operacje i usługi są dostarczane bezpiecznie i nieprzerwanie. Na kształt Strategii zasadniczy wpływ mają przygotowania do igrzysk olimpijskich w Tokio w 2020 r., które mogą stanowić zachętę do cyberataków. Dlatego każdy interesariusz musi poradzić sobie z każdą sytuacją poprzez konsekwentne wypełnianie swoich ról i współpracę, aby zapewnić płynne wdrożenie igrzysk Tokio 2020 i innych wydarzeń[40].

Ponieważ cyberprzestępczość i ataki cybernetyczne stają się coraz bardziej wyrafinowane i złożone, a rodzaje ataków są zróżnicowane, nie można ich już obsłużyć wyłącznie tradycyjnymi środkami pasywnymi i należy zastosować bardziej proaktywne środki niż wcześniej stosowane zaimplementowano. W tej sytuacji rząd, współpracując z przedsiębiorstwami cybernetycznymi,

[38] *Cyber Security Strategy 2018*, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf [dostęp: 17.12.2019].

[39] Stretegia Cyberbezpieczeństwa Japonii z 27 lutego 2018 r., s. 22.

[40] Ibidem.

będzie promować politykę „Proaktywnej cyberobrony”[41], która zapewnia rządowi wdrożenie aktywnej inicjatywy, która aktywnie broni przed atakami cybernetycznym i wykorzystując środki zapobiegawcze z wyprzedzeniem. W szczególności rząd będzie działał na rzecz promowania takich inicjatyw w celu zapobiegania szkodom wynikającym z cyberprzestępczości lub ataków cybernetycznych, takich jak promowanie udostępniania i wykorzystywania informacji o zagrożeniach, w celu umożliwienia obrony i zapobieganiu wykorzystywaniu technologii do wywoływania ataków w celu gromadzenia informacji o atakujących oraz prowadzenie działań przeciwko atakującym[42].

Strategia nakreśliła też zadania rządu, który będzie:

- promował rozwój niezawodnej infrastruktury informacyjnej, w tym wzmocnienie międzynarodowych podmorskich kabli i innych obiektów infrastruktury;
- współpracował z dostawcami usług kryptowalut w celu promowania środków, aby ludzie mogli bezpiecznie angażować się w handel kryptowalutami;
- w odniesieniu do pojazdów i dronów samojezdnych rząd będzie promować środki mające na celu uniknięcie nieautoryzowanych operacji z powodu cyberataków;
- promował zwalczanie takich przestępstw, współpracując jednocześnie z powiązanymi instytucjami lub organizacjami w prowadzeniu publicznych kampanii uświadamiających, aby każda osoba promować niezależne środki przeciw cyberprzestępczości. Ponadto poprawa zdolności dochodzeniowych i technologicznych jest również niezbędna do zajęcia się nowymi rodzajami cyberprzestępczości[43];
- wzmacniał swoje możliwości w zakresie cyfrowej medycy-

[41] *Proactive Cyber Defense.*

[42] Strategia Cyberbezpieczeństwa Japonii 2018, op.cit., s. 23.

[43] Ibidem.

ny sądowej, zwiększając możliwości technologiczne w zakresie analizowania najnowszych urządzeń cyfrowych lub złośliwego oprogramowania;
– przeprowadzał kompleksową analizę w celu przewidywania zagrożeń dla cyberprzestrzeni i za technologiczne rozwikłanie tych zagrożeń;
– promował pozytywne wykorzystanie wiedzy i doświadczenia prywatnych przedsiębiorstw, wymianę personelu między sektorem publicznym i prywatnym oraz środki przeciw cyberprzestępczości, w których w świetle wymiany informacji, analizy informacji, zapobiegania szkodom wynikającym z cyberprzestępczości[44].

W Strategii zauważono, że w zakresie ochrony infrastruktury krytycznej rząd wdrożył inicjatywy mające na celu zapewnienia usług infrastruktury krytycznej w sposób bezpieczny i ciągły. Problemem jest istnienie różnic w poziomie świadomości w zakresie bezpieczeństwa cybernetycznego i postępach w inicjatywach między poszczególnymi sektorami infrastruktury krytycznej. Aby rozwiązać te problemy, konieczne jest podniesienie ogólnego poziomu bezpieczeństwa cybernetycznego. W związku z tym rząd będzie współpracował z sektorami prywatnymi w celu zapewnienia proaktywnego wsparcia, ponieważ każdy interesariusz pracuje nad własnymi niezależnymi inicjatywami, w tym rozważaniem modeli środków bezpieczeństwa cybernetycznego w odniesieniu do operatorów infrastruktury krytycznej o ograniczonych zasobach zarządzania, dla których trudno jest odpowiednio zainwestować w cyberbezpieczeństwo[45]. Do tej pory rząd sformułował i zrewidował „Politykę bezpieczeństwa cybernetycznego" w zakresie ochrony infrastruktury krytycznej i będzie nadal wdrażał oparte na niej inicjatywy. „Polityka cyberbezpieczeństwa" oczeku-

[44] Ibidem, s. 24.
[45] Ibidem.

je na przegląd po igrzyskach w Tokio 2020. Jednak w razie potrzeby zostaną one poddane przeglądowi nawet przed wyznaczoną datą, jeśli będzie tego wymagała sytuacja[46].

W celu utrzymania bezpieczeństwa rząd odpowiednio poprawi ramy instytucjonalne stosując takie środki, jak pozycjonowanie środków bezpieczeństwa cybernetycznego jako przepisów bezpieczeństwa w powiązanych przepisach ustawowych i wykonawczych itp.[47] Zgodnie z najnowszymi trendami w atakach cybernetycznych konieczne jest umożliwienie zainteresowanym stronom, takim jak organy rządowe i operatorzy infrastruktury krytycznej, szybkiego dzielenia się wiedzą i stwierdzenia czy konieczna jest szybka reakcja w przypadku[48] wykrycia cyberataku. W tym celu rząd przygotuje „Skalę dotkliwości incydentów cybernetycznych NISC w przypadku awarii WNP" oraz oceni i opublikuje dotkliwość incydentów, aby zachęcić i umożliwić różnym zainteresowanym stronom racjonalne i odpowiednie reagowanie, biorąc pod uwagę efekt i wpływ dokładnego informowania publiczny. Rząd dokona również przeglądu Skali w celu jej ulepszenia.

W Strategii zawarto także postulat wspólnych szkoleń i ćwiczeń między sektorem publicznym i prywatnym. Ważne jest, aby prowadzić szkolenia i ćwiczenia z założeniem wystąpienia awarii usług, aby zwiększyć możliwości operatorów infrastruktury krytycznej, aby mogli odpowiednio reagować na takie sytuacje. Rząd i powiązane instytucje będą kontynuować wdrażanie szkoleń i ćwiczeń wśród interesariuszy różnej wielkości ponad granicami sektora publicznego i prywatnego, a także poszerzać zakres i ulepszać ich zawartość w miarę potrzeb dla ich dalszego rozwoju[49].

[46] Ibidem, s. 25.

[47] Ibidem, s. 26.

[48] Ibidem.

[49] Ibidem.

W Strategii dostrzeżono też potencjał samorządu lokalnego, który mogą mieć znaczący wpływ na działalność społeczeństwa. Chociaż istnieją ograniczenia w zakresie rozwiązań technicznych, które mogą być podejmowane indywidualnie dla środków bezpieczeństwa cybernetycznego przez organizacje o ograniczonych zasobach, konieczne jest przede wszystkim wdrożenia środków zapobiegających wyciekowi informacji, w tym numeru indywidualnego, z powodu przerwy w świadczeniu usług lub błędu ludzkiego[50]. Biorąc pod uwagę tę sytuację i ze względu na obecny podział ról między samorządy krajowe i lokalne, samorządy krajowe w całym kraju podjęto zasadnicze wzmocnienie środków, a rząd krajowy będzie w razie potrzeby aktualizował wytyczne dotyczące polityki bezpieczeństwa w świetle konieczności osiągnięcia wysokiego poziomu bezpieczeństwa. Rząd będzie również pracował nad osiągnięciem niezbędnego poziomu bezpieczeństwa sieci operacyjnych i promował inicjatywy mające na celu zabezpieczenie i rozwój zasobów ludzkich związanych z cyberbezpieczeństwem, ulepszanie systemów, a także zabezpieczenie niezbędnego budżetu, pamiętając jednocześnie o potrzebie płynnego działania samorządów[51].

W Strategii wskazano, że do tej pory starano się podnieść ogólny poziom bezpieczeństwa informacji organów rządowych poprzez opracowanie środków bezpieczeństwa informacji opartych na ujednoliconych standardach, inicjatyw audytu opartych na tych standardach oraz monitorowanie nieautoryzowanej komunikacji, a rząd jest zobowiązany do kontynuowania prac nad tymi inicjatywami. Inicjatywy te zostały rozszerzone w taki sam sposób, jak w przypadku organów rządowych poprzez przegląd ustawy podstawowej o cyberbezpieczeństwie i będą one być ważnym zagadnieniem, mającym na celu pro-

[50] Ibidem, s. 26–27.

[51] Ibidem.

mowanie skutecznych środków bezpieczeństwa informacji w inkorporowanych agencjach administracyjnych itp., biorąc pod uwagę cechy ich różnorodnych form biznesowych[52].

Strategia założyła zwiększenie zdolności obronnych i świadomości warunkowej systemów informatycznych Agencje, które będą działać zapobiegawczo zapobiegając szkodom i zapobiegając ich rozprzestrzenianiu się, wykrywając zachowanie szkodliwego oprogramowania w punkcie końcowym (komputer osobisty itp.), w którym uruchamiane są programy. Dzięki automatyzacji zarządzania zasobami informatycznymi agencje będą monitorować stan systemów informatycznych w czasie rzeczywistym i umożliwią szybkie usuwanie luk w oprogramowaniu. Inicjatywy ochrony danych zostaną również przeprowadzone dla wszystkich agencji, aby zapobiec wyciekom informacji w razie wystąpienia incydentów. Ponadto konieczne jest zbadanie środków służących do identyfikacji ataków trudnych do wykrycia poprzez analizę zagrożenia, łącząc zjawiska występujące na różnych urządzeniach i informacje o zarządzaniu kontem. Aby skutecznie wdrożyć te środki należy ustanowić systemy mające na celu automatyzację pracy wymaganej do analizy informacji[53]. Aby każda agencja mogła wybrać odpowiednią formę systemu informacyjnego zgodnie z charakterystyką informacji oraz aby środki bezpieczeństwa mogły być skutecznie realizowane dla całego rządu, rząd będzie promować stosowanie usług w chmurze, w tym migracji do wspólnej platformy rządowej w formie prywatnej chmury rządowej, która może wykorzystać korzyści wynikające z konsolidacji budowy i działania systemów oraz zwiększenia poziomu bezpieczeństwa. Promując korzystanie z chmury, rząd rozważy i podejmie kroki w celu promowania korzystania z niezawodnej chmury, w któ-

[52] Ibidem, s. 27.

[53] Ibidem, s. 28.

rej zapewniony jest odpowiedni poziom bezpieczeństwa, taki jak ocena bezpieczeństwa[54].

W Strategii pojawił się postulat zacieśnienia współpracy agencji rządowych ze środowiskiem naukowym i badawczym. Dotyczy to wymiany informacji i budowy systemu reagowania. Takie zadanie Strategia postawiła przed rządem. Rząd też będzie promować niezależne i organizacyjne inicjatywy uniwersytetów, tj. tworzenie i rozpowszechnianie wytycznych dotyczących bezpieczeństwa cybernetycznego; wdrażanie praktyk dla każdego poziomu w zakresie zarządzania ryzykiem i reagowania na incydenty oraz praktycznych szkoleń i ćwiczeń, a także wsparcie dla początkowej reakcji na zdarzenie incydentów[55]. Z tego też powodu organizacje obsługujące sieci informacji naukowej będą współpracować z krajowymi uniwersytetami w celu opracowania systemu monitorowania, wykrywania i analizy cyberataków oraz dostarczania informacji o tych atakach, a także przeprowadzania wspólnych badań i szkoleń dla personelu technicznego w celu utrzymania i wzmocnić funkcje monitorowania i rozwinąć poziom zarządzania strategicznego oraz szkolenie personelu technicznego. Aby wzmocnić zespół reagowania na incydenty na tych uniwersytetach rząd będzie również wspierać inicjatywy, w których zespół zajmujący się incydentami dla wielu uniwersytetów i instytutów badawczych dzieli się informacjami, wspólnymi problemami i wiedzą na temat reagowania na incydenty związane z cyberatakami[56].

Jednym z zasadniczych celów, jakie postawiła sobie Strategia jest przygotowanie systemu ochrony przed cyberatakami podczas igrzysk w Tokio w 2020 r. i wykorzystanie tych rozwiązań na przyszłość[57]. Analizując incydenty na poprzednich

[54] Ibidem.

[55] Ibidem, s. 30.

[56] Ibidem, s. 31.

[57] Ibidem.

olimpiadach[58], zauważano, że niezliczeni sportowcy, zagraniczni dygnitarze i kibice zgromadzą się z całego świata na igrzyskach olimpijskich/paraolimpijskich, zapewniając gospodarzowi wydarzenia najwyższy możliwy poziom uwagi i potencjalnie czyniąc go celem cyberataków. Według Strategii oczekuje się, że olimpiada w Tokio 2020 r. będzie jeszcze bardziej narażona na ataki cybernetyczne niż w przeszłości i istnieje obawa, że ataki te będą wielokierunkowe. Z tego powodu rząd zapewni cyberbezpieczeństwo podczas igrzysk Tokio 2020 i będzie promować dalsze działania wykraczające poza to wydarzenie. Te różnorodne środki zostaną rozszerzone i będą kontynuowane po igrzyskach w Tokio 2020, a dziedzictwo systemów zostanie opracowane; doświadczenie i wiedza w ich działaniu będą wykorzystywane do ciągłego wzmacniania cyberbezpieczeństwa w Japonii w przyszłości[59].

W dniu 26 grudnia 2018 r. Izba Reprezentantów uchwaliła projekt ustawy zmieniającej ustawę podstawową o cyberbezpieczeństwie z 2014 r.[60] Poprawka ma na celu zapewnienie bezpieczeństwa cybernetycznego, podczas gdy Japonia będzie gospodarzem igrzysk olimpijskich w Tokio i paraolimpiady w 2020 r., rząd powoła radę, która omawiać będzie promocję środków bezpieczeństwa cybernetycznego. Rada będzie składać się z krajowych agencji rządowych, samorządów lokalnych, operatorów infrastruktury informacji krytycznej, podmiotów gospodarczych związanych z cyberprzestrzenią oraz instytucji

[58] W Strategii odniesiono się do poprzednich igrzysk olimpijskich/paraolimpijskich, doniesiono, że podczas igrzysk w Londynie w 2012 r. Miała miejsce ogromna liczba cyberataków, choć nie miały one wpływu na przebieg imprezy. Podobnie, według niektórych raportów, znaczna liczba cyberataków spowodowała szkody w grach Rio de Janeiro 2016 i Pyeongchang 2018. Ibidem, s. 32.

[59] Ibidem.

[60] Act No. 91, 2018 r.

edukacyjnych i badawczych. Ponadto znowelizowana ustawa umożliwi Centrali Strategicznej ds. Cyberbezpieczeństwa delegowanie części swoich funkcji na zamówienie gabinetu takim podmiotom, jak Agencja Promocji Technologii Informacyjnych. Funkcje, które mają zostać przekazane, obejmują ustanowienie standardów dla środków bezpieczeństwa cybernetycznego dla krajowych organów administracyjnych; promowanie wdrażania środków oceny, w tym audytów; oraz koordynacja z odpowiednimi osobami i podmiotami w Japonii i za granicą w przypadku naruszenia bezpieczeństwa cybernetycznego i zagrożeń[61].

V. Podsumowanie

Liczne ataki hakerskie na japońską administrację i agencje rządowe stały się impulsem do wieloetapowego i wielostronnego budowania systemu cyberbezpieczeństwa. W wypracowaniu tych założeń uwzględniano sytuację międzynarodową i realizację umów międzynarodowych[62]. Wszystkie wysiłki zostały skupione na stworzeniu ochrony, która zabezpieczyłaby przeprowadzenie igrzysk olimpijskich w Tokio w 2020 r. Jest to wzywanie, które obserwuje świat i wnioski, jakie zostaną wyciągnięte z przeprowadzenia tego wydarzenia są niedoprzeceniania dla całej społeczności międzynarodowej.

Początkowa opieszałość legislacyjna rządu japońskiego spowodowała wzmożone prace nad podstawą prawną działania systemu. Zidentyfikowanie zagrożeń przyczyniło się do budowy rozwiązań cywilnych i wojskowych, czego skutkiem było

[61] S. Umeda, *Japan: Basic Act on Cybersecurity Amended*, https://www.loc.gov/law/foreign-news/article/japan-basic-act-on-cybersecurity-amended/ [dostęp: 17.12.2019].

[62] Szerzej na temat polityki międzynarodowej w zakresie cyberbezpieczeństwa zob. P. Soja, op.cit., s. 296–300.

uznanie cyberbezpieczeństwa jako dziedziny bezpieczeństwa narodowego.

Jak wspomniano przełomem w realizacji zadań w zakresie cyberbezpieczeństwa było powołanie NCIS. Zarówno podstawowa ustawa o cyberbezpieczenstwie, jak i strategie cyberbezpieczeństwa z lat 2015 i 2018 podkreśliły jego szczególną rolę, jako ogniwa, która kreuje, koordynuje i nadzoruje całą politykę Japonii w zakresie cyberbezpeczeństwa. Jak zaznaczono w Strategii z 2018 r. oczekiwania w zakresie realizacji są jeszcze większe. Oprócz mechanizmów instytucjonalnych, stworzono cały system podnoszenia świadomości społecznej, inwestycji w wyspecjalizowane kadry i współpracy międzysektorowej oraz współpracy ze środkami naukowo-badawczymi.

Bibliografia

Act on the Protection of Specially Designated Secrets, No. 108, http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=2&dn=1&x=42&y=6&co=01&ia=03&ja=04&ky=protection+of+specially+designated+secrets&page=16.

Cyber Security Strategy 2018, https://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf.

Cybersecurity Strategy. Towards a world-leading, resilient and vigorous cyberspace, https://www.nisc.go.jp/eng/pdf/cybersecuritystrategy-en.pdf.

Defense of Japan 2019, https://www.mod.go.jp/e/publ/w_paper/pdf/2019/DOJ2019_Full.pdf.

Guideline for Establishing Safety Principles for Ensuring Information Security of Critical Infrastructure (5th Edition), https://www.nisc.go.jp/eng/pdf/principles_ci_eng_v5.pdf.

Jakubczak W., Konopka A., *Strategie bezpieczeństwa w globalizujący się świecie*, Gdańsk 2012.

Kallender P., Hughes Ch.W., *Japan's Emerging Trajectory as a "Cyber Power": From securitization to Militarization at Cyberspace*, „Journal of Strategic Studies" 2017, Vol. 40, Issue 1–2.

Kallender P., *Japan, the Ministry of Defense and Cyber-Security: Progress and Pitfalls*, „The RUSI Journal" 2014, Vol. 159, Issue 1.

Konstytucja Japonii z 3 listopada 1946 r., tłum. T. Suzuki, https://www.pl.emb-japan.go.jp/relations/konstytucja.htm.

Soja P., *Cyberbezpieczeństwo Japonii w XXI w.*, „Rocznik Bezpieczeństwa Międzynarodowego" 2017, vol. 11, nr 1.

The Basic Act on Cybersecurity, Act No. 104, 12.11.2014, http://www.japaneselawtranslation.go.jp/law/detail/?ft=1&re=2&dn=1&x=0&y=0&co=01&ia=03&ja=04&ky=cyber+security&page=3.

The Second National Strategy on Information Security, https://www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf.

Umeda S., *Japan: Basic Act on Cybersecurity Amended*, https://www.loc.gov/law/foreign-news/article/japan-basic-act-on-cybersecurity-amended/.

Abstrakt

Początkowa opieszałość legislacyjna rządu japońskiego spowodowała wzmożone prace nad podstawą prawną działania systemu. Zidentyfikowanie zagrożeń przyczyniło się do budowy rozwiązań cywilnych i wojskowych, czego skutkiem było uznanie cyberbezpieczeństwa za dziedzinę bezpieczeństwa narodowego. Liczne ataki hakerskie na japońską administrację i agencje rządowe stały się impulsem do wieloetapowego i wielostronnego budowania systemu cyberbezpieczeństwa. W wypracowaniu tych założeń uwzględniano sytuację międzynarodową i realizację umów międzynarodowych. Wszystkie wysiłki zostały skupione na stworzeniu ochrony, która zabezpieczyłaby przeprowadzenie igrzysk olimpijskich w Tokio w 2020 r. Celem artykułu jest przedstawie-

nie prawnych podstaw działania systemu cyberbezpieczeństwa Japonii i wypracowanych na tej podstawie rozwiązań administracyjnych.

Słowa kluczowe: system cyberbezpieczeństwa Japonii, cyberprzestrzeń Japonii, strategia cyberbezpieczeństwa Japonii

Abstract

The initial legislative sluggishness of the Japanese government has intensified work on the legal basis for the system. Identification of threats contributed to the construction of civil and military solutions, which resulted in the recognition of cyber security as a field of national security. Numerous hacker attacks on Japanese administration and government agencies have become an impulse for a multi-stage and multilateral building of a cyber security system. The elaboration of these assumptions took into account the international situation and the implementation of international agreements. All efforts have been focused on creating protection that would secure the Olympic Games in Tokyo in 2020. The purpose of the article is to present the legal basis of Japan's cybersecurity system and administrative solutions developed on this basis.

Keywords: Japan's cybersecurity system, Japan's cyberspace, Japan's cybersecurity strategy

Filip Radoniewicz
Akademia Sztuki Wojennej
ORCID ID: https://orcid.org/0000-0002-7917-4059

Przestępstwa przeciwko danym oraz systemom komputerowym w japońskim prawie karnym

Uwagi wprowadzające

Przedmiotem niniejszego opracowania są przestępstwa przeciwko danym komputerowym oraz systemom komputerowym w japońskim prawie karnym. Na wstępie konieczne jest zatem wyjaśnienie, jakie czyny zabronione zaliczane są do tej grupy.

W doktrynie przestępstwa komputerowe (cyberprzestępstwa) dzieli się zwykle na trzy grupy – te czyny, w których:

1) komputer, dane komputerowe lub sieć są celem przestępstwa (niejako „ofiarą"; *computer as a target*), inaczej po prostu *computer crimes*, np. hacking, podsłuch komputerowy, zakłócanie pracy sieci – właśnie te przestępstwa są przedmiotem niniejszego artykułu;
2) komputer lub sieć są narzędziem przestępstwa (*computer as an instrument or* a *tool*), inaczej *computer related crimes*, np. rozpowszechnianie pornografii dziecięcej, oszustwo[1];

[1] Często spotykane jest rozbicie tej kategorii na dwie grupy: *computer assisted (related) crimes* – przestępstwa związane z użyciem komputera, takie jak oszustwo komputerowe oraz *computer content crimes* – cyberprzestępstwa związane z treścią przetwarzanej informacji, takie jak np. rozpowszechnianie pornografii dziecięcej. Zob. np. B.J. Koops, T. Robinson, *Cybercrime Law: A European Perspective*, [w:] *Digital Evidence and Computer Crime* red. E. Casey, Waltham–San Diego–London 2011 s. 130–133; D. Wall, *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013, s. 49–50.

3) komputer lub sieć mogą być użyte do zadań dodatkowych, związanych z popełnieniem przestępstwa, np. do przechowywania danych o nielegalnej sprzedaży narkotyków[2].

Powyższa klasyfikacja przyjęta została również w Konwencji o cyberprzestępczości[3] – jedynej wielostronnej umowie międzynarodowej dotyczącej zwalczania przestępstw popełnianych za pośrednictwem Internetu oraz sieci komputerowych. Przestępstwa odpowiadające czynom zabronionym z pierwszej grupy zostały w niej zebrane w jednym tytule jako „Przestępstwa przeciwko poufności, integralności i dostępności danych komputerowych i systemów komputerowych" (rozdział II – „Środki, jakie należy podjąć na szczeblu krajowym", część l – „Prawo karne materialne")[4].

Przedmiotem niniejszego opracowania są zatem przestępstwa określone w Konwencji o cyberprzestępczości jako przestępstwa przeciwko poufności, integralności i dostępności danych komputerowych i systemów komputerowych, czyli tzw. przestępstwa komputerowe (cyberprzestępstwa) *sensu stricte*, tj. nielegalny dostęp (*hacking*), nielegalne przechwytywanie da-

---

[2] S. Brenner, [w:] *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime,* red. R.D. Clifford, Durham 2011, s. 17–20; J. Clough, *Principles of cybercrime*, New York 2013, s. 10; P. Grabosky, *Electronic Crime*, New Jersey 2006, s. 11; F. Radoniewicz, *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016, s. 119–127.

[3] Konwencja Rady Europy o cyberprzestępczości, otwarta do podpisu w Budapeszcie dnia 23 listopada 2001 r. (Dz.U. 2015, poz. 728).

[4] Przestępstwa z drugiej grupy znalazły się w trzech kolejnych tytułach tego rozdziału: „Przestępstwa związane z komputerami" (fałszerstwo komputerowe i oszustwo komputerowe), „Przestępstwa związane z treścią" (przestępstwa dotyczące pornografii dziecięcej) oraz „Przestępstwa związane z naruszeniem praw autorskich i praw pokrewnych". Ostatnia grupa z przytoczonej klasyfikacji nie jest przedmiotem zainteresowania prawa karnego materialnego, ale raczej procesowego, a zwłaszcza dowodowego. Zob. też A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, s. 34–35.

nych (podsłuch komputerowy), naruszenie integralności danych, naruszenie integralności systemu, tzw. niewłaściwe użycie urządzeń, tj. czyny dotyczące tzw. narzędzi hackerskich[5].

Na zakończenie części wstępnej – przed przejściem do omówienia cyberprzestępstw w japońskim prawie karnym – należy zwrócić uwagę jeszcze na dwie kwestie. Po pierwsze, japońskie prawo karne czerpie z wzorców europejskich – z prawa niemieckiego. Pierwszy Kodeks karny z 1880 r. był oparty wprawdzie na francuskim Kodeksie karnym, jednak obecnie obowiązujący Kodeks karny (*Keihō*) z 1907 r. (ustawa nr 45 z 24 kwietnia 1907 r.[6], dalej jako k.k.) czerpie ze wzorców niemieckich[7].

Po drugie, przedstawiciele Japonii uczestniczyli – obok reprezentantów Kanady i Stanów Zjednoczonych – w charakterze obserwatorów (jako państwa spoza Rady Europy) w pracach nad Konwencją o cyberprzestępczości. Co więcej – Japonia podpisała Konwencję natychmiast – w dniu otwarcia jej do podpisu, ale ratyfikowała dopiero 3 lipca 2012 r. (jej postanowienia weszły

---

[5] W prawie polskim przestępstwa te są stypizowane w przepisach art. 267–269b Kodeksu karnego (ustawa z dnia 6 czerwca 1997 r. Kodeks karny – t.j. Dz.U. 2019, poz. 1950 z późn. zm.) w rozdziale XXXIII „Przestępstwa przeciwko ochronie informacji".

[6] Teksty wielu japońskich aktów prawnych (w tym omawianych w niniejszej publikacji) są dostępne w oficjalnym serwisie Japanese Law Translation Database, http://www.japaneselawtranslation.go.jp/law/detail/?id=3390&vm=04&re=02 [dostęp: 31.12.2019]. Z informacji w nim zamieszczonych wynika, że teksty aktów prawnych w nim umieszczonych mogą być cytowane i powielane Nie mają jednak charakteru oficjalnego. Rząd Japonii nie ponosi odpowiedzialności za dokładność, wiarygodność ani aktualność materiałów umieszczonych na stronach serwisu. Ponadto teksty aktów prawnych, zawierające w tytule pojęcie „wstępne tłumaczenie" („*tentative translation*"), nie zostały jeszcze poprawione ani poprawione przez native speakera języka angielskiego lub eksperta w dziedzinie tłumaczeń prawniczych.

[7] Zob. szerzej: J. Izydorczyk, *Japoński kodeks karny,* „Prokuratura i Prawo" 2008, nr 5, s. 131–132; M. Majewska, *Specyfika prawa karnego w Japonii,* [w:] *Prawo i kultura we współczesnej Japonii*, red. J. Marszałek-Kawa, M. Bidziński, Toruń 2018, s. 57–59; J. Widacki, *Przestępczość i wymiar sprawiedliwości karnej w Japonii*, Lublin 1990, s. 113–114.

w życie wobec Japonii 1 listopada 2012 r.). Oznacza to, że interpretując przepisy japońskie sięgać należy do tekstu Konwencji o cyberprzestępczości.

Kodeks karny

W rozdziale XIXbis Kodeksu karnego („Przestępstwa związane z elektronicznymi lub magnetycznymi zapisami oraz nieuprawnionymi rozkazami") zgrupowano przestępstwa dotyczące tzw. narzędzi hackerskich, np. trojanów, wirusów, exploitów[8]. Ustawodawca japoński posłużył się dla ich określenia pojęciem zapisu elektronicznego lub magnetycznego, przez które należy rozumieć każdy zapis, który został wytworzony za pomocą elektronicznych, magnetycznych lub innych środków nieroz-

[8] Trojany (konie trojańskie) są to nieszkodliwe na pierwszy rzut oka programy, w których zapisano dodatkowe instrukcje. Wykonują one działania, o których użytkownik nie wie. Służą one hackerom do obejścia zabezpieczeń systemu. Po zainstalowaniu trojana hacker może uzyskiwać dostęp do danych. Ponadto sam trojan może wykonywać pewne czynności, takie jak usuwanie lub modyfikacja danych, przesyłanie plików do napastnika. Trojany często zamaskowane są jako nieszkodliwe programy (np. wygaszacze ekranu), czy jako skrypty wykonywalne na witrynach internetowych. Exploity (programy służące do wykorzystania luk w oprogramowaniu, których wykorzystanie umożliwia sprawcy zakłócenie pracy sieci, a nawet uzyskanie nieuprawnionego dostępu do działających w jej ramach komputerów). Wirusy – programy instalujące się bez wiedzy i zgody użytkownika, wykonujące różne działania, które mogą polegać na zakłócaniu pracy systemu, np. wyświetlają różne komunikaty lub na niszczeniu danych; mogą się replikować własny kod oraz atakować inne komputery – czy to poprzez zapisywanie się na fizycznych nośnikach, na których są potem przenoszone przez użytkowników czy przez sieć, przesyłając się jako załączniki do e-maili). Programy te zaliczane są do kategorii tzw. *malware* (jest to skrót od *malicious software* – oprogramowanie złośliwe). Ponadto do tej grupy zalicza się m.in. programy typu *spyware* – przesyłające swojemu producentowi dane zebrane w komputerze użytkownika (np. dane osobowe, numery kart płatniczych, hasła, adresy odwiedzanych stron internetowych) czy tzw. oprogramowanie szantażujące (*ransomware*) blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych, a następnie żąda okupu za przywrócenie stanu pierwotnego.

poznawalnych przez naturalne funkcje percepcyjne człowieka i jest wykorzystywany do przetwarzania danych przez komputer (art. 7bis § 1 k.k.). Z tej niezbyt precyzyjnej definicji wynika, że pod pojęciem zapisu należy rozumieć dane komputerowe przetwarzane w systemie komputerowym, pod każdą ich postacią, czyli w formie zapisu magnetycznego (np. na magnetycznym dysku twardym – *hard disk drive* – *hdd*), elektronicznego (elektrycznego; np. impulsów elektrycznych przesyłanych siecią) lub inną (w tym nieznaną obecnie), która jest „zrozumiała" dla systemów komputerowych (np. komputerów, urządzeń sieciowych, smartfonów itd., zob. dalsze uwagi) i może być przez nie w tej formie przetwarzana, a jednocześnie nie podlega percepcji zmysłowej człowieka. Należy pamiętać, że pod pojęciem danych komputerowych (ang. *computer data*[9]) – w świetle ratyfikowanej przez Japonię Konwencji o cyberprzestępczości, należy rozumieć dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system komputerowy. Użycie pojęcia „forma właściwa do przetwarzania w systemie komputerowym" oznacza, że dane komputerowe są nośnikiem czy też medium informacji (faktów czy koncepcji), które dopiero sprowadzone do postaci danych komputerowych są czytelne dla systemu komputerowego. Co istotne – w świetle tej definicji danymi komputerowymi są też programy odpowiadające za wykonywanie funkcji przez system komputerowy. Za program komputerowy powszechnie uważa się zbiór instrukcji (rozkazów, poleceń), wyrażonych w postaci zrozumiałej dla komputera (słowami, symbolami matematycznymi, znakami graficznymi) i mający na

[9] W polskim Kodeksie karnym oraz w polskim tłumaczeniu Konwencji o cyberprzestępczości posłużono się pojęciem danych informatycznych, ale powszechnie uważa się, że jest ono równoznaczne z „danymi komputerowymi".

celu wywołanie zamierzonych przez twórcę programu działań systemu komputerowego, prowadzących do osiągnięcia określonego rezultatu[10].

Program komputerowy występuje w dwóch zasadniczych formach – w postaci kodu źródłowego (ang. *source code*) zapisanego w języku programowania oraz kodu wynikowego (ang. *object code*), będącego rezultatem procesu kompilacji programu komputerowego z kodu źródłowego do postaci „zrozumiałej" dla komputera[11].

W świetle Konwencji o cyberprzestępczości systemem komputerowym (ang. *computer system*)[12] jest każde urządzenie

---

[10] Por. P. Adamczewski, *Słownik informatyczny*, Gliwice 2005, s. 180; B. Pfaffenbergen, *Słownik terminów komputerowych*, Warszawa 1999, s. 236; J. Woodcock, *Microsoft. Encyklopedia komputerowa*, Warszawa 2002, s. 416.

[11] W tym celu dane komputerowe zapisywane są w języku binarnym (zwanym też językiem maszynowym czy kodem maszynowym) w systemie dwójkowym, czyli w postaci ciągów „0" i „1".

[12] Wskazać w tym miejscu należy, że w dyrektywie Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW (Dz.Urz. UE L 218 z 14.08.2013 r., s. 8), a wcześniej w decyzji ramowej Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne (Dz.Urz. UE L 69 z 16.03.2005 r., s. 67), posłużono się pojęciem na pozór zbliżonym, a mianowicie „systemem informatycznym" (ang. *information system*), zdefiniowanym jako urządzenie lub grupa wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, dokonuje automatycznego przetwarzania danych komputerowych, jak również danych komputerowych przechowywanych, przetwarzanych, odzyskanych lub przekazanych przez to urządzenie lub tę grupę urządzeń, w celach ich eksploatacji, użycia, ochrony lub utrzymania (art. 2 lit. a dyrektywy 2013/40 oraz art. 1 lit. a decyzji ramowej 2005/222). Powyższa definicja ma szeroki – w porównaniu do podobnie brzmiącej definicji „systemu komputerowego" z Konwencji o cyberprzestępczości, przez który – jak wskazano wyżej – rozumie się pojedynczy host (urządzenie podłączone do sieci komputerowej, np. komputer, smartfon, router, serwer) – zakres przedmiotowy. Pod pojęciem systemu informatycznego należy bowiem rozumieć zarówno pojedyncze urządzenie, jak i sieć komputerową (np. sieć LAN – ang. *local area network*). Dlatego błędem jest posłużenie się w polskim tłumaczeniu Konwencji o cyberprzestępczości pojęciem „system informatyczny" zamiast „system komputerowy". Z uwagi na ograniczenia

lub grupa wzajemnie połączonych lub powiązanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne (tj. odbywające się w całości lub częściowo za pomocą zautomatyzowanych środków, czyli bez ingerencji człowieka) przetwarzanie danych.

Zgodnie z *Explanatory Report to Convention on Cybercrime*[13] (dalej jako *Explanatory Report*) system komputerowy jest to urządzenie, na które składa się *hardware* (sprzęt) oraz *software* (programy). Na sprzęt składają się w szczególności urządzenia wejścia/wyjścia oraz magazynujące dane. Programem komputerowym – jak była mowa wyżej – jest zestaw instrukcji, które mogą być wykonane w celu osiągnięcia zamierzonego rezultatu przez system komputerowy. System komputerowy składa się zazwyczaj z wielu urządzeń. Niezbędnym elementem jest procesor. Pozostałymi „nieobligatoryjnymi" składnikami są urządzenia peryferyjne (czyli urządzenia, które wykonują określone zadania, wchodząc w interakcje z jednostką centralną, będzie to np. monitor, drukarka, napęd DVD, urządzenie magazynujące dane itp.). Systemem komputerowym w świetle Konwencji o cyberprzestępczości będzie zatem telefon komórkowy, dekoder, a przede wszystkim to, co potocznie rozumie się jako samodzielny komputer osobisty (PC – ang. *personal computer*), czyli pojedynczy host. Natomiast co najmniej dwie niezależne, powiązane ze sobą (tj. zdolne do wymieniania między sobą danych) systemy komputerowe będą stanowiły sieć. Typizując cyberprzestęp-

objętościowe niniejszego opracowania, szczegółowe rozważania tej kwestii zostaną pominięte. Zob. szerzej: F. Radoniewicz, *Odpowiedzialność*..., op.cit., s. 244–249.

[13] Komentarz do Konwencji o cyberprzestępczości (*Explanatory Report to Convention on Cybercrime*) – komentarz sporządzony do Konwencji o cyberprzestępczości przez jej autorów. Nie stanowi on wykładni autentycznej (co podkreślono w jego pkt. II, wskazując jednocześnie, że może „służyć pomocą przy stosowaniu postanowień Konwencji o cyberprzestępczości"). Jego tekst jest dostępny na stronach Rady Europy pod adresem, http://conventions.coe.int/Treaty/en/Reports/Html/185.htm [dostęp: 31.12.2019].

stwa ustawodawca japoński nie posługuje się pojęciem systemu komputerowego, ale po prostu komputera, nie używa również pojęcia sieci, ale linii telekomunikacyjnej, do której podłączony jest komputer.

Przechodząc do prezentacji przestępstw z rozdziału XXbis należy zwrócić uwagę, że nie użyto dla tych szkodliwych „zapisów" żadnej specjalnej nazwy (umownie nazywać je można narzędziami hackerskimi), poprzestając na ich opisie – zgodnie z art. 168bis § 1 k.k. zakazane jest tworzenie lub udostępnianie bez uzasadnionych podstaw w celu wykorzystania ich do wykonywania poleceń na komputerze innej osoby:

1) zapisów elektronicznych lub magnetycznych, które wydają nieautoryzowane polecenia w celu uniemożliwienia komputerowi wykonywania funkcji zgodnie z intencją użytkownika lub umożliwienia mu wykonywania funkcji wbrew woli użytkownika (czyli programy komputerowe w postaci);
2) zapisów, w tym zapisów elektronicznych lub magnetycznych, w których opisano nieautoryzowane polecenia, o których mowa wyżej (czyli programy komputerowe w postaci kodu źródłowego[14]).

Sprawca tego czynu podlega karze pozbawienia wolności z obowiązkiem pracy na nie więcej niż 3 lata lub grzywny w wysokości nie wyższej niż 500 tys. jenów[15].

---

[14] Wydaje się, że za formę zapisu można uznać również np. tzw. schemat blokowy (ang. *flow charts*, inaczej – graficzna sieć działań), czyli graficzny sposób zapisania algorytmu przed sporządzeniem kodu źródłowego. Na jego podstawie kod programu może stworzyć osoba inna niż autor. Zob. F. Radoniewicz, *Ochrona programów komputerowych w prawie UE (cz. I)*, „Europejski Przegląd Sadowy" 2009, nr 3, s. 25–26.

[15] 100 jenów (JPY) to – wg kursu średniego NBP na dzień 31 grudnia 2019 r. – 3,4923 zł. Japoński Kodeks karny przewiduje następujące kary: karę śmierci jako karę główną, karę pozbawienia wolności – dożywotniego lub karę „terminową" wysokości od miesiąca do 20 lat, występującą w dwóch postaciach – z obowiązkiem pracy (jest ona zasadą – w Kodeksie karnym

Identyczną sankcję przewidziano za korzystanie uprawnienia z zapisów elektronicznych lub magnetycznych określonych w punkcie w art. 168bis § 2 k.k. do wykonywania poleceń na komputerze innej osoby. Usiłowanie obu opisanych wyżej czynów zabronionych jest karalne (art. 168bis § 3 k.k.)[16].

W świetle japońskiego prawa karalne jest również nabywanie lub posiadanie narzędzi hackerskich (zarówno w postaci wykonywalnej, jak i w formie „zapisów, w których je opisano"). Warunkami odpowiedzialności karnej jest brak uzasadnionych podstaw ku temu oraz zamiar wykorzystania ich do wykonywania poleceń na komputerze innej osoby, a grożącą karą – pozbawienie wolności z obowiązkiem pracy na nie więcej niż 2 lata lub grzywna w wysokości nie wyższej niż 300 tys. jenów.

Kolejny przepis typizujący cyberprzestępstwo z omawianej w niniejszej publikacji grupy to określający przestępstwo tzw. sabotażu komputerowego art. 234bis k.k., umiejscowiony w rozdziale XXXV „Przestępstwa przeciwko działalności kredytowej i gospodarczej". Zgodnie z jego treścią karze do pięciu lat pozbawienia wolności z obowiązkiem pracy lub

posłużenie się pojęciem „kary pozbawienia wolności" bez dookreślenia czy jest ona z obowiązkiem pracy, czy bez, oznacza, że jest to jej forma z obowiązkiem pracy, w przypadku innych ustaw – doprecyzowuje się tę kwestię) oraz bez niego, karę grzywny (nie niższą niż 10 tys. jenów), karę aresztu (od 1 do 30 dni; bez obowiązku pracy) oraz drobnej grzywny (od 1000 do 10 tys. jenów), a także konfiskatę jako karę dodatkową (art. 9–15 k.k.). Przy okazji należy poczynić jedną uwagę. Otóż w prawie japońskim nie ma podziału na przestępstwa i wykroczenia. Wyróżnia się tzw. czyny drobne, które *de facto* odpowiadają wykroczeniom. Grozi za nie kara aresztu lub drobnej grzywny. Uregulowane są one w Keihanzaihō (Minor Offences Law No. 39, 1948) (Por. J. Izydorczyk, *Japoński*..., op.cit., s. 136; J. Widacki, *Przestępczość*..., op.cit., s. 115–116).

[16] Zgodnie z art. 44 k.k. usiłowanie jest karalne jedynie, gdy ustawa tak stanowi. Kara za usiłowanie wymierzana jest w granicach zagrożenia przewidzianego dla danego przestępstwa, z tymże może zostać zredukowana. W przypadku jednak, gdy sprawca dobrowolnie odstąpił od popełnienia przestępstwa redukcja kary jest obligatoryjna, co więcej – sprawca może zostać nawet uniewinniony (art. 43 k.k.). Przygotowanie jest niekaralne.

grzywny nie wyższej niż 1 mln jenów podlega sprawca, który utrudnia prowadzenie działalności gospodarczej osobie trzeciej przez zakłócenie funkcjonowania komputera używanego do prowadzenia działalności lub poprzez spowodowanie jego funkcjonowania niezgodnie z celem, do jakiego jest używany, przez jego uszkodzenie bądź uszkodzenie zapisu elektromagnetycznego (czyli danych komputerowych, w tym programu komputerowego), z którego ów komputer korzysta, poprzez wprowadzenie fałszywych danych lub nieuprawnione wydanie komend lub w jakikolwiek inny sposób.

W rozdziale XL „Przestępstwa uszkodzenia mienia oraz zatajenia dokumentów" zawarto dwa przestępstwa komputerowe. Zgodnie z art. 258 k.k. kto uszkadza dokument[17] lub zapis elektromagnetyczny używany przez urząd publiczny[18] (czyli o charakterze publicznym) podlega karze pozbawienia wolności z obowiązkiem pracy przez okres od 3 miesięcy do 7 lat. Natomiast w art. 259 k.k. przewidziano odpowiedzialność za taki czyn skierowany przeciwko dokumentowi lub zapisowi elektromagnetycznemu, z którym związane są prawa i obowiązki, należący do innej osoby. Grożąca sprawcy sankcja jest oczywiście mniej surowa – kara pozbawienia wolności z obowiązkiem pracy do 5 lat.

---

[17] Termin „dokument" nie został zdefiniowany w Kodeksie. W świetle utrwalonych poglądów judykatury jespońskiej jest to „wyrażenie lub oświadczenie woli lub zamiaru wyrażone w formie liter albo innych znaków". M. Yanaga, *Japan. Part VII. Computer Related Crime,* [w:] *International Encyclopaedia of Laws*, vol. 3: *Cyber Law – Supplement 2004,* red. J. Dumortier, Boston 2004, s. 195).

[18] Zgodnie z art. 7 § 2 k.k. „urząd publiczny" oznacza urząd, w którym funkcjonariusz publiczny wykonuje swoje obowiązki. Natomiast funkcjonariuszem publicznym – stosownie do art. 7 § 1 k.k. – jest funkcjonariusz administracji rządowej lub lokalnej, członek zgromadzenia lub komitetu, a także każdy pracownik zaangażowany w wykonywanie publicznych obowiązków na podstawie obowiązujących przepisów.

Ustawa nr 128 o zakazie nieuprawnionego dostępu („UCAL")

Przestępstwa komputerowe przeciwko danym i systemom komputerowym stypizowane są nie tylko w Kodeksie karnym, ale w szeregu innych ustaw, wśród których przede wszystkim wskazać należy ustawę nr 128 z 13 sierpnia 1999 r. o zakazie nieuprawnionego dostępu (Act on the Prohibition of Unauthorized Computer Access, poprzednia nazwa Unauthorized Computer Access Law – „UCAL", mimo zmiany nazwy ustawy w powszechnym użyciu pozostał poprzedni skrót).

W ustawie nr 128 o zakazie nieuprawnionego dostępu skryminalizowano czyny zabronione polegające na uzyskaniu nielegalnego dostępu do komputera, czyli tzw. hackingu. W art. 1 UCAL, będącym w zasadzie preambułą, wskazano, że jej celem jest zapobieganie przestępstwom związanym z komputerami popełnianym za pośrednictwem sieci telekomunikacyjnych i utrzymywanie bezpieczeństwa przetwarzania danych w sieciach telekomunikacyjnych (czemu służyć ma funkcja kontroli dostępu) poprzez zakazanie czynów nieautoryzowanego dostępu do komputera i określeniu kar za nie oraz ustanowieniem instytucji środków pomocowych podejmowanych przez Prefekturalną Komisję ds. Bezpieczeństwa Publicznego, mających służyć zapobieżeniu ponownego wystąpienia takich incydentów, przyczyniając się tym samym do prawidłowego rozwoju zaawansowanego społeczeństwa informacyjnego i telekomunikacyjnego.

Zanim jednak będzie można przystąpić do omówienia przestępstw stypizowanych w UCAL, niezbędne jest przytoczenie definicji pojęć, które ustawodawca japoński zamieścił w treści art. 2 ustawy.

Definicji samego uzyskania dostępu do komputera nie sformułowano, ale doktryna japońska odwołuje się w tej kwestii do

Konwencji o cyberprzestępczości[19]. Przez uzyskanie dostępu do systemu komputerowego należy rozumieć zdobycie możliwości korzystania z jego zasobów (czyli przechowywanych w nim danych oraz używanie sprzętu, co sprowadza się również do dostępu do danych – do oprogramowania nim sterującego) – używając języka potocznego – wejście do niego. Dla przypisania sprawcy odpowiedzialności nie ma znaczenia rodzaj sieci, za pośrednictwem której się włamuje – czyli uzyskuje nieuprawniony dostęp. Obojętne czy czyni to za pośrednictwem publicznej sieci telekomunikacyjnej, czy działając w ramach tej samej sieci, np. sieci LAN. Nie jest istotne również medium, którego w tym celu używa, np. naziemna sieć telekomunikacyjna, bezprzewodowa sieć mobilna czy Wi-Fi.

W doktrynie japońskiej wskazuje, że art. 2 UCAL jest jednym z najtrudniejszych przepisów w prawie japońskim. Nie jest to związane tylko z trudnością w jego przetłumaczeniu na język angielski. W rzeczywistości już oryginalny przepis w języku japońskim jest zbyt skomplikowany i pełen długich zdań, by być łatwym do zrozumienia nawet dla japońskich zawodowych prawników[20].

---

[19] Nie znajdziemy jej nigdzie, w żadnym ustawodawstwie, za wyjątkiem angielskiej ustawy o nadużyciach komputerowych z 1990 r. (Computer Misuse Act 1990; c. 18), gdzie zdefiniowano uzyskanie dostępu do programów lub danych jako sytuację, w której sprawca może spowodować wykonanie przez komputer ich zmiany, skasowania, skopiowania lub przeniesienia na inny nośnik (albo do innej lokalizacji w ramach tego samego nośnika), użycia ich bądź wygenerowania z komputera w formie danych wyjściowych (obojętne czy poprzez wyświetlenie na ekranie, czy w inny sposób). Zob. szerzej: F. Radoniewicz, *Odpowiedzialność...*, op.cit., s. 408 i n.

[20] T. Natsui, *Cybercrimes in Japan: recent cases, legislations, problems and perspectives*, s. 12, tekst jest dostępny pod adresem, https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjV8_Tm_NjmAhXHk4sKHcTGAfoQFjAAegQIBhAC&url=http%3A%2F%2Fcyberlaw.la.coocan.jp%2FDocuments%2Fnetsafepapers_takatonatsui_japan.pdf&usg=AOvVaw1uilzd3EA1RpBIq7ENKORC [dostęp: 31.12.2019].

Zgodnie z art. 2 § 1 UCAL pod pojęciem „administratora dostępu" należy rozumieć osobę, która zarządza działaniami komputera, podłączonego do linii telekomunikacyjnej (dalej jako „właściwy komputer"), w związku z jego użyciem (ograniczonym do operacji wykonywanych za pośrednictwem linii telekomunikacyjnej, dalej jako „właściwe użycie"). Karalne zatem jest tylko uzyskanie dostępu za pośrednictwem sieci telekomunikacyjnej, a nie poprzez np. uzyskanie fizycznego dostępu do komputera.

W art. 2 § 2 UCAL dla potrzeb ustawy przyjęto, że „kodem identyfikacyjnym" jest kod dostępu przyznany osobie (dalej jako „uprawniony użytkownik") upoważnionej przez administratora dostępu zarządzającego właściwym dostępem tego właściwego komputera, by mógł on dokonywać właściwego użycia tego właściwego komputera lub kod przyznany temu administratorowi (dalej jako „uprawniony użytkownik") w celu identyfikacji tego uprawnionego użytkownika oraz odróżnienia go od innego użytkownika.

W konkretnych warunkach może to być dowolny z poniższych kodów lub kombinacja któregokolwiek z poniższych kodów z innym kodem:

1) kod, taki jak login, którego treść nie może, zgodnie z instrukcjami administratora dostępu bez powodu zostać ujawniona stronie trzeciej;
2) kod, który został wygenerowany z obrazu całości lub części ciała upoważnionego użytkownika itp. lub jego głos użyty za pomocą metody określonej przez danego administratora dostępu (kod biometryczny);
3) inny kod uzyskany za pomocą metody określonej przez danego administratora dostępu, np. kod wygenerowany z podpisu autoryzowanego użytkownika. Innymi słowy – taki sposób identyfikacji, którego nie wskazał ustawodawca (może to być sposób autoryzacji nieznany obecnie).

Kolejnym zdefiniowanym w UCAL pojęciem (wprowadzonym zresztą dla potrzeb tej ustawy) jest „funkcja kontroli dostępu" rozumiana – w świetle 2 § 3 UCAL – jako funkcja dodana (przyznana) przez administratora zarządzającego właściwym użyciem, właściwemu komputerowi lub innemu właściwemu komputerowi połączonemu z tym pierwszym za pomocą linii telekomunikacyjnej, w celu automatycznej kontroli właściwego użycia tego właściwego komputera i usuwającego część lub wszystkie ograniczenia tego właściwego użycia po potwierdzeniu tego, iż kod wprowadzony przez osobę, która zamierza dokonać właściwego użycia jest kodem identyfikacyjnym dla tego właściwego użycia. Przepisami ustawy chroniony jest zatem tylko komputer zabezpieczony funkcją dostępu[21].

W przepisie art. 3 § 1 UCAL zakazano nieuprawnionego uzyskania dostępu, natomiast w treści art. 2 § 4 UCAL określono jakie zachowania mogą do tego prowadzić:

1) uczynienie dostępnym właściwego użycia zastrzeżonego przez funkcję kontroli dostępu poprzez wykonywanie działań we właściwym komputerze mającego tę funkcję kontroli dostępu, przez wprowadzenie do tego właściwego komputera za pośrednictwem linii telekomunikacyjnej kodu indentyfikacyjnego innej osoby powiązanego z daną funkcją kontroli dostępu (wyłączając z zakresu przedmiotowego tego czynu działania podejmowane przez administratora dostępu, który nadał funkcję kontroli dostępu oraz działania dokonane za zgodą tego administratora lub uprawnionego do tego kodu użytkownika);
2) uczynienia dostępnym właściwego użycia (wbrew ograniczeniom ku temu nałożonym funkcją kontroli dostępu) przez wykonanie operacji we właściwym komputerze przez wprowadzenie do niego za pośrednictwem

[21] Zob. szerzej: T. Natsui, *Cybercrimes*..., op.cit., s. 12 i n.; M. Yanaga, *Japan*..., op.cit., s. 199.

linii telekomunikacyjnej każdej informacji (z wyjątkiem kodu identyfikacyjnego) lub komendy, które mogą obejść ograniczenia nałożone przez funkcję kontroli dostępu na to właściwe użycie (z wyłączeniem takich działań dokonywanych przez administratora dostępu, który nadał tę funkcję kontroli dostępu lub użytkownika, który uzyskał pozwolenie tego administratora);

3) uczynienie dostępnym właściwego użycia przez wykonanie operacji we właściwym komputerze, którego właściwe użycie jest ograniczone przez funkcję automatycznego dostępu zainstalowaną na innym właściwym komputerze, połączonym linią telekomunikacyjną do tego właściwego komputera i tą linią telekomunikacyjną wprowadzane są informacje lub komendy, które mogą te ograniczenia obejść (z wyłączeniem takich działań dokonywanych przez administratora dostępu, który nadał tę funkcję kontroli dostępu lub użytkownika, który uzyskał pozwolenie tego administratora).

W art. 4 UCAL zakazano uzyskiwania cudzego kodu identyfikacyjnego powiązanego z funkcją kontroli dostępu w celu uzyskania dostępu do chronionego komputera.

Ustawa nr 128 o zakazie nieuprawnionego dostępu kryminalizuje również działania polegające na ułatwianiu nieuprawnionego dostępu. W treści art. 5 UCAL zakazano udostępniania – wyjąwszy wypadki, gdy istnieją ku temu podstawy prawne – kodu identyfikacyjnego związanego z funkcją automatycznego dostępu osobie trzeciej innej niż administrator dostępu właściwy dla tej funkcji automatycznego dostępu lub uprawniony do tego kodu inny użytkownik, z wyjątkiem sytuacji, gdy dokonuje tego administrator dostępu lub osoba przez niego upoważniona lub ten uprawniony użytkownik.

Zgodnie z art. 6 UCAL zabronione jest przechowywanie cudzego kodu identyfikacyjnego związanego z funkcją kontroli

dostępu, która została bezprawnie uzyskana w celu zaangażowania się w nieautoryzowany dostęp do komputera.

a) W UCAL dokonano kryminalizacji phishingu[22] w sposób niespotykany w innych ustawodawstwach karnych. Zgodnie z art. 7 jest to czyn zabroniony polegający na nielegalnym żądaniu wprowadzenia kodu identyfikacyjnego. W przepisie tym określono dwie jego formy, obie polegające na podszyciu się pod administratora dostępu bądź wywołania fałszywego wrażenia bycia administratorem dostępu (oczywiście nie dotyczy to sytuacji, gdy „prawdziwy" administrator udzielił sprawcy pozwolenia na takie zachowanie):

1) zwrócenie się za pośrednictwem publicznie dostępnej transmisji dokonywanej linią telekomunikacyjną do nieokreślonego kręgu podmiotów przez fałszywego administratora dostępu o podanie przez upoważnionego użytkownika kodu identyfikacyjnego, tj. np.

[22] Celem phishingu (zwykle wskazuje się, że termin ten pochodzi od ang. *password harvesting fishing* – łowienie haseł) jest uzyskanie poufnych danych poprzez podszywanie się pod podmioty i instytucje, zwykle znane i zaufane, takie jak banki, sklepy internetowe, serwisy aukcyjne, serwisy pocztowe. Zdarza się, że sprawca w celu uwiarygodnienia przesłanych e-maili fałszuje adresy źródłowe (stosuje IP spoofing). Nie jest to niezbędne, często wystarczą adresy specjalnie założonych kont, które będą się kojarzyć z daną instytucją, np. z bankiem. Phishing polega bowiem na masowym wysyłaniu e-maili kierujących na fałszywą stronę, łudząco przypominającą oryginalną, która w rzeczywistości przechwytuje informacje wpisywane przez użytkownika. Ilustracją może być sytuacja, gdy atakujący wysyła wiadomości e-mail z linkiem do stworzonej przez siebie strony imitującej stronę banku (niekoniecznie banku użytkownika – e-maile wysyłane są zwykle masowo – sprawca zakłada, że wśród adresatów będą klienci tego banku) z prośbą o zalogowanie w związku z wprowadzeniem nowych zabezpieczeń i związaną z tym koniecznością zmiany ustawień. W momencie próby zalogowania się przez nieświadomego użytkownika wpisywane przez niego dane (hasło, login oraz inne, o jakie zwróci się atakujący, np. hasło jednorazowe służącego do potwierdzenia operacji bankowych) trafiają do autora strony, który w ten sposób uzyskuje dostęp do konta w serwisie banku użytkownika. Zob. F. Radoniewicz, *Odpowiedzialność...*, op.cit., s. 107–108.

stworzenia fałszywej strony internetowej (np. serwisu banku), przy pomocy której fałszywy administrator żąda od uprawnionego użytkownika wprowadzenia na właściwym komputerze kodu identyfikacyjnego powiązanego z daną funkcją kontroli dostępu;

2) posłużenie się pocztą elektroniczną – przesłanie uprawnionemu użytkownikowi wiadomości e-mail, w której fałszywy administrator dostępu żąda od tego uprawnionego użytkownika wprowadzenia na właściwym komputerze kodu identyfikacyjnego powiązanego z daną funkcją kontroli dostępu.

Zgodnie z art. 11 UCAL sprawcy czynu zabronionego określonego w art. 3 grozi kara pozbawienia wolności z obowiązkiem pracy do trzech lat lub grzywny do 1 mln jenów. Natomiast za przestępstwo określone w art. 4, art. 5 (w przypadku, gdy sprawca wiedział, że odbiorca zamierza wykorzystać kod identyfikacyjny do popełnienia przestępstwa nieautoryzowanego dostępu do komputera), art. 6 oraz art. 7 UCAL kara pozbawienia wolności z obowiązkiem pracy do roku lub grzywny do 500 tys. jenów (art. 12 UCAL). Natomiast w przypadku, gdy sprawca czynu z art. 5 nie wiedział o zamiarach odbiorcy kodu – grozi mu kara grzywny do 300 tys. jenów (art. 13 UCAL).

Ustawa nr 86 o działalności telekomunikacyjnej (Telecommunication Business Act)

W prawie japońskim przestępstwo zwane potocznie podsłuchem komputerowym[23] – czyli nielegalne przechwytywanie

[23] Podsłuch komputerowy jest potocznym określeniem inwigilacji systemów informatycznych. Wyróżnia się dwa jego rodzaje: pasywny – gdy sprawca jedynie zapoznaje się z treścią informacji oraz aktywny – gdy dokonuje modyfikacji przesyłanych danych, np. poprzez przekierowanie ich transmisji do innego miejsca w sieci. Przykładem podsłuchu pasywnego jest

danych – stypizowane zostało w rozdziale VI ustawy nr 86 z 25 grudnia 1984 r. o działalności telekomunikacyjnej (*Telecommunication Business Act* – TBA). W świetle art. 179 § 1 TBA kara pozbawienia wolności do lat dwóch lub grzywny wysokości do 1 mln jenów grozi za naruszenie tajemnicy przekazu wykonywanego przez operatora telekomunikacyjnego. W następnym paragrafie przewidziano typ kwalifikowany tego czynu zabronionego. Znamieniem kwalifikującym jest cecha, jaką musi posiadać sprawca (jest to zatem przestępstwo indywidualne) – może się go dopuścić jedynie osoba spełniające wskazane w ustawie wymogi. W tym wypadku musi to być osoba zaangażowana w działalność telekomunikacyjną, czyli np. pracownik operatora telekomunikacyjnego. Grożącą sankcją jest kara pozbawienia wolności do lat trzech lub grzywna wysokości do 2 mln jenów. Usiłowanie wskazanych wyżej przestępstw jest karalne (art. 179 § 3 TBA). Ustawodawca japoński stypizował w omawianym rozdziale jeszcze jedno przestępstwo komputerowe, a mianowicie w art. 180 § 1 TBA, przewidującym karę nie dłuższą niż dwa lata lub grzywna w wysokości nie większej niż pięćset tysięcy jenów czyn polegający na korzystaniu bez uprawnienia z urządzeń telekomunikacyjnych wykorzystywanych do prowadzenia działalności przez operatora telekomunikacyjnego, jeżeli skutkiem jest zakłócenie świadczenia usług telekomunikacyjnych. Ta sama kara grozi sprawcy, będącemu osobą prowadzącą

sniffing, czyli przechwytywanie pakietów (w uproszczeniu: „porcji", na jakie dzielone są dane, by mogły zostać przesłane siecią). Przykładem podsłuchu aktywnego jest atak *man-in-the-middle* (czyli „człowiek pośrodku"), polegający – w znacznym uproszczeniu – na „wpięciu się" w trwającą transmisję danych między dwoma komputerami i niejako pośredniczeniu w procesie wymiany wiadomości między nimi. Sprawca przekierowuje bowiem zapytania wysyłane przez komputer ofiary (komputer „A") do komputera docelowego (komputer „B") do własnego komputera i dopiero z niego kieruje dane do komputera B. W rezultacie komunikacja między komputerem A a komputerem B przebiega przez komputer sprawcy, który ma w nią wgląd. Co więcej – może ją modyfikować. Zob. szerzej: ibidem, s. 89–97.

działalność telekomunikacyjną, która nie wykonuje, bez uzasadnionych podstaw, czynności związanych z utrzymaniem lub eksploatacją urządzeń telekomunikacyjnych wykorzystywanych do prowadzenia działalności telekomunikacyjnej przez operatora telekomunikacyjnego i tym samym powoduje utrudnienia w świadczeniu usług telekomunikacyjnych (art. 180 § 2 TBA). W przypadku obu czynów usiłowanie jest karalne (art. 180 § 3 TBA). Pozostałe przewidziane w tej ustawie przestępstwa mają charakter indywidualny – dopuścić się ich może jedynie np. przedsiębiorca prowadzący działalność telekomunikacyjną. W większości są to przestępstwa polegające na niedopełnieniu obowiązków nałożonych na te osoby przez ustawę, niemające charakteru przestępstw komputerowych.

Inne akty prawne

Na zakończenie warto wskazać, że przepisy typizujące przestępstwa komputerowe, których przedmiotem ochrony są dane komputerowe lub bezpieczne ich przetwarzanie znajdują się m.in. ustawie nr 47 z 19 maja 1993 r. o zapobieganiu nieuczciwej konkurencji (*Unfair Competition Prevention Act* – UCPA) oraz w ustawie nr 57 z 30 maja 2003 r. o ochronie informacji osobistych (*Act on the Protection of Personal Information* – APPI). Wszystkie przewidziane w tych ustawach czyny zabronione mają charakter indywidualny.

Podsumowanie

Dokonana powyżej pobieżna – z uwagi na ograniczenia objętościowe publikacji – analiza japońskich regulacji, których przedmiotem są przestępstwa komputerowe przeciwko danym i systemom komputerowym, pozwala na wyciągnięcie pew-

nych wniosków. Po pierwsze, przepisy kryminalizujące czyny zaliczane do tej kategorii są rozproszone po kilku aktach prawnych – przede wszystkim w Kodeksie karnym, a także w ustawie nr 128 o zakazie nieuprawnionego dostępu (w której stypizowano *hacking* i *phishing*) oraz w ustawie nr 86 o działalności telekomunikacyjnej (podsłuch komputerowy).

Ponadto przepisy kryminalizujące cyberprzestępstwa z tej grupy znajdują się w innych ustawach, np. w ustawie nr 47 o zapobieganiu nieuczciwej konkurencji oraz w ustawie nr 57 o ochronie informacji osobistych, co nie jest oczywiście niczym wyjątkowym, a wręcz przeciwnie – normą jest przecież umieszczanie przepisów karnych w aktach prawnych regulujących inne kwestie, zamiast umieszczać je w Kodeksie karnym.

Po drugie, ponieważ Japonia ratyfikowała Konwencję o cyberprzestępczości, do wykładni przepisów dotyczących przestępstw komputerowych można (a nawet trzeba) sięgać do jej postanowień.

Po trzecie, w związku z tym, że japońskie prawo karne czerpie z prawa niemieckiego, a ponadto Japonia ratyfikowała Konwencję o cyberprzestępczości, przepisy japońskie są w zasadzie zbliżone do europejskich. Wyjątek stanowi ustawa nr 128 o zakazie nieuprawnionego dostępu, będąca w pełni oryginalną regulacją japońską.

Bibliografia

Adamczewski P., *Słownik informatyczny*, Gliwice 2005.

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Brenner S., [w:] *Cybercrime. The Investigation, Prosecution and Defense of a Computer-related Crime*, red. R.D. Clifford, Durham 2011.

Clough J., *Principles of cybercrime*, New York 2013.

Explanatory Report to Convention on Cybercrime (Komentarz do Konwencji o cyberprzestępczości), http://conventions.coe.int/Treaty/en/Reports/Html/185.htm.

Grabosky P., *Electronic Crime*, New Jersey 2006.

Izydorczyk J., *Japoński kodeks karn*y, „Prokuratura i Prawo" 2008, nr 5.

Koops B.J., Robinson T., *Cybercrime Law: A European Perspective*, [w:] *Digital Evidence and Computer Crime. Forensic Science, Computers and the Internet*, red. E. Casey, Waltham–San Diego–London 2011.

Majewska M., *Specyfika prawa karnego w Japonii*, [w:] *Prawo i kultura we współczesnej Japonii*, red. J. Marszałek-Kawa, M. Bidziński, Toruń 2018.

Natsui T., *Cybercrimes in Japan: recent cases, legislations, problems and perspectives*, tekst jest dostępny pod adresem: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=2ahUKEwjV8_Tm_NjmAhXHk4sKHcTGAfoQFjAAegQIBhAC&url=http%3A%2F%2Fcyberlaw.la.coocan.jp%2FDocuments%2Fnetsafepapers_takatonatsui_japan.pdf&usg=AOvVaw1uilzd3EA1RpBIq7ENKORC.

Pfaffenbergen B., *Słownik terminów komputerowych*, Warszawa 1999.

Radoniewicz F., *Ochrona programów komputerowych w prawie UE (cz. I)*, „Europejski Przegląd Sadowy" 2009, nr 3.

Radoniewicz F., *Odpowiedzialność karna za hacking i inne przestępstwa przeciwko danym komputerowym i systemom informatycznym*, Warszawa 2016.

Wall D., *Cybercrime. The Transformation of Crime in the Information Age*, Malden 2013.

Widacki J., *Przestępczość i wymiar sprawiedliwości karnej w Japonii*, Lublin 1990.

Woodcock J., *Microsoft. Encyklopedia komputerowa*, Warszawa 2002.

Yanaga M., *Japan. Part VII. Computer Related Crime,* [w:] *International Encyclopaedia of Laws*, vol. 3: *Cyber Law – Supplement 2004,* red. J. Dumortier, Boston 2004.

Abstrakt

Przedmiotem artykułu są przestępstwa komputerowe skierowane przeciwko bezpieczeństwu danych komputerowych oraz systemów komputerowych – w Konwencji Rady Europy o cyberprzestępczości nazwane przestępstwami przeciwko poufności, integralności i dostępności danych informatycznych i systemów komputerowych. W japońskim prawie karnym uregulowane są w szeregu aktów prawnych. W związku z tym niniejszym artykule przedstawione są przepisy Kodeks karnego (*Keihō*) z 1907 r. (ustawa nr 45 z 1907 r.), ustawy nr 128 z 1999 r. o zakazie nieuprawnionego dostępu (*the Act on the Prohibition of Unauthorized Computer Access*) oraz ustawy o działalności telekomunikacyjnej ustawy nr 86 z 1984 r. o działalności telekomunikacyjnej (*the Telecommunication Business Act*).

Słowa kluczowe: cyberprzestępczość, *hacking*, oprogramowanie szkodliwe, nielegalne przechwytywanie danych, podsłuch komputerowy, *phishing*

Abstract

The subject of the article are computer crimes directed against the security of computer data and computer systems – in the Council of Europe Convention on Cybercrime, called Offences against the confidentiality, integrity and availability of computer data and systems. In Japanese criminal law they are regulated in a number of legal acts. Therefore, in this article, the provisions of the Penal Code (Act No 45 of 1907), the Act on the Prohibition of Unauthorized Computer Access (Act No. 128 of 1999; the "UCAL") and the Telecommunication Business Act Telecommunication Business Act (Act No. 86 of 1984; the "TBA") are presented.

Keywords: cybercrime, hacking, malware, illegal interception, phishing

Tadeusz Detyna
Uniwersytet Opolski
ORCID ID: https://orcid.org/0000-0003-1475-5511

Timor Wschodni – 20 lat nadziei i rozczarowań

Gdy byliśmy okupowani przez Indonezję,
było więcej biznesu. Teraz kryzys, mniej się dzieje.
Jest ciężko. Ale dobrze, że jesteśmy niepodlegli
Wypowiedź jednego z taksówkarzy[1]

Ogromne zapotrzebowanie na poprawę bytu sprawiło, że mieszkańcy terytoriów zależnych wiązali wielkie nadzieje z uzyskaniem lub odzyskaniem niepodległości swych państw zarówno w formalnym procesie dekolonizacji, jak i poza nim. Niepodległy byt państwowy, mający zerwać z kolonialnym wyzyskiem, lub wręcz terrorem, w wielu przypadkach przyniósł ogromne rozczarowanie, kojarząc się z bezprawiem, korupcją, nepotyzmem, nieudolnymi rządami, kolejnymi zamachami stanu, a nawet tyranią (Uganda, Gwinea Równikowa) czy wojną domową. Po latach mieszkańcy niektórych terytoriów uświadomili sobie też, że kolonizatorem nie musi być polityczny podmiot zamorski, lecz sąsiad, wcześniej aż tak negatywnie nie postrzegany. Zaowocowało to powstaniem niepodległej Erytrei, a po latach także niepodległego Sudanu Południowego – oczywiście po to, by mieszkańcom tych nowych państw żyło się lepiej. W tych przypadkach powszechnie wiadomo, że rozczarowanie jest

[1] M. Lenarcik, *Ciężkie życie w Timor-Leste*, Polityka Globalna.pl, http://www.politykaglobalna.pl/2009/11/ciezkie-zycie-w-timor-leste/ [dostęp: 27.11.2009].

ogromne, a perspektywy – przynajmniej krótkoterminowe – raczej beznadziejne. Jeszcze bardziej skomplikowana była droga do niepodległości Timoru Portugalskiego. Zanim mieszkańcy tego kraju mogli docenić korzyści płynące z niepodległego bytu czy też się rozczarować niepodległością, Indonezja – w zasadzie na prośbę USA, które obawiały się powstania kolejnego państwa rządzonego przez ruch komunistyczny – dokonała inwazji, inkorporując Timor Wschodni, co dla jego mieszkańców było zamianą jednego kolonizatora (zamorskiego) na innego (z najbliższego sąsiedztwa). I choć kwestia trwałej utraty niepodległości wydawała się przesądzona, krwawa walka partyzancka (z likwidacją „swoich" – uznanych za zdrajców – włącznie), naciski społeczności międzynarodowej, dotkliwy kryzys gospodarczy w regionie, przemiany polityczne w samej Indonezji – doprowadziły ostatecznie do referendum, którego wyniki oznaczały, że kraj ten stanie się pierwszym niepodległym państwem XXI w. Rozwój sytuacji pokazał, że tuż po zwycięskim referendum nastąpiła niewyobrażalna eskalacja przemocy, w wyniku której Timor Wschodni wszedł w niepodległość jako kraj zdewastowany infrastrukturalnie i demograficznie (tysiące zabitych oraz wielokrotnie więcej wypędzonych i uciekinierów). Nowa, trwała niepodległość rozpoczęła się od dramatu, a przecież nie takiego scenariusza spodziewali się głosujący za nią.

Mimo peryferyjności Timoru Wschodniego w polityce światowej, polskie zainteresowanie tym państwem nie jest marginalne. Należy tu docenić ogrom pracy wykonanej przez Łukasza Bonczola, której efektem jest jak dotąd jedyna książka prezentująca ten kraj „od reliktu kolonializmu do problemu międzynarodowego"[2]. Wydana w 2008 r., nie może obejmować wydarzeń z ostatnich jedenastu lat. Inną godną odnotowania pozycją jest *Dom nad rzeką Loes*. Nie jest to publikacja nauko-

[2] Jest to podtytuł książki Łukasza Bonczola, *Timor Wschodni*, Wrocław 2008.

wa, ale jej walory narracyjne sprawiają, że znakomicie przybliża polityczno-społeczno-kulturowy klimat Timoru Wschodniego – widziany oczami pracującego tam polskiego lekarza – oraz zmusza do krytycznej refleksji na temat „przemysłu humanitarnego"[3] czy to w ramach struktur ONZ, czy poza nimi. Polski czytelnik może też zapoznać się ze znakomicie zaprezentowaną analizą przeszkód związanych z drogą Timoru Wschodniego do członkostwa w ASEAN-ie – w naukowym artykule Pawła Soi[4]. Tekstów polskich poświęconych Timorowi Wschodniemu jest znacznie więcej; niektóre z nich zawierają informacje nieprawdziwe, na co także należy być wyczulonym w trakcie lektury.

Pierwsi biali (grupa Portugalczyków) przybyli na wyspę w 1511 r.[5] Dziesięć lat później jeden ze statków Magellana dopłynął do wybrzeży Timoru. Początek faktycznej władzy Portugalczyków datuje się jednak dopiero na 1676 r. Od XVII w. wyspa Timor była podzielona pomiędzy Holandię (część zachodnia) a Portugalię (część wschodnia). W połowie XVIII w. Holendrzy odbili większą część Timoru z rąk Portugalczyków. W 1859 r. utworzono granicę na Timorze; delimitację dopełniła konwencja z 1902 r. Pełną kontrolę nad wyspą Europejczycy zaczęli sprawować na początku XX w. Dopiero od 1912 r. można mówić o kontroli administracyjnej nad wnętrzem wyspy[6]. Przez wiele wieków strategicznym bogactwem Timoru było drewno

---

[3] M. Janiszewski, *Dom nad rzeką Loes*, Wołowiec 2014, s. 154.

[4] ASEAN jest integracyjnym stowarzyszeniem regionalnym, które aktualnie obejmuje wszystkie państwa Azji Południowo-Wschodniej – z wyjątkiem Timoru Wschodniego, co dobitnie świadczy o ekonomicznym, strukturalnym i kadrowym niedorozwoju tego kraju, a przecież wymogi stawiane państwom aspirującym do członkostwa w tej wspólnocie są zdecydowanie mniej restrykcyjne niż w przypadku Unii Europejskiej. Gospodarka Timoru Wschodniego po przyłączeniu do ASEAN-u miałaby wielkość zaledwie 15% najsłabszej gospodarki ugrupowania, czyli Laosu.

[5] Ł. Bonczol, op.cit., s. 15.

[6] W. Olszewski, *Timor Wschodni i jego problemy*, „Sprawy Narodowościowe" 1996, t. V, z. 1(8), s. 227.

sandałowe. W XIX w. jego miejsce już zdecydowanie zajęła kawa.

Plemiona timorskie przez wieki prowadziły wojny wewnętrzne. Miały też miejsce wojny o ziemię i wodę. Pokonanym ścinano głowy. Krwawe obrzędy miały charakter rytualny, inspirowany wierzeniami animistycznymi[7].

Timor Portugalski miał w parlamencie jednego posła, białego. Było normą, że taka osoba nigdy nie była w tej kolonii[8]. Podczas II wojny światowej Australia przy współudziale Holendrów pokojowo prewencyjnie zajęła Timor Portugalski, a od lutego 1942 r. do końca wojny był on pod okupacją japońską. W jej wyniku ok. 10% mieszkańców (ok. 40 tys.) straciło życie. Przeciwko okupantowi walczyli jako partyzanci m.in. Australijczycy, którzy nie zdołali się ewakuować[9].

Cechą charakterystyczną tej kolonii portugalskiej był niemal zupełny brak własnej elity politycznej. Od 1961 r. mieszkańcy posiadłości stali się *de iure* obywatelami Portugalii[10]. W tym *rezerwacie paleolitu* normą była gospodarka wypaleniskowa, tak fatalna z ekologicznego punktu widzenia. Rola pieniądza w gospodarce była niewielka nawet pod koniec panowania portugalskiego. Powszechny analfabetyzm (ponad 95%) i brak dostępu do czystej wody to kolejne wyznaczniki rzeczywistości Timoru Portugalskiego.

Zasadniczym podziałem społeczeństwa był podział na niewielkie plemiona. Faktycznie w 1975 r. chrześcijaństwo wyznawała tylko 1/3 ludności. Zdecydowanie dominował animizm. Timor Portugalski nie był dla Portugalczyków kolonią osadniczą. Jego atrakcyjność była wręcz żadna. W kolonii tej nie

[7] Ł. Bonczol, op.cit., s. 16–18.

[8] Ibidem, s. 27–28.

[9] Ibidem, s. 30–31.

[10] Ibidem, s. 33.

powstał typowy ruch komunistyczny[11]. Trudno też stwierdzić czy ktokolwiek z Timoru Portugalskiego, w przeciwieństwie do Angoli czy Mozambiku, ukończył studia w ZSRR lub innym państwie socjalistycznym.

Gdy w kwietniu 1974 r. Portugalia po upadku dyktatury (rewolucja czerwonych goździków) zadeklarowała chęć pozbycia się swych kolonii, w Timorze Portugalskim zaczęły formować się partie polityczne. W lipcu 1975 r. miały miejsce wybory do rad lokalnych, które okazały się pierwszą i jakże ważną lekcją demokracji. W tymże roku (w sierpniu) doszło jednak do dwumiesięcznej wojny domowej między zwolennikami *União Democrática Timorense* (UDT) a FRETILIN (*Frente Revolucionária de Timor-Leste Independente*). Zwyciężyli ci drudzy, ogłaszając 28 grudnia 1975 r. niepodległość Demokratycznej Republiki Timoru Wschodniego[12]. Zaledwie dziewięć dni później Indonezja, tuż po wyjeździe z Dżakarty prezydenta USA oraz sekretarza stanu, dokonała inwazji, zajmując to państwo na prawie ćwierć wieku.

W 1975 r. Timorczycy z kolonii woleli panowanie portugalskie niż indonezyjskie, tym bardziej że była to już Portugalia po rewolucji czerwonych goździków, która kolonializm uznała za anachronizm i moralne zło, powodując nawet zbyt szybkie i faktycznie nieodpowiedzialne wycofywanie się ze swych kolonii. W przypadku Timoru Portugalskiego oznaczało to pozostawienie tego państwa i jego ludności na pastwę losu. Ogłoszenie niepodległości nie spotkało się z pospiesznym uznaniem świata, nie

[11] FRETILIN był z pewnością radykalnie lewicowy, lecz jedynie w 1981 r. na krótko to konspiracyjne wówczas ugrupowanie polityczne przyjęło oficjalnie orientację marksistowsko-leninowską.

[12] Demokratyczna Republika Timoru Wschodniego to była nazwa oficjalna, wyraźnie ideologiczna. W zasadzie normą było wówczas (w połowie lat 70.), że jeżeli jakieś państwo miało w oficjalnej nazwie demokrację, to znaczyło to tyle co lewicowa dyktatura (NRD, KRLD, DRW, DK – Demokratyczna Kampucza).

przyjęto też Timoru Wschodniego w 1975 r. do ONZ czy innych organizacji międzynarodowych. Może po prostu nie zdążono? By do tego nie doszło, reakcja Indonezji – za cichym przyzwoleniem USA i Australii – była bardzo szybka. Dla mieszkańców Timoru Wschodniego opanowanie kraju przez Indonezję było okupacją (nowym kolonializmem); dla Indonezji – naturalnym efektem dekolonizacji. Tych punktów widzenia nie dało się uzgodnić. W 1975 r. niepodległość Timoru Wschodniego uznało tylko dziewięć państw: Chiny, Wietnam, Albania, Gwinea oraz pięć byłych kolonii portugalskich, lecz nie Portugalia.

W końcu 1976 r. liczbę ofiar wojny w Timorze Wschodnim szacowano na ok. 60 tys. zabitych[13]. W 1978 r. Australia i Nowa Zelandia uznały polityczny stan faktyczny na wyspie. W latach 1977–1979 tragiczny głód pochłonął przypuszczalnie 100 tys. ofiar[14].

W 1989 r. katolicki biskup Dili (stolicy Timoru Wschodniego) Carlos Bello wystosował apel do sekretarza generalnego ONZ z prośbą o podjęcie międzynarodowej interwencji na wyspie i wsparcie niepodległościowych aspiracji Timorczyków. W apelu tym znalazły się wstrząsające słowa: „Jako lud i naród umieramy". Zwykły mieszkaniec za takie słowa pod okupacją indonezyjską raczej skazałby się na tortury i śmierć. W polityce Indonezji, nastawionej na mieszankę surowych represji, nawet przez wielu nazywanych ludobójstwem[15], oraz gestów pojednawczych, obliczonych w dużym stopniu na zagranicę, znalazło się nawet miejsce

[13] W. Olszewski, op.cit., s. 228.

[14] Ibidem.

[15] Ludobójstwo w potocznym, zdroworozsądkowym i emocjonalnym rozumieniu jest po prostu zabijaniem ludzi na dużą skalę. Z formalnoprawnego punktu widzenia ludobójstwem są jednak tylko takie działania, które Konwencja ONZ w sprawie zapobiegania i karania zbrodni ludobójstwa określa jako ludobójstwo. Należy tu dodać, że treść konwencji była i jest efektem kompromisu, a na jej kształt w 1948 r. w znaczącym stopniu wpłynęło stanowisko ZSRR oraz kilku latynoskich dyktatur.

na wizytę papieża Jana Pawła II w Timorze Wschodnim w październiku 1989 r. oraz na inne znaczące gesty, z których należy wymienić wzniesienie kościoła, który następnie został katedrą katolicką – i to największą w Azji Południowo-Wschodniej[16], czy też odsłonięcie przez prezydenta Suharto w 1996 r. 27-metrowej figury Chrystusa (*Cristo Rei*). Podczas tej uroczystości nie doszło jednak do spotkania prezydenta z biskupem Belo, który właśnie został współlaureatem Pokojowej Nagrody Nobla.

W przełomowym 1975 r. byli tacy Wschodni Timorczycy, niekoniecznie chodzi o nieliczną społeczność muzułmańską, którzy mieli okazję być po indonezyjskiej stronie granicy. W porównaniu ze *skansenem paleolitu*[17] nawet zachodnia część Timoru mogła imponować znacznie wyższym poziomem życia i zdecydowanie lepszą infrastrukturą. Można się tylko domyślać, jakie wrażenie mogła na mieszkańcu Timoru Wschodniego (Portugalskiego) zrobić najlepiej rozwinięta część Indonezji. Nawet pojedyncza osoba opowiadająca, co zobaczyła na Jawie czy na Bali, mogła na innych oddziaływać proindonezyjsko, przynajmniej do czasu, gdy żołnierze-grabieżcy i zabójcy dokonali inwazji w grudniu 1975 r.

Świat socjalistyczny przez wiele lat przygotowywał działaczy komunistycznych z różnych państw, w tym z kolonii portugalskich do przejęcia władzy. Polityka ta okazała się wielkim sukcesem, skoro niemal w każdej byłej kolonii portugalskiej do władzy doszli marksiści-leniniści, jak choćby wykształcony w Moskwie Agostinho Neto czy w Berlinie Wschodnim – Manuel Pinto da Costa, ustanawiając monopartyjne dyktatury, a nawet zapraszając wojska kubańskie do walki z antykomunistyczną partyzant-

[16] M. Witkowska, *Z moich wypraw. Tam, gdzie ryż rośnie. Timor Wschodni (Timor-Leste)*, http://www.monikawitkowska.pl/blogi/z-moich-wypraw/734-timor-wschodni [dostęp: 11.01.2020]; J.A. Ureta, *Tragiczna sytuacja w Timorze Wschodnim. Rozmowa z Lídią Gonçalves Soares*, „Polonia Christiana" 2011, nr 18, s. 55.

[17] Ł. Bonczol, op.cit., s. 34.

ką. Priorytetem dla bloku socjalistycznego była Angola i Mozambik, o Timorze Portugalskim raczej „zapominano", może zakładając, że i tak Indonezja przejmie ten kraj.

USA, Australia czy Indonezja stały na stanowisku, że przynajmniej Timor Portugalski nie musi podążać drogą socjalistyczną. I tu interesy świata zachodniego i Indonezji były zbieżne. Uznano, że lepsza aneksja przez Indonezję niż państwo timorskie z marksistowskim ugrupowaniem FRETILIN u władzy.

Dla Indonezji procesy dekolonizacyjne w świecie były najczęściej postrzegane jako niekompletne. Z punktu widzenia Dżakarty podział Timoru był sztuczny, a odrębność polityczna i kulturowa Timoru Wschodniego była po prostu reliktem kolonializmu. Zauważmy, że granica była i jest na wyspie skomplikowana – Timor Portugalski posiadał i Timor Wschodni odziedziczył strukturę państwa dwuczęściowego: prócz większej części istnieje jeszcze eksklawa Ocussi. Zresztą nie tylko dwie granice były przez Indonezję postrzegane jako sztuczny twór kolonialny, lecz także katolicyzm – jako ewidentny produkt portugalskiego kolonializmu – i oczywiście język portugalski jako język edukacyjny. Dla Indonezji zdekolonizować – znaczyło maksymalnie wyrugować wpływy europejskie. Kolonializm niderlandzki bowiem nie schrystianizował Indonezji, a islam nie był postrzegany jako produkt kolonializmu arabskiego. Jedyne, co Indonezja „zawdzięcza" kolonializmowi (prócz kolonialnych budowli i niektórych zwyczajów), to alfabet łaciński i wiele europejskich słów w języku bahasa.

W 1975 r. polskie media donosiły o postawach proaustralijskich w Timorze Portugalskim, co miało wyrażać się w ruchu politycznym na rzecz przyłączenia tej kolonii właśnie do Australii. Dziś na próżno szukać śladów tej politycznej inicjatywy, co znaczy, że była ona bardzo słaba i efemeryczna. Zresztą z pewnością nie tylko z dbałości o poprawne stosunki z Portugalią Australia nie była zainteresowana przyłączeniem tego kraju do

swego terytorium jako kolejnej jednostki administracyjno-politycznej. Automatyczne nadanie pogrążonym w biedzie i zacofaniu oraz przeżywającym eksplozję demograficzną Wschodnim Timorczykom australijskiego obywatelstwa oznaczałoby ich masowy napływ i liczne problemy z tym związane. Do tego doszłaby jeszcze granica lądowa z Indonezją, przez którą z pewnością płynęłaby fala nielegalnych imigrantów. Inicjatywa ta zatem już w zalążku była skazana na niepowodzenie.

Można zadawać sobie pytanie zarówno w Indonezji, jak i w Timorze Wschodnim, a nawet w Europie, co w procesie dekolonizacji jednak z kolonializmu pozostawić? Czy zachować granice, nawet bardzo sztucznie wytyczone; czy zachować język byłych kolonizatorów i zaszczepioną przez nich religię? Czy wymazać najwięcej, jak się da? W przypadku polityki Indonezji w Timorze Wschodnim wielu historyków, politologów i publicystów uważa, że było to realizowanie indonezyjskiego nacjonalizmu metodami kryminalnymi – z gwałtami i sadyzmem włącznie. W jakim stopniu te poczynania były inspirowane z Dżakarty, a w jakim do głosu dochodziła samowola w terenie – na niskim szczeblu, tego nie sposób ustalić. Największe natężenie represji miało miejsce od inwazji do końca lat 70. Potem sytuacja się uspokoiła, więc można było osiedlać Indonezyjczyków i rozbudowywać infrastrukturę. W maju 1976 r. powołano lokalne Zgromadzenie Ludowe, które zwróciło się prośbą o integrację z Indonezją. Procedura ta przypominała włączenie do ZSRR polskiego terytorium, zajętego w 1939 r. Timor Wschodni miał w indonezyjskim parlamencie czterech posłów.

Wojsko indonezyjskie rozstrzeliwało podczas inwazji nawet działaczy proindonezyjskich; niektórzy podobno próbowali pokazać swe legitymacje ugrupowań działających na rzecz przyłączenia do Indonezji, ale nie zdążyli. Były to działania zupełnie nielogiczne, powodujące od początku zrażanie ludności zajmowanego kraju.

USA w raportach na temat praw człowieka w świecie w drugiej połowie lat 70. nie zauważały kwestii Timoru Wschodniego, tym bardziej że infrastruktura, edukacja i opieka zdrowotna pod indonezyjską okupacją ulegały znaczącej poprawie – równolegle do masowych zbrodni. Ćwierć wieku okupacji to także wzrost długości dróg utwardzonych (asfaltowych), z 30 km do 3500 km, co też dobitnie świadczy o tym, jak zacofana była ta kolonia portugalska. Nakłady Indonezji na rozwój tej 27. prowincji były bardzo wysokie w stosunku do jej powierzchni i liczby ludności. Zbudowano ponad tysiąc nowych szkół, uniwersytet, lotnisko w stolicy, szpitale, mosty; dokonano elektryfikacji, znacząco rozwinięto sieć telekomunikacyjną.

Portugalia od 1975 r. działała aktywnie i konsekwentnie w sprawie Timoru Wschodniego, ponosząc klęski na przemian z względnymi sukcesami. To dzięki Portugalii sprawa Timoru Wschodniego nie schodziła z porządku obrad ZO NZ (choć w latach 1983–1988 ONZ nie zajmowała się sprawami Timoru Wschodniego, więc mogło się wydawać, iż jest to sprawa przegrana). Inwazja Indonezji została już po kilku dniach potępiona przez ZO NZ, a Portugalia była na forum międzynarodowym traktowana jako prawowity zarządca Timorem Wschodnim; oczywiście Indonezja miała na ten temat odmienne zdanie. W jednej z rezolucji ZO NZ potwierdzono nawet prawo Timorczyków Wschodnich do walki o samostanowienie i niepodległość[18]. Należy tu zauważyć, iż na forum ONZ Indonezję w kwestii Timoru Wschodniego popierały konsekwentnie Indie i Japonia, od 1976 r. USA, a od 1978 r. również Australia[19].

Jeszcze w 1977 r. ogromne połacie kraju były pod kontrolą partyzantów. Wieśniacy zabijali Indonezyjczyków nawet dmuchawkami z zatrutymi strzałami. Z kolei czołowi oficerowie

[18] Ibidem, s. 73–74.

[19] Ibidem, s. 74.

indonezyjscy byli właścicielami plantacji kawy; oficerowie średniego szczebla zakładali bary czy restauracje, w których żołnierze zostawiali pieniądze[20]. Czy poczynania Indonezji w Timorze Wschodnim to była wyjątkowo brutalna forma neokolonializmu, jak szef Komitetu Noblowskiego powiedział, uzasadniając przyznanie Pokojowej Nagrody Nobla dwóm Wschodnim Timorczykom w 1996 r.?[21] Czy może był to po prostu syndrom tzw. strefy buforowej lub przyfrontowej, z charakterystyczną dla takich obszarów dominacją wojska w gospodarce oraz łamaniem praw człowieka?

Trudno stwierdzić, na ile echa przemian w Polsce i następnie w innych państwach socjalistycznych pod koniec lat 80. sprawiły, że Timor Wschodni przeżył kontrolowaną pierestrojkę, jeszcze pod indonezyjskim panowaniem. Po masakrze na cmentarzu Santa Cruz w stolicy w listopadzie 1991 r. przynajmniej symbolicznie skazano maksymalnie na półtora roku więzienia żołnierzy-wykonawców (wyroki wydane na uczestników, a tym bardziej domniemanych organizatorów protestów były dużo bardziej surowe)[22]. Jednakże część mediów indonezyjskich – choćby niewielka – była oburzona tymi wydarzeniami, wyrażając solidarność z Timorczykami, co można uznać za sygnał, że poparcie dla represji w samej Indonezji nie było już wówczas powszechne. Brak rzetelnych czy nawet jakichkolwiek badań opinii na ten temat sprawia, że nie znamy postaw Indonezyjczyków i ich ewolucji wobec kwestii Timoru Wschodniego na przestrzeni lat.

---

[20] Ibidem, s. 84. To pokazuje, że Indonezja plasowała się zdecydowanie po stronie świata kapitalistycznego. Nawet wysocy rangą oficerowie państw socjalistycznych nie mogli bowiem być w posiadaniu środków produkcji – czy to u siebie w kraju, czy za granicą. Na przykład żołnierze radzieccy w Afganistanie angażowali się w przedsięwzięcia o charakterze gospodarczym, jednakże zawsze była to działalność czarnorynkowa.

[21] Ł. Bonczol, op.cit., s. 130.

[22] Ibidem, s. 135.

Jak wiadomo, nie sposób odnieść się do badań, których nigdy nie przeprowadzono. Trudno też stwierdzić, jakie były u progu niepodległości – tej po referendum – na skali optymizmu postawy Timorczyków Wschodnich wobec przyszłości. Czy i w jakim stopniu wiązano nadzieje choćby z pomocą zagraniczną oraz eksploatacją podmorskich złóż ropy naftowej i gazu ziemnego. Jeżeli nadzieje i wymagania nie są zbyt wygórowane, to i rozczarowania nie przybierają form zbyt drastycznych zarówno w wymiarze indywidualnym, rodzinnym, jak i społeczno-politycznym.

W okupowanym Timorze Wschodnim Indonezja na przestrzeni lat tworzyła paramilitarne bojówki złożone ze Wschodnich Timorczyków. Pierwszy oddział już w 1982 r. zabił i wziął do niewoli kilkudziesięciu żołnierzy ruchu oporu. Członkowie takich oddziałów na trwałe poróżnili się z resztą społeczności[23]. To częściowo może tłumaczyć, dlaczego po latach w referendum niepodległościowym[24] część Wschodnich Timorczyków głosowała za pozostaniem w granicach Indonezji, a przecież do udziału w plebiscycie nie byli uprawnieni osadnicy oraz ich dzieci[25] urodzone już w Timorze Wschodnim (było może nawet 200 tys. osiedleńców, co oprócz terroru także umacniało rdzennych Timorczyków Wschodnich w poczuciu wspólnoty narodowej i katolicyzmie)[26].

[23] Ibidem, s. 136.

[24] Należy zauważyć, że referenda (plebiscyty) były zwykle wymuszane na państwach przegranych (np. w przypadku Górnego Śląska), a przecież Indonezja państwem takim nie była. W tym przypadku decyzję o referendum podjął jednoosobowo prezydent Habibie pod wpływem Australii, bez konsultacji z doradcami oraz wbrew wojskowym.

[25] Przyjęto tu zasadę, że zamieszkiwanie tych osób w Timorze Wschodnim jest związane z indonezyjską okupacją, zatem w innej sytuacji politycznej osadników tych w tym kraju by nie było.

[26] Dziś ponad 95% Wschodnich Timorczyków deklaruje katolicyzm.

W 1983 r. zaprzysiężono 3844 nowych członków „jednostek pomocniczych", czyli z punktu widzenia przeciwników Indonezji – po prostu zdrajców. Nie brakowało oddziałów samowolnych, nierzadko skryminalizowanych; inne działały pod płaszczykiem społecznych organizacji masowych. Były nawet powstałe z prywatnej inicjatywy pojedynczych dowódców – takie musiały utrzymać się same, kosztem swych ofiar. Członkami proindonezyjskich bojówek byli sfrustrowani osadnicy oraz osoby, które straciły członków rodziny z rąk partyzantów[27]. Paradoksalnie nadzieją dla Timoru Wschodniego stał się dramatyczny kryzys ekonomiczny z 1997 r., który bardzo osłabił Indonezję. Kolejną odsłoną stało się zmuszenie wieloletniego prezydenta Suharto do ustąpienia. Dla prezydenta Indonezji Timor Portugalski (Wschodni) to było ostatnie niewyzwolone jeszcze terytorium indonezyjskie. Nie może więc dziwić, że gdy Suharto został odsunięty od władzy, rozwiązanie kwestii Timoru Wschodniego nie tylko pojawiło się na horyzoncie, ale od razu nabrało tempa. Nowy prezydent Jusuf Habibie wyraził zgodę na przeprowadzenie referendum niepodległościowego i pozwolił w 1999 r. na rozmieszczenie na terytorium Timoru Wschodniego misji wojskowej INTERFET (*International Force for East Timor*), która przygotowała grunt pod obecność Tymczasowej Administracji ONZ w Timorze Wschodnim w latach 1999–2002.

Nadzieje związane z referendum, które odbyło się 30 sierpnia 1999 r., przeszły wszelkie oczekiwania, zarówno gdy chodzi o frekwencję (98%), jak i rezultat. 78,5% uczestników opowiedziało się za niepodległością. Swój wkład wniosła tu również grupa polskich wolontariuszy (m.in. Krzysztof Wiśniowiecki, Grzegorz Kucharczyk[28], Anna Górska), prowadząca spotkania

[27] Ł. Bonczol, op.cit., s. 136–137.

[28] Grzegorz Kucharczyk, autor m.in. artykułu *Chrześcijanie w Indonezji i Timorze Wschodnim*, to inna osoba. Rozmowy z G. Kucharczykiem, Murowana Goślina – Opole, maj 2019–kwiecień 2020.

przedreferendalne, obserwująca przebieg kampanii politycznej, a także organizująca i nadzorująca przebieg referendum. Przed referendum gubernator Timoru Wschodniego wydawał rozkazy zabijania księży i zakonnic. Dla Indonezji było to już za wiele, więc w 2002 r. został skazany[29].

Wypadki potoczyły się jednak dramatycznie. Odwetem stał się pogrom rdzennej ludności, a wrzesień przyniósł przymusowe deportacje Timorczyków ze wschodniej do zachodniej części wyspy. Ocenia się, że dotknęło to około 300 tys. osób. Wynik referendum stał się początkiem kampanii terroru i wypędzeń, systematycznie prowadzonej przez władze indonezyjskie. Na 800 tys. mieszkańców ponad połowa utraciła swoje domy, a 140 tys. trafiło do Timoru Zachodniego, do wcześniej przygotowanych przez władze indonezyjskie miejsc wysiedlenia. Kres pogromom położyła dopiero misja wojskowa ONZ, którą powołano niemal błyskawicznie, ale i tak dwa tygodnie za późno.

15 września 1999 r. Rada Bezpieczeństwa ONZ przyjęła jednogłośnie rezolucję o wysłaniu sił pokojowych do Timoru Wschodniego (INTERFET). Rdzeń sił pokojowych (4,5 tys. żołnierzy) tworzyli Australijczycy. Wówczas też rozpoczął się exodus na zachód proindonezyjskich oddziałów ochotniczych. Milicjanci zabierali ze sobą całe rodziny i dobytek. Lojalistom towarzyszyły duże grupy muzułmanów. Dochodziło do masowych podpaleń i dewastowania wszystkich pozostawionych dóbr i instalacji, z nienawiści do Wschodnich Timorczyków, którzy okazali się niewdzięczni i nie docenili tego, ile choćby w zakresie infrastruktury uczyniła dla nich Indonezja. Oczywiście taki był indonezyjski i proindonezyjski punkt widzenia.

Po referendum, w Timorze Zachodnim było ok. 230 tys. uchodźców – najczęściej zmuszonych siłą do opuszczenia swego kraju. Dopiero w czerwcu 2001 r. zlikwidowano obozy dla

[29] Ł. Bonczol, op.cit., s. 150.

uchodźców. Część z nich pozostała w Indonezji, w większości ostatecznie osiedlając się na innych wyspach archipelagu[30]. Uchodźcy, którzy nie zdecydowali się na powrót do Timoru Wschodniego, niekoniecznie reprezentowali opcję proindonezyjską. Często po prostu byli świadomi, że nie mają do czego wracać. Zmęczeni tragedią ostatniego ćwierćwiecza, woleli wybrać stabilizację i bezpieczeństwo oraz wyższy poziom życia w Indonezji, niż niepewność i biedę w swej ojczyźnie. Wśród uchodźców były osoby wykwalifikowane, których brak oznaczał, że wiele sektorów po prostu przestało funkcjonować, dopóki nie napłynęli pracownicy zagraniczni, również z organizacji pozarządowych. W początkowym okresie podstawowe źródło dochodów budżetu młodego państwa „(wyłączając pomoc zagraniczną) stanowiły cła i podatki pośrednie nakładane na alkohol, papierosy, samochody oraz inne dobra konsumpcyjne nabywane przez przybyszów"[31].

W październiku 1999 r. powołano oenzetowską przejściową administrację UNTAET, mającą przygotować kraj do samodzielnego funkcjonowania w warunkach autentycznej niepodległości, która jednak rozczarowała już na starcie. Może nie tyle niepodległość, co to, jak to młode państwo – zależne od pomocy międzynarodowej – funkcjonowało. Cudzoziemski personel żył w specjalnych enklawach, a zwykli Timorczycy byli co najwyżej sprzątaczami, dozorcami, sprzedawcami owoców i zapalniczek[32]. Powstała dwubiegunowa gospodarka – świat stosunkowo nielicznych cudzoziemców oraz świat autochtonicznych biednych mas. W zasadzie nawet świat Wschodnich Timorczyków też był podzielony – inaczej niż tradycyjnie. Młodzi ludzie z choćby średnią znajomością an-

30 Ibidem, s. 162.

31 Ibidem, s. 163.

32 Ibidem.

gielskiego byli znacznie bardziej cenieni niż wioskowa starszyzna, a świadczący proste usługi cudzoziemcom zarabiali znacznie więcej niż wódz plemienia czy nauczyciel[33].

Należy zauważyć, iż oenzetowscy administratorzy w wielu krajach siłą rzeczy stwarzali dystans wobec biednej ludności miejscowej. Inaczej mieszkali, bardzo dużo zarabiali i wydawali, co rodziło zawiść, ale także pragnienie wyciągnięcia z tego maksymalnych korzyści. Oferowanie ze strony miejscowych różnych dóbr i usług, także seksualnych, było częścią wielu misji oenzetowskich i wiele wskazuje na to, że jest to cecha stała takich przedsięwzięć. Trudno bowiem sobie wyobrazić, by w imię skracania dystansu międzynarodowi administratorzy żyli siermiężnie, by nie drażnić miejscowej ludności, zarazem nie dając też jej odpowiednio zarobić; zatem Timor Wschodni nie był tu wyjątkiem, choć oczywiście był zdecydowanie biedniejszy niż np. Liban, Kosowo czy Irak.

UNTAET była w zasadzie pierwszym przypadkiem, gdy misja ONZ dysponowała pełnią suwerennością. Wiązało się to z tym, iż dla ONZ Timor Wschodni przez cały czas indonezyjskiej okupacji był terytorium niesamodzielnym[34].

Ponaddwutygodniowy terror, jaki po ogłoszeniu wyników referendum rozpętali przeciwnicy niepodległości, był wielką klęską społeczności międzynarodowej. Tysiące zabitych, straszliwe zniszczenie infrastruktury oraz masowy exodus ludności sprawiły, że start tego kraju w niepodległy byt okazał się przez to zdecydowanie trudniejszy. Jedynym pozytywnym aspektem tamtych wydarzeń było jednak z pewnością to, że wrogowie niepodległego Timoru Wschodniego w większości opuścili ten kraj, by już nigdy do niego nie powrócić. Społeczność międzynarodowa co prawda potrafiła szybko się zmobilizować, by rato-

[33] Ibidem, s. 164.

[34] Ibidem, s. 164–165.

wać sytuację w Timorze Wschodnim, ale kilkanaście dni terroru przyniosło straty, których skutki są widoczne do dziś – skutki demograficzne, psychiczne, ekonomiczne, infrastrukturalne i wiele innych.

Dla Australii, poza innymi aspektami korzyści z niepodległości Timoru Wschodniego, nowa sytuacja była sprzyjająca także dlatego, że każdy nielegalny imigrant z państwa teraz formalnie wolnego i demokratycznego mógł być uważany za emigranta ekonomicznego, nie zaś za ofiarę prześladowań, której należy się azyl polityczny.

W ramach misji ONZ z całego świata zjechało 11 tys. żołnierzy, urzędników, doradców ekonomicznych i prawników z zadaniem zbudowania państwa. Trzeba było od podstaw stworzyć administrację, policję, wojsko i gospodarkę, która nie licząc upraw kawy, praktycznie nie istniała[35]. Już na początku istnienia oenzetowskiej administracji Timor Wschodni był państwem w dużym stopniu patologicznym. Byli partyzanci oraz inni bezkarnie trudnili się przemytem dóbr z terenu „wroga", czyli z Indonezji, nakładali nielegalne podatki (haracz) na dopiero co odradzających się przedsiębiorców, do czego dochodził jeszcze czarnorynkowy obrót paliwem kradzionym z garnizonów sił pokojowych[36].

Przerażający brak kadr, nieznajomość innego prawa niż zwyczajowe, skłonność do przemocy, tradycje korupcyjne, postrzeganie wielu instytucji kojarzonych z nowoczesnym państwem jako odległych i niedostępnych – to tylko najważniejsze przeszkody w budowie dobrze funkcjonującego, choćby nawet bardzo biednego państwa.

Instytucje państwa jawią się wielu Wschodnim Timorczykom jako trudne do ogarnięcia, nieprzejrzyste, oderwane od

[35] Rozmowy z G. Kucharczykiem..., op.cit.

[36] Ibidem, s. 165.

realiów życia prostego człowieka, a nawet po prostu obce. Wiadomo, że zręby współczesnego państwa, budowanego niemal od zera w dużym stopniu przez cudzoziemców, bazują na obcych wzorcach. Implementowany system prawny nie wyrasta z lokalnych tradycji i ma więcej wspólnego z rzymską tradycją niż z miejscowym prawem zwyczajowym. To sprawia, że wiele aspektów państwa wschodniotimorskiego było i jest dla większości ludności niezrozumiałych, obcych lub po prostu słabo rozpoznanych. Jak niegdyś pisał Guy Sorman o państwach Trzeciego Świata: masy nie zawsze muszą być wyzyskiwane, masy mogą być po prostu pominięte[37].

Scenariusz działań, którego realizacja miała doprowadzić do samodzielnego funkcjonowania państwa wschodniotimorskiego, został niewątpliwie nakreślony „za biurkiem", uwzględniając tradycje, doświadczenia i stan wyjściowy tylko częściowo. Po uzyskaniu niepodległości w Timorze Wschodnim miał nadal obowiązywać indonezyjski system prawny (czyli system niedawnego ludobójcy), uzupełniony następnie pomocniczymi przepisami portugalskimi, czyli prawem wcześniejszego kolonizatora[38]. Spowodowało to zamęt o daleko idących konsekwencjach.

30 sierpnia 2001 r. odbyły się pierwsze wybory parlamentarne. W tym wypadku nie można mówić o rozczarowaniu, a raczej o niespotykanym w „starych" demokracjach entuzjazmie. Frekwencja 91,3% świadczyła o ogromnych nadziejach

---

[37] G. Sorman, *Nowe bogactwo narodów*, Łódź–Warszawa 1989, s. 33. W przypadku choćby Brazylii czy Meksyku państwo prowadziło politykę faworyzowania elit z sektorów gospodarczych wybranych przez rządzących jako wiodące, zaniedbując resztę społeczeństwa w zakresie ochrony zdrowia, edukacji, infrastruktury. Timor Portugalski był z kolei przykładem zaniedbania niemal całości społeczeństwa przez Portugalię, która wysyłała tam administratorów cywilnych i wojskowych na zasadzie selekcji negatywnej. W czasach współczesnych kolonia ta nie stała się też miejscem atrakcyjnym do stałego osiedlania się Portugalczyków w wymiarze większym niż śladowy, jak to miało miejsce w przypadku Angoli czy Mozambiku.

[38] Ł. Bonczol, op.cit., s. 167.

związanych z wyborem konstytuanty[39]. Podobnie było zresztą w Kambodży, gdzie osiem lat wcześniej, także pod nadzorem ONZ, przeprowadzono pierwsze od kilkudziesięciu lat wolne wybory. Jeżeli bardzo wysoka frekwencja ma miejsce w państwie, które wolnością cieszy się od niedawna, to znaczy, że nawet biedne, niewykształcone i boleśnie doświadczone społeczeństwo wiąże z takimi wyborami ogromne nadzieje, nierzadko rozbudzone przez nierealistyczne obietnice poszczególnych partii oraz konkretnych kandydatów. Oczywiście jest też bardzo prawdopodobne, że po pewnym czasie nadzieje zaczną ustępować miejsca rozczarowaniom i cynicznemu stosunkowi do polityki jako takiej, bo przecież w bardzo biednych i zapóźnionych w rozwoju państwach nie sposób zdecydowanie poprawić położenia ludności w krótkim czasie. Nie dokonają tego nawet najbardziej demokratyczne instytucje czy pracowici politycy, a demokracja szybko może być kojarzona z nieustannymi kłótniami, postrzeganymi jako działania raczej destrukcyjne, szczególnie gdy pojawi się przemoc – z ofiarami śmiertelnymi włącznie.

Timor Wschodni jest skazany na indonezyjskie sąsiedztwo (dwie granice państwowe), zatem musi zabiegać o jak najlepsze stosunki z tym byłym okupantem, również ze względów gospodarczych. Pozytywne jest niewątpliwie to, że w samej Indonezji zaszły i nadal zachodzą demokratyczne przemiany, co na przestrzeni lat czyni to sąsiedztwo mniej konfliktowym, a zmiany pokoleniowe, łatwiejsze w sytuacji eksplozji demograficznej, jedynie temu sprzyjają. Czy kiedykolwiek dojdzie do jakiejś formy zadośćuczynienia ze strony Indonezji: przyznania się do popełnionych zbrodni; choćby symbolicznego ukarania niektórych winowajców; ekshumacji części masowych grobów? Trudno stwierdzić, jednak przykład Kambodży pokazuje, że

[39] Ibidem, s. 168.

rozliczenia są czasem łatwiejsze po kilkudziesięciu latach niż w krótkim czasie, choć oczywiście Kambodża i Timor Wschodni to przykłady, których nie można mechanicznie porównywać.

Z oenzetowską misją UNTAET Wschodni Timorczycy wiązali wygórowane oczekiwania, toteż rozczarowanie nią obciążało również tych, którzy z tą misją współdziałali, tym bardziej, że współpracując znacząco poprawili swój byt, podczas gdy absolutna większość ludności takiej poprawy subiektywnie nie doświadczyła. Sprawiło to, że w wyborach do konstytuanty konieczne było prześciganie się w obietnicach. Kto głosił, że w krótkim czasie niewiele można zmienić na lepsze, w zasadzie nie miał szans. Zapotrzebowanie na nadzieję nieraz już sprawiło, że nierealistyczne obietnice wygrywały zdecydowanie z realizmem.

Po dwóch latach rządów UNTAET bezrobocie – jak pisał F. Gaglioti – wynosiło około 80%[40]. Chodzi tu chyba również o bezrobocie ukryte, gdyż Timor Wschodni to kraj przede wszystkim wiejski, a w takich państwach bezrobocie jawne z reguły jest niskie.

Perturbacje młodej demokracji przybierały czasem formy zaskakujące. Podczas wyborów prezydenckich w 2002 r. dwaj czołowi kandydaci byli osobami faktycznie niechcącymi kandydować. Prowadzili kampanię niekonfrontacyjną, a właściwie przyjacielską. To wszystko przebiegało w warunkach młodej demokracji, które to pojęcie wielu Wschodnim Timorczykom było obce. Dobrze się stało, że w kraju tym pojawiły się wreszcie sondaże i inne badania socjologiczne, w zasadzie wcześniej nieznane. Dzięki nim można było się przekonać, że demokracja jest dla bardzo wielu Wschodnich Timorczyków pojęciem w zasadzie nieznanym lub źle rozumianym[41], a jak wiadomo, wolność auto-

[40] Ibidem, s. 170. Nie znaczy to, że misja ta za taki stan rzeczy jest odpowiedzialna.

[41] Ibidem, s. 170–171.

matycznie nie gwarantuje demokracji rozumianej jako nie tylko dobre prawo i odpowiednie struktury, ale również system ciał pośredniczących, składających się na społeczeństwo obywatelskie. Jedyne, co w państwie tym można uznać za plus, to wysoka frekwencja wyborcza, która – choć nie taka jak dawniej – chyba już zdążyła stać się normą.

W maju 2002 r. Timor Wschodni stał się oficjalnie niepodległym państwem. Według raportu Banku Światowego, mimo 150 mln dolarów corocznej pomocy, pod władzą ONZ Timor Wschodni jeszcze bardziej zbiedniał.

Zasadniczymi problemami młodego państwa w pierwszych latach po rządach oenzetowskich były rozliczenie z przeszłością i kwestie gospodarcze, a konkretnie – konieczność podejmowania zdecydowanych i często niepopularnych decyzji. Jeżeli konstytuanta odmawia rozwiązania się po uchwaleniu konstytucji, a państwo przybiera oficjalną nazwę, odnoszącą się do nazwy z 1975 r., silnie kojarzącą się z „demokracjami ludowymi", to można było to odebrać jako dryfowanie w kierunku autorytarnym, choć niekoniecznie radykalnie lewicowym.

Wielkim wyzwaniem dla młodego państwa było i jest powstanie znaczącej klasy średniej, wywodzącej się z biznesu, oraz odpowiednio wykształconej kadry urzędniczej, nie mówiąc już o młodych liderach politycznych. Poza fizyczną odbudową kraju Timor Wschodni musiał stworzyć własną służbę cywilną, policję, sądownictwo, edukację i system zdrowotny od podstaw. – To kraj budowany od zera – wyjaśnia Paul Joicey, szef timorskiego programu w Oxfam[42]. Nawet wiele lat po uzyskaniu niepodległości problemy kadrowe były dramatyczne, opóźniając choćby przyjęcie państwa do ASEAN-u. Jak zauważył ówczesny (lata 2012–2015) minister spraw zagranicznych Luís Guterres: „ze względu na zgromadzone przez państwo

[42] M. Lenarcik, op.cit.

fundusze, pochodzące z wydobycia ropy naftowej, możliwym rozwiązaniem [...] byłoby zatrudnienie obcych ekspertów w roli miejscowych dyplomatów[43].

W grudniu 2002 r. w Dili doszło do ostrych zamieszek. Lata biedy i frustracji okazały się być zbyt wielkim obciążeniem dla raczkującej demokracji. Gospodarka praktycznie nie istniała, a ludzie czekali na szybką poprawę w kraju, niemalże całkowicie zależnym od pomocy zagranicznej. W połowie 2005 r. w Timorze Wschodnim stacjonował jedynie mały kontyngent bojowy ONZ. Gdy obcokrajowcy zaczęli wyjeżdżać, liczba problemów związanych z tworzeniem zrębów nowego państwa okazała się być aż nazbyt widoczna. W 2006 r. było jasne, że oczekiwania były zbyt wielkie w zbyt krótkim czasie. Timor Wschodni miał być wolnorynkową demokracją z zapleczem socjalnym (społeczna gospodarka rynkowa) i w pewnym sensie takim się stał, tyle że zaplecze to jest niezwykle skromne, a wolny rynek automatycznie nie generuje przecież dobrobytu.

Przeprowadzone w 2008 r. badanie amerykańskiego Republican Institute wykazało, że ponad 75% obywateli cieszy się z obecności wojsk ONZ w ich kraju głównie z powodu zwiększenia się poziomu bezpieczeństwa. Wynik nie dziwi, biorąc pod uwagę, że za każdym razem, gdy wyjeżdżają żołnierze, państwo pogrąża się w chaosie[44].

Partyzanci antyniepodległościowi z biegiem lat coraz rzadziej napadali na graniczne wioski. W 2000 r. w takich potycz-

[43] P. Soja, *Droga Timoru Wschodniego do ASEAN – członek trzeciej generacji czy wieczny obserwator?*, „Teka of Political Science and International Relations" 2018, vol. 13, nr 1, s. 129–130, https://journals.umcs.pl/teka/article/view/8417 [dostęp: 19.12.2018], za: J.L. Gutteres, *Timor Leste ready to fulfil ASEAN obligations*, http://www.bt.com.bn/news-national/2014/03/18/timor-leste-ready-fulfil-asean-obligations-pm [dostęp: 15.08.2017]. Lídia Gonçalves Soares zauważa, że od 2005 r. przez jakiś czas przybywało też wielu kubańskich lekarzy i nauczycieli. J.A. Ureta, op.cit., s. 57. O jednym z nich (lekarzu) pisze M. Janiszewski, op.cit., s. 104–106.

[44] M. Lenarcik, op.cit.

kach zginął żołnierz Nowej Zelandii, w innej – z Nepalu oraz policjant ONZ.

W ciągu czterech lat indonezyjskiej okupacji populacja Timoru Wschodniego zmniejszyła się o 23% – w 1974 r. liczba ludności tego państwa liczyła 653 211 osób, podczas gdy w 1978 r. już tylko 498 433[45], a przecież normą dla tego kraju w tym czasie powinna być eksplozja demograficzna, tak jak ma to miejsce obecnie. Właśnie wysoki przyrost naturalny sprawia, że nawet lata bardzo pomyślnej koniunktury gospodarczej oznaczają czasem spadek PKB *per capita*. W 2006 r. przewidywano, że w 2023 r. liczba ludności się podwoi. Gęstość zaludnienia Timoru Wschodniego jest ciągle mniejsza niż Polski, a mimo to występuje w tym państwie głód ziemi (tylko 5% gospodarstw rolnych miało w 2005 r. więcej niż hektar)[46]. Niedostatek ziemi uprawnej w kraju, w którym trzy czwarte ludności żyło z pracy na roli, musiał w warunkach eksplozji demograficznej zaowocować rabunkowym stosunkiem do lasów i dzikich zwierząt[47]. Na to wszystko nałożył się jeszcze problem ustalenia praw własności po zniszczeniach z 1999 r., exodusie ludności, a potem powrocie tysięcy uchodźców, którzy zajmowali ziemię i domy nadające się do zamieszkania – w sytuacji nieistnienia dokumentów potwierdzających prawa konkretnych osób do ziemi czy domów (tragicznych kilkanaście dni po ogłoszeniu wyników referendum to również pożary, w których spłonęły niemal wszystkie archiwalia)[48].

---

[45] M. Witkowska, op.cit.

[46] Ł. Bonczol, op.cit., s. 173.

[47] Lídia Gonçalves Soares twierdzi, że wysoki poziom dzietności jest pożądany z różnych względów, aby odrobić straty z czasów indonezyjskich (choć straty w ludziach zostały już dawno odrobione). J.A. Ureta, op.cit., s. 54.

[48] Ł. Bonczol, op.cit., s. 174. Prawa własności odtwarzano zatem na podstawie zeznań właścicieli oraz świadków.

Pod rządami UNTAET Timor Wschodni otrzymał pomoc w wysokości ok. 2,3 mld dolarów[49]. Gdy strumień pomocy ustał, gospodarka w 2005 r. popadła niemal w stagnację, co przy wysokim przyroście ludności oznaczało spadek PKB *per capita*. Eksplozja demograficzna w warunkach ogromnej biedy zawsze jest przejawem braku odpowiedzialności wobec siebie oraz wobec rodziny. Przyjmuje się jednak, że biednych nie wypada krytykować za żywiołowy stosunek do prokreacji. Z kolei biedni wielodzietni, nie poczuwając się do odpowiedzialności, uważają, że za ich złą sytuację materialną odpowiadają wyłącznie rządzący, gdyż ludzie władzy żyją zawsze w zdecydowanie lepszych warunkach niż biedne masy. Taki schemat postrzegania społecznej i ekonomicznej rzeczywistości może trwać latami, może być dziedziczony i wprowadzać na stałe zaprawiony cynizmem antagonizm między rządzonymi a rządzącymi. Ci ostatni z kolei uważają zwykle, że od ludzi należy również wymagać, by pomogli sobie sami, np. ograniczając rozrodczość. Wiele wskazuje na to, że w schemat ten wpadli również Wschodni Timorczycy, widząc, że niepodległość wcale nie jest skutecznym lekarstwem na biedę i zacofanie.

W 2006 r. w Timorze Wschodnim miały miejsce tragiczne wydarzenia. Około 600 żołnierzy, a była to prawie połowa armii, zbuntowało się, domagając się dymisji premiera Alkatiriego (potomka arabskich kupców, muzułmanina – w kraju, w którym wyznawcy Mahometa stanowią obecnie jedynie, w zależności od źródeł, od kilku promili do 4% społeczeństwa). Żołnierze ci byli już wówczas wydaleni ze służby, jak twierdzili, ze względu na pochodzenie etniczne. Zaczęło się od buntu w armii. Prawie 600 żołnierzy z ludu Kaladi (niemal połowa wojska) zamieszkującego zachodnią część kraju, obrażonych za pomijanie ich przy awansach, opuściło koszary. Zżymali się,

[49] Ibidem.

że najwyższe stanowiska zagarnęli dla siebie członkowie ludu Firaku ze wschodu. Firaku zaś uważali, że to oni w czasie indonezyjskiej okupacji poszli w góry i zaczęli walkę z najeźdźcą. W roli wybawiciela wystąpiła Australia, która przysłała ponad dwa tysiące żołnierzy, a z Malezji i Nowej Zelandii doszło kolejnych 500. O swojej byłej kolonii nie zapomniała Portugalia, która wsparła Timorczyków 120 policjantami.

Korzystając z nieobecności policji, bandy młodych Timorczyków, sfrustrowanych biedą i bezrobociem, plądrowały, dewastowały i zabijały. Dili pokryła gęsta chmura dymu, gdyż w płomieniach stanęły samochody, sklepy i domy. W krajobraz kraju wpisały się gangi, które nawet mają swe nazwy. Najsilniejsze z nich to „77" i „PSHP", do których należy łącznie blisko 50 tys. osób[50].

Należy tu zauważyć, że różnice etniczne w latach walki o niepodległość i jeszcze później nie były w tym kraju istotnym kryterium podziału społeczeństwa. Różne społeczności etniczne żyły raczej zgodnie, więc walki uliczne w Dili pomiędzy niezwykle brutalnymi gangami młodych ludzi, dla których głównym kryterium podziału były różnice plemienne, oznaczały, że w społeczeństwie wschodniotimorskim stało się coś nieoczekiwanego. Gdy zabrakło wspólnego wroga, a sytuacja gospodarczo-społeczna rozczarowywała z roku na rok, do głosu doszło nowe pokolenie, które zaczęło doszukiwać się przyczyn trudnego życia tam, gdzie wcześniej ich nie lokalizowano – w plemiennym zróżnicowaniu ludności[51]. Nienawiść została ponadto skierowana w stronę zagranicznych inwestorów, gdyż byli obcy, a żyli znacznie lepiej niż miejscowi, czyli byli postrzegani jako

[50] https://www.szkolnictwo.pl/szukaj,Timor_Wschodni [dostęp: 11.01.2020].

[51] Lídia Gonçalves Soares stwierdziła, że: „Pomiędzy Timorczykami nie ma różnic etnicznych, są jedynie różnice kulturowe i językowe". J.A. Ureta, op.cit., s. 54.

wyzyskiwacze[52]. Podczas starć doszło nawet do tego, że wojsko zastrzeliło 10 nieuzbrojonych policjantów. W sumie konflikt trwał ponad miesiąc, powodując powszechny chaos. Przywódca buntu dwa lata później próbował dokonać zamachu stanu – zginął podczas ataku na prezydenta, w którym prezydent został ciężko ranny, jednakże już po dwóch miesiącach powrócił do swych obowiązków[53].

Jak już nieraz było w historii najnowszej Timoru Wschodniego, także w 2006 r. część mieszkańców opuściła czasowo swe domy, by chronić się w prowizorycznych koczowiskach (ok. 130 tys. osób)[54]. I tym razem sytuację ratowała oenzetowska misja (UNMIT), choć wcześniej wydawało się, że młode państwo już zdecydowanie okrzepło. Okazało się jednak, że państwo wkroczyło w kolejną fazę, w której wrogami Wschodnich Timorczyków są oni sami dla siebie, a że kraj jest wieloetniczny, a wielu mieszkańców ma za sobą tragiczne przeżycia, o wzajemne obwinianie się jest bardzo łatwo. Wschodni Timorczycy nie mogą zrozumieć, dlaczego na sąsiednich wyspach kwitnie gospodarka turystyczna i nie ma eksplozji przemocy, a na tej małej podzielonej wyspie każdy, wydawałoby się nieistotny, problem przeradza się w potężny konflikt, niosąc śmierć i cierpienie ludzi. Czyżby Wschodni Timorczycy byli bardziej skłonni do posługiwania się przemocą niż mieszkańcy wielu innych wysp archipelagu?

Od 20 maja 2002 r. do 20 maja 2005 r. w Timorze Wschodnim w celu zapewnienia bezpieczeństwa w nowo powstałym państwie stacjonowały siły ONZ (UNMISET). Wiosną 2006 r. doszło do wspomnianego buntu ok. 600 żołnierzy i gwałtow-

---

52 Ł. Bonczol, op.cit., s. 177.

53 M. Janiszewski pisze, że bardzo długi przebieg zamachu nie został do dziś wyjaśniony i budzi wiele podejrzeń i wątpliwości, np. z pałacu prezydenckiego podczas zamachu nie telefonowano do odpowiednich służb, a wykonywano inne połączenia. M. Janiszewski, op.cit., s. 128–130.

54 Ł. Bonczol, op.cit., s. 177.

nych zamieszek, w wyniku których zginęło około 30 osób, a ponad 100 tys. było zmuszonych opuścić swoje domy. To sprawiło, że od 25 sierpnia 2006 r. do Timoru Wschodniego zaczęły przybywać po raz kolejny siły ONZ (UNMIT), które znajdowały się tam do 31 grudnia 2012 r. W latach następnych okazało się, że siły takie już w tym kraju nie muszą być angażowane, co napawa ostrożnym optymizmem.

W wielu państwach tzw. Trzeciego Świata, gdy państwo ze swymi instytucjami zawodzi, następuje zwrot w kierunku starych struktur etniczno-klanowych, co sprawia, że wracają również stare antagonizmy, zadawnione waśnie i dawne sposoby zadawania cierpienia osobom uznanym za wrogów.

W 2007 r. nieurodzaj doprowadził do śmierci kilku tys. osób, a wiele tysięcy osób uratowała pomoc żywnościowa ze strony organizacji międzynarodowych. W ostatnim dziesięcioleciu taka sytuacja już się nie powtórzyła, co również można uznać za sukces.

Po trzynastu latach od wyzwolenia spod indonezyjskiego panowania dało się w kraju zauważyć zmęczenie elitami wykształconymi za granicą, stąd sukces w wyborach prezydenckich w 2012 r. José Marii Vasconcelosa (od 2018 r. – premier). Poziom wykształcenia Wschodnich Timorczyków jest ciągle bardzo niski, choć wskaźnik analfabetyzmu sukcesywnie spada, a wysoki przyrost naturalny sprawia, że rezerwuar taniej niewykwalifikowanej siły roboczej szybko się powiększa. Czynnikiem odstraszającym zarówno inwestorów, jak i turystów jest realna przemoc oraz stereotypy dotyczące tego problemu[55].

Paradoksem jest, że w tak biednym kraju energia elektryczna jest bardzo droga, a wyłączenia prądu zdarzają się bardzo często. Ogromne nasłonecznienie sprawia, że przyszłością

[55] Potencjalny turysta może zrezygnować z wyjazdu do tego kraju choćby po przeczytaniu tekstów straszących zagrożeniem ze strony krokodyli, które cieszą się tam od wieków nabożną czcią.

może być wykorzystanie energii słonecznej, lecz wymagałoby to ogromnych nakładów. Rynek wewnętrzny jest ciągle mały i płytki (niewielka siła nabywcza mieszkańców i wysokie ceny towarów importowanych). Bieda sprawia, że jeszcze dziesięć lat temu aż 70% budżetu przeznaczano na walkę z ubóstwem, służbę zdrowia i oświatę[56], co oznaczało, że wydatki na inwestycje przynoszące zyski nie tylko w dłuższej, ale i w krótszej perspektywie były bardzo skromne.

Można założyć, że bardzo wielu mieszkańców Timoru Wschodniego u progu niepodległości nie zdawało sobie sprawy, iż żyją w jednym z najbiedniejszych państw świata i nawet najbardziej genialni politycy nie byliby w stanie tego zmienić w krótkim czasie, szczególnie w warunkach eksplozji demograficznej.

W 2000 r. konstytuanta wybrała język portugalski jako drugi język oficjalny, choć tylko 5% mieszkańców deklarowało posługiwanie się nim w domu[57]. Można tu zaznaczyć, że ten relikt kolonializmu przeszedł wówczas reanimację ze szkodą dla kraju – w świecie, w którym rola angielskiego wydaje się być niezachwiana, a nawet rosnąca.

Indonezyjczycy generalnie uważają, że granica, a właściwie dwie granice na wyspie Timor to relikt (efekt) kolonializmu, język portugalski również, tak jak katolicyzm. W przypadku Indonezji tych reliktów jest znacząco mniej. Upór Wschodnich Timorczyków sprawił, że pewne relikty kolonializmu okazały się pożądane, a zatem silniejsze, niż przypuszczano – i wydają się obecnie kwestią ponadczasową: granica państwowa na wyspie – sztuczna w sensie geograficznym, trudna komunikacyjnie (eksklawa Ocussi) i wyraźnie dzieląca – oraz katolicyzm, którego rola, jak wcześniej zaznaczono, ogromnie wzrosła w latach walki z indonezyjskim panowaniem; co do przyszłości języka portugal-

[56] Ł. Bonczol, op.cit., s. 174.

[57] Ibidem, s. 176.

skiego, to dziś trudno stwierdzić, jaka będzie jego rola za dwadzieścia czy pięćdziesiąt lat.

Czy w takim państwie jak Timor Wschodni może się zdarzyć, że politycy nie ulegną korupcji, nepotyzmowi czy zapędom autorytarnym? Dzieje najnowsze innych państw na podobnym poziomie rozwoju pokazują, że raczej nie, różnice mogą dotyczyć najwyżej skali zjawiska. Można z pewnością stwierdzić, że w ostatnich dziesięciu latach perspektywa dryfowania Timoru Wschodniego w kierunku tzw. państwa upadłego jednak się odwróciła, być może na stałe.

W 2003 r. rozpoczęły się procesy oskarżonych o akty przemocy dokonane w związku z referendum w 1999 r. Akt oskarżenia sporządzony przy współpracy agencji ONZ mówi o zbrodniach przeciwko ludzkości. Indonezja jednak – co było do przewidzenia – odmówiła wydania przywódców paramilitarnych bojówek winnych rozpętania terroru. Mimo funkcjonowania aż dwóch specjalnych komisji ds. zbrodni z okresu indonezyjskiej okupacji, do tej pory skazano tylko jedną osobę. Okazał się nią Martenus Bere, przywódca militarnej milicji oskarżanej o zbrodnie przeciwko ludzkości w 1999 r. Spędził on jednak za kratami zaledwie dwa miesiące.

Należy odnotować, że Timor Wschodni nie rozstał się z Indonezją na zasadach wrogości. W uroczystościach inaugurujących niepodległość uczestniczyła pani prezydent Indonezji, a wcześniej oba państwa zawarły dwie umowy. Ponadto Indonezja stała się gorącym zwolennikiem przystąpienia najbiedniejszego kraju Azji do ASEAN-u. W 2005 r. podpisano porozumienie w sprawie granicy z Indonezją. Mimo podkreślania tragizmu indonezyjskiej okupacji, czego przykładem może też być, oprócz wymienionych już specjalnych komisji, dobrze urządzone muzeum ruchu oporu przeciw indonezyjskim okupantom, Timor Wschodni jest w dużym stopniu skazany na swego jedynego lądowego sąsiada. Pierwszą wizytę prezydent elekt José Ra-

mos-Horta (również laureat Pokojowej Nagrody Nobla w 1996 r.) złożył w 2007 r. w Indonezji. Polityka zagraniczna Timoru Wschodniego opiera się jak dotąd na dwóch filarach – relacjach gospodarczych z Indonezją, która odpowiada za ponad połowę handlu zagranicznego, oraz intensywnej współpracy w sektorze bezpieczeństwa (szkolenia wojska, policji) ze stroną australijską. Coraz większą rolę w gospodarce, a pośrednio także w polityce odgrywa też trzeci gracz – Chiny, nawet jeżeli wschodniotimorscy politycy wolą o tym nie mówić zbyt głośno.

W 2005 r. powstał fundusz Timor-Leste Petroleum Fund, gromadzący zysk z ropy naftowej i gazu ziemnego. Ponad 90% finansów rządowych pochodzi z Petroleum Fund, co czyni go instrumentalnym źródłem utrzymania dla mieszkańców tego kraju. Timor-Leste Petroleum Fund jest wzorowany na norweskim suwerennym funduszu majątkowym. Na koniec 2017 r. jego saldo wyniosło 16,8 mld dol.[58] Norwegia była zresztą krytykowana za narzucanie Timorowi Wschodniemu swego modelu wykorzystywania dochodów oraz blokowania – wg amb. T. Łukaszuka – zdywersyfikowanego inwestowania.

Roczny budżet rządu wzrósł z 70 mln dol. w 2004 r. i 650 mln dol. w 2009 r. do 1,3 mld dol. w 2011 r. oraz 1,8 mld dol. zaproponowanych na 2012 r. – przy prawie wszystkich środkach pochodzących z Petroleum Fund[59]. Jednakże od 2018 r. wiele wskaźników makroekonomicznych uległo pogorszeniu. Drugim co do wielkości towarem eksportowym jest kawa, która generuje od 15 do 30 mln dol. rocznie. Głównym nabywcą kawy jest Starbucks Coffee Company. Timor Wschodni wyróżnia się jako najbardziej zależna od ropy naftowej gospodarka

[58] https://en.wikipedia.org/wiki/Timor-Leste_Petroleum_Fund [dostęp: 22.10.2019]; https://eiti.org/fr/implementing_country/40 [dostęp: 6.01.2020].

[59] International Monetary Fund, *Public Information Notice*, nr 11 (31), 8.03.2011, https://www.imf.org/en/News/Articles/2015/09/28/04/53/pn1131 [dostęp: 22.10.2019].

na świecie, dystansując nawet Arabię Saudyjską. W 2009 r. dochody z ropy naftowej stanowiły około 95% całkowitych dochodów rządowych i prawie 80% dochodu narodowego brutto.

Dużego znaczenia nabiera też uruchomiony w 2011 r. Fundusz Rozwoju Kapitału Ludzkiego. Niemal 200 mln dolarów przeznaczonych na jego aktywność w pierwszych pięciu latach ma zapewnić do 2030 r. odpowiedni pułap wykwalifikowanych specjalistów, których brak jest jedną z głównych przeszkód na drodze do stania się członkiem ASEAN-u[60]. Jest bowiem rzeczą powszechnie wiadomą, że w gospodarce oraz życiu politycznym i społecznym dobry system prawny to nie wszystko. Ważne jest wypełnienie różnych sfer odpowiednim czynnikiem ludzkim. Ogromnie ważne jest to, co społeczeństwo potrafi, jaka jest etyka pracy, relacje międzyludzkie, jakie są umiejętności w zakresie organizacji pracy. Pod tym względem sytuacja przedstawia się ciągle bardzo źle.

Znacznie lepiej przedstawia się kwestia sytuacji wewnętrznej, niegdyś bardzo niespokojnej. Timor Wschodni odniósł sukcesy, „zwalczając przestępczość zorganizowaną, ograniczając [inne – przyp. T.D.] wskaźniki przestępczości oraz wygaszając konflikty wynikające z etniczno-religijnego czy ideologicznego zróżnicowania osób zamieszkujących wyspę"[61]. „Z kolei w odniesieniu do polityki zewnętrznej młode państwo dało się poznać jako rzetelny partner i aktywny uczestnik licznych projektów międzynarodowych, dzięki którym zdobyło niezbędne doświadczenie na tej płaszczyźnie"[62].

---

[60] Należy też odnotować, że Timor Wschodni nie posiada własnej waluty, co zresztą skutecznie zapobiega hiperinflacji i powoduje oszczędzanie na emisji pieniądza.

[61] P. Soja, op.cit., s. 134.

[62] Ibidem, za: „The Asia Foundation" 2017, https://asiafoundation.org/publication/2017-survey-of-travelers-to-timor-leste/ [dostęp: 13.08.2018]; https://asiafoundation.org/2017/06/09/asia-foundation-marks-25-years-timor-leste/ [dostęp: 9.06.2017].

Problemem społecznym na znaczącą skalę jest ciągle „tradycyjna" przemoc domowa. Od 2009 r. jest ona karalna, jednak nadal większość mieszkańców tego kraju woli o niej nie mówić, a domowe akty agresji uznaje się za sprawę prywatną. Nie ma jednak danych porównawczych, by ustalić, jak ta przemoc ma się do przemocy domowej np. w Indonezji czy Papui-Nowej Gwinei. Inną kwestią patologiczną o ogromnym znaczeniu zdrowotnym jest nikotynizm. Timor Wschodni ma jeden z najwyższych wskaźników palenia papierosów na świecie, z prawie dwiema trzecimi uzależnionych mężczyzn.

Od 2009 r. wyniki gospodarcze i wskaźniki rozwoju społecznego były i można mieć nadzieję, że będą – w porównaniu z okresem wcześniejszym – bardzo dobre, jak na tamtejsze realia i oczekiwania za granicą. Odbywające się zgodnie z terminami wybory prezydenckie i parlamentarne (choć w 2018 r. wyborcy szli do urn zaledwie dziesięć miesięcy po poprzednich wyborach parlamentarnych) przebiegają bez zakłóceń, wyłaniając borykające się z rozmaitymi problemami, lecz stabilne rządy. Polityczni liderzy, przez lata skłóceni, potrafią przy tym budować szersze fronty porozumienia i współpracować z opozycją. Liberalny wizerunek wzmacniają wolne od cenzury media, rzadko spotykany w tych stronach globu całkowity zakaz kary śmierci czy rekordowy w skali kontynentu udział kobiet w parlamencie[63]. Już w 2004 r. ówczesny sekretarz generalny ONZ Kofi Annan stwierdził, że w Timorze Wschodnim ma miejsce stabilny postęp. Jak wiadomo, od tego czasu kraj ten przeżywał kilka dramatów, zatem wówczas był to optymizm przedwczesny. Nawet niedawno (2017/2018) miał miejsce kryzys parlamentarny i tym samym rządowy, kiedy Timor Wschodni niemal przez rok nie miał zatwierdzonego budżetu, co doprowadziło państwo

[63] P. Soja, op.cit., s. 131.

na skraj paraliżu[64]. Ciągle też można mówić o fatalnym stanie infrastruktury, choć dzięki chińskim inwestycjom zmiany na lepsze są zauważalne.

HAK, organizacja pozarządowa z Timoru Wschodniego, twierdzi w raporcie opublikowanym w „The Dili Weekly", że prawa człowieka są nagminnie łamane przez policjantów i żołnierzy. Nadużywają oni swojej władzy i stosują nieuzasadnioną przemoc. Według danych innej organizacji, Belun, w samym 2012 r. co najmniej piętnastu członków sił zbrojnych Timoru Wschodniego popełniło rażące naruszenia praw człowieka.

Innym problemem jest stan środowiska. Na ten temat można spotkać się ze skrajnie różnymi opiniami – od takich, że dominuje nienaruszona przyroda, do twierdzeń wręcz absurdalnych, że biedna ludność zjadła już niemal wszystkie dzikie zwierzęta z wyjątkiem nabożnie czczonych krokodyli, które zresztą stanowią odstraszające zagrożenie. Rzeczywiście niewiele jest skażeń chemicznych[65], ale środowisko można też dewastować w inny sposób, szczególnie gdy populacja szybko rośnie.

Timor Wschodni był wielokrotnie prezentowany jako kraj, który może czerpać coraz większe zyski z turystyki, a w tym z ekoturystyki. Rozwój turystyki (ekoturystyki) napotyka jednak na znaczące przeszkody, sprawiając, że jest to ciągle kraj dla nielicznej i specyficznej kategorii turystów. Brak dużych i dobrze utrzymanych miast jest w tym wypadku bardziej wadą niż zaletą, a niedorozwój infrastruktury komunikacyjnej jest ogromną przeszkodą w krótkim czasie nie do pokonania. Timor Wschodni nie będzie też jeszcze długo krajem rezydencjonalnym na znacząca skalę. Aktualnie jest znacznie gorszym miejscem do życia dla bogatych emerytów z różnych państw świata, którzy poszukują przyjaznego i atrakcyjnego miejsca do

[64] Ibidem, s. 134.

[65] Trudno stwierdzić, na jaką skalę zatruwa się wodę w akwenach cyjankiem, by następnie zbierać śnięte ryby. M. Janiszewski, op.cit., s. 75.

zamieszkania w sprzyjającym klimacie za pieniądze znacznie mniejsze niż w krajach ojczystych.

Podczas ostatnich wyborów parlamentarnych wyborcy byli przede wszystkim zainteresowani tym, żeby nowy rząd zapewnił im czystą wodę, stabilną elektryczność, lepsze drogi, dostęp do szkół, szpitali i – przede wszystkim – pracę[66]. Są to postulaty wyborców w większości państw tzw. Trzeciego Świata, a Timor Wschodni jest jednym z nich. Wyłoniony po wyborach rząd popadł w impas na wiele miesięcy, czego się wcześniej nie spodziewano. Tym razem nie wywołało to eksplozji przemocy, co jest godne odnotowania. Być może wschodniotimorskie społeczeństwo zmienia się na lepsze, widząc, że wojowniczość w warunkach pokoju jest dysfunkcjonalna.

Najnowsze dzieje Timoru Wschodniego pokazują dobitnie, że nie wszystkie pozostałości kolonializmu należy wykorzeniać. Timorczycy Wschodni nie chcą po prostu być Indonezyjczykami, nie chcą likwidacji granicy państwowej na wyspie, a właściwie dwóch granic; nie chcą też porzucić katolicyzmu, odwrócić się od języka portugalskiego choćby na rzecz angielskiego, od specjalnych relacji z Portugalią; nie chcą wreszcie zrezygnować z portugalskich imion i nazwisk.

Gdyby nie zyski z eksploatacji ropy naftowej i gazu ziemnego[67], Timor Wschodni prawdopodobnie byłby państwem bezterminowo uzależnionym od międzynarodowej pomocy, a właściwie subsydiowanym przez zagranicę. Byłby to wielki

[66] D. Sipiński, *Nastoletnie państwo dorasta. Timor Wschodni kończy 16 lat*, „Polityka", https://www.polityka.pl/tygodnikpolityka/swiat/1749314,1,nastoletnie-panstwo-dorasta-timor-wschodni-konczy-16-lat.read [dostęp: 20.05.2018].

[67] Korzyści z ropy naftowej i gazu ziemnego „trafiają głównie do Australii, która je wydobywa, przetwarza i sprzedaje dalej, łaskawie dzieląc się niewielką częścią zysków z Timorem [Wschodnim]". Ibidem. Według innej wersji: „W dniu podpisania deklaracji niepodległości Timoru Wschodniego wpływy z pola naftowego Greater Sunrise przyznane zostały w 90% Timorowi [Wschodniemu]". M. Janiszewski, op.cit., s. 46.

paradoks historii – państwo, które po latach okupacji zaistniało dzięki społeczności międzynarodowej, okazałoby się niezdolne do samodzielnego funkcjonowania. Na szczęście jego upadłość dziś zdecydowanie się oddaliła. W tym wypadku ropa naftowa nie okazała się przekleństwem, lecz zbawieniem. Należy jednak już teraz poważnie myśleć o czasach, kiedy zasoby się wyczerpią (jak czyni to od lat Brunei) i trzeba będzie radzić sobie bez tych potężnych, jak na tak mały kraj, dochodów, z populacją zdecydowanie większą niż obecnie i zapewne ciągle rosnącą. Dywersyfikacja gospodarki nie jest bowiem wyzwaniem, któremu można sprostać z roku na rok, nie mówiąc już o wyzwaniach społecznych. To ostatecznie kapitał społeczny samych Wschodnich Timorczyków zadecyduje o tym, jakim państwem będzie Timor Wschodni w epoce postpetrodolarowej.

* * *

Wielce istotną kwestią jest liczba ofiar indonezyjskiej okupacji. W obiegu, głównie publicystycznym, są różne dane, nierzadko nieuzasadnione. Oczywiście nie jest możliwe dokładne ustalenie liczby ofiar, ale szacunki też mogą być bardziej lub mniej racjonalne. Jak zawsze ostrożny w swych szacunkach Ben Kiernan z uniwersytetu Yale, od lat zajmujący się problematyką ludobójstwa, twierdzi że zginęło od 116 do 174 tys. osób. Co ciekawe, strona indonezyjska także przyznawała, że do 1979 r. mogło umrzeć 120 tys. mieszkańców[68]. Ponadto Timor Wschodni na przestrzeni lat pochłonął może nawet 20 tys. żołnierzy indonezyjskich[69]. Nie brakuje autorów, w tym uznanych publicystów, którzy podają zdecydowanie nieprawdziwe informacje na temat liczby ofiar. „W ciągu roku [sic!] zginęła

[68] Ł. Bonczol, op.cit., s. 96–97.

[69] Ibidem, s. 98.

1/3 ludności Timoru. Z 650 tysięcy mieszkańców przy życiu pozostało 420 tysięcy"[70]. „Indonezyjska okupacja kosztowała życie nawet 300 tys. wschodnich Timorczyków"[71]. „W 1976 r. oficjalnie wcielono Timor do Indonezji […] Tylko w tym roku w walkach zginęło prawie 200 tys. Timorczyków, czyli prawie 1/3 mieszkańców kraju"[72]. „Podczas przyłączania Timoru [Wschodniego] do Indonezji [czyli w pierwszym roku?! – T.D.] zostało zabitych i zmarło z powodu głodu lub chorób około 200 tys. mieszkańców – podają źródła kościelne"[73]. To też nie jest prawdą. Ten sam autor pisze też, że posąg Chrystusa zbudowali Indonezyjczycy przed 24 laty, czyli w 1976 r.; faktycznie stało się to dwadzieścia lat później.

Bibliografia

Bankowicz M., *Timor Wschodni: trudna droga do niepodległości*, „Tygodnik Powszechny" 1999, nr 37 (2618).

Bonczol Ł., *Timor Wschodni. Od reliktu kolonializmu do problemu międzynarodowego*, Wrocław 2008.

Grzymski S., *Państwo w inkubatorze*, „Rzeczpospolita" 2000, nr 216 (5686).

Janiszewski M., *Dom nad rzeką Loes*, Wołowiec 2014.

Korespondencja z ambasadorem tytularnym Tomaszem Łukaszukiem, kwiecień 2020.

Kubiak K., *Australijczycy na Timorze*, „Komandos" 2001, nr 2.

[70] *Timor Wschodni – wyspa podzielona przez historię*, PolskieRadio.pl; https://www.polskieradio.pl/39/156/Artykul/1211291,Timor-Wschodni-%E2%80%93-wyspa-podzielona-przez-historie [dostęp: 30.08.2016].

[71] P. Tarczyński, *Operacja Lotos. Jak Indonezja przejęła Timor Wschodni*, „Polityka" 2015, nr 50 (3039), s. 64.

[72] K. Kowalewska, *Timor Wschodni. Historia raju, o którym zapomniał świat*, https://kamieverywhere.com/timor-wschodni/ [dostęp: 12.01.2020].

[73] S. Grzymski, *Państwo w inkubatorze*, „Rzeczpospolita" 2000, nr 216 (5686), s. A6.

Kubiak K., *Australijczycy na Timorze (2)*, „Komandos" 2001, nr 3.
Kucharczyk G., *Chrześcijanie w Indonezji i Timorze Wschodnim*, „Miłujcie się!" 2006, nr 5.
Olszewski W., *Timor Wschodni i jego problemy*, „Sprawy Narodowościowe" 1996, t. V, z. 1 (8).
Pokorski K., *Konflikt o Timor Wschodni*, „Dolnośląski Ośrodek Studiów Strategicznych", czerwiec 2007.
Rozmowy z Grzegorzem Kucharczykiem, Murowana Goślina – Opole, maj 2019–kwiecień 2020.
Sorman G., *Nowe bogactwo narodów*, Łódź–Warszawa 1989.
Szostkiewicz A., *Wszystkich nie przyjmujemy. Rozmowa z ministrem spraw zagranicznych Australii Alexandrem Downerem*, „Polityka" 2002, nr 14 (2344).
Tarczyński P., *Operacja Lotos. Jak Indonezja przejęła Timor Wschodni*, „Polityka" 2015, nr 50 (3039).
Ureta J.A., *Tragiczna sytuacja w Timorze Wschodnim. Rozmowa z Lídią Gonçalves Soares*, „Polonia Christiana" 2011, nr 18.
Zybura G., *Dwadzieścia lat okupacji*, „Przegląd Tygodniowy" 1996, nr 43 (712).

Źródła internetowe

International Monetary Fund, *Public Information Notice*, nr 11 (31), 8.03.2011, https://www.imf.org/en/News/Articles/2015/09/28/04/53/pn1131.
Jan Paweł II w obronie pokoju w Timorze Wschodnim (opracowanie: „L'Osservatore Romano"), 5 wystąpień papieża, https://opoka.org.pl/biblioteka/W/WP/jan_pawel_ii/przemowienia/timor_1999.html.
Kaniecka A., *W Timorze Wschodnim policja i wojsko łamią prawa człowieka*, http://www.polska-azja.pl/w-timorze-wschodnim-policja-i-wojsko-lamia-prawa-czlowieka/.
Kowalewska K., *Timor Wschodni. Historia raju, o którym zapo-*

mniał świat, https://kamieverywhere.com/timor-wschodni/.

Lenarcik M., *Ciężkie życie w Timor-Leste*, Polityka Globalna.pl, http://www.politykaglobalna.pl/2009/11/ciezkie-zycie-w-timor-leste/.

Sipiński D., *Nastoletnie państwo dorasta. Timor Wschodni kończy 16 lat*, „Polityka", https://www.polityka.pl/tygodnikpolityka/swiat/1749314,1,nastoletnie-panstwo-dorasta-timor-wschodni-konczy-16-lat.read.

Soja P., *Droga Timoru Wschodniego do ASEAN – członek trzeciej generacji czy wieczny obserwator?*, „Teka of Political Science and International Relations" 2018, vol. 13, nr 1, https://journals.umcs.pl/teka/article/view/8417.

Szczerkowski P., *W Timorze Wschodnim rządzą maczety i sms-y*, Wyborcza.pl, http://wyborcza.pl/1,75399,3443217.html.

Świerczyńska K., *Rzeź w Timorze Wschodnim*, https://wiadomosci.dziennik.pl/swiat/artykuly/175793,rzez-w-timorze-wschodnim.html.

„The Asia Foundation" 2017, https://asiafoundation.org/publication/2017-survey-of-travelers-to-timor-leste/; https://asiafoundation.org/2017/06/09/asia-foundation-marks-25-years-timor-leste/.

Timor Wschodni – wyspa podzielona przez historię, Polskie Radio.pl; https://www.polskieradio.pl/39/156/Artykul/1211291,Timor-Wschodni-%E2%80%93-wyspa-podzielona-przez-historie.

Tortured Beginnings. Police Violence and the Beginnings of Impunity in East Timor, https://www.hrw.org/report/2006/04/19/tortured-beginnings/police-violence-and-beginnings-impunity-east-timor.

Witkowska M., *Z moich wypraw. Tam, gdzie ryż rośnie. Timor Wschodni (Timor-Leste)*, http://www.monikawitkowska.pl/blogi/z-moich-wypraw/734-timor-wschodni.

https://eiti.org/fr/implementing_country/40.
https://en.wikipedia.org/wiki/Timor-Leste_Petroleum_Fund.
https://www.szkolnictwo.pl/szukaj,Timor_Wschodni.

Abstrakt

Timor Wschodni jest jednym z najbardziej tragicznie doświadczonych krajów drugiej połowy XX wieku. Ta niegdyś cywilizacyjnie zacofana portugalska kolonia ogłosiła niepodległość w 1975 r., lecz już ponad tydzień później padła ofiarą wojsk indonezyjskich, które od początku popełniały morderstwa na ludności cywilnej i grabieże mienia na dużą skalę. Dla Indonezji Timor Wschodni jako odrębna jednostka polityczna był produktem kolonializmu, więc jego przejęcie miało na celu przezwyciężenie tej pozostałości. Granica, a właściwie dwie granice na wyspie Timor, katolicyzm, język portugalski – wszystko to dla Indonezji było wynikiem historycznej niesprawiedliwości, jaką był kolonializm. Mieszkańcy Timoru Wschodniego, a zwłaszcza partyzanci antyindonezyjscy, zostali poddani wyjątkowym represjom, którym towarzyszył głód. W wyniku polityki Indonezji w Timorze Wschodnim w ciągu około 25 lat mogło stracić życie nawet około 200 tys. osób. Paradoksalnie w tym okresie Indonezja dokonała znaczących inwestycji, które sprawiły, że Timor Wschodni jako 27. prowincja Indonezji stał się beneficjentem programów znacznie poszerzających edukację, opiekę zdrowotną oraz infrastrukturę drogową. W wyniku działań społeczności międzynarodowej oraz Timorczyków Wschodnich w kraju i na emigracji Timor Wschodni odzyskał niepodległość, lecz sytuacja gospodarcza i społeczna spowodowała, że konieczne były dalsze misje ONZ. Kraj ten – pozbawiony nawet własnej waluty – przez wiele lat był prawie całkowicie zależny od pomocy międzynarodowej. Dzięki zyskom z wydobycia morskich złóż ropy naftowej i gazu ziemnego jest teraz w stanie funkcjonować niezależnie, ale poziom życia absolutnej większości mieszkańców jest wciąż przerażająco niski, szczególnie w sytuacji eksplozji demograficznej. Oprócz poprawy kondycji gospodarczej w ostatnich latach kraj osiągnął także spokój społeczny i stabilność polityczną. Wcześniej czy później kraj ten z pewnością zostanie przyjęty do ASEAN-u jako ostatnie państwo regionu. Mieszkańcy Timoru Wschodniego – podsumowując 20 lat od referendum, po którym nastąpiły wyjątkowo brutalne represje, ale także stopniowe odradzanie państwowości – mają prawo do wielu rozczarowań. Niezależność stwarza bowiem jedynie określone

warunki, ale nie zapewnia automatycznie choćby namiastki dobrobytu, a nawet bezpieczeństwa.

Słowa kluczowe: Timor Wschodni, masowe represje, Indonezja, kolonializm, FRETILIN

Abstract

East Timor is one of the most tragically experienced countries of the second half of the 20th century. This formerly economically backward Portuguese colony declared independence in 1975, but more than a week later it fell victim to Indonesian troops, which from the beginning committed the murder of civilians and plunder of property on a large scale. For Indonesia, East Timor as a separate political entity was a product of colonialism, so its occupation was meant to overcome this residue. The border, or practically two borders on the island of Timor, Catholicism, Portuguese language – all this for Indonesia was the result of great injustice, which was colonialism. The inhabitants of Timor-Leste, and especially anti-Indonesian partisans, were subjected to exceptional repression, which was accompanied by famine. As a result of Indonesia's policies in Timor-Leste, around 200,000 people could even lose their lives in around 25 years. Paradoxically, Indonesia made investments that resulted in East Timor being the 27th province of Indonesia significantly expanding in education, health care and paved roads. As a result of the activities of the international community and East Timorians in the country and in exile, East Timor regained independence, but the economic and social situation meant that further UN missions were necessary. This country – deprived of even its own currency – for many years was almost completely dependent on international assistance. Thanks to the profits from the mining of offshore oil fields, it is now able to function independently, but the standard of living of the absolute majority of residents is still frighteningly low – and in a situation of demographic explosion. In addition to improving the economic situation, the country has also achieved social peace and political stability in recent years. Sooner or later this country will certainly be admitted to ASEAN. The inhabitants of Timor-Leste certainly – to sum up 20 years after the referendum, after which there was an extremely brutal repression, but also a gradual revival of East-Timorese statehood – have

the right to many disappointments. Independence creates only certain conditions, but it does not ensure prosperity or even security.

Keywords: East Timor, mass repression, Indonesia, colonialism, FRETILIN

Michał Bielecki
Polska Akademia Nauk

Zbrodnia bez nazwy? O zasadności użycia terminu *ludobójstwo* w odniesieniu do indonezyjskich masowych mordów z lat 1965–1966

Wprowadzenie

Nocą z 30 września na 1 października 1965 r. w Indonezji doszło do zamachu stanu. Grupa wojskowych średniego szczebla porwała, a wkrótce potem zabiła sześciu wysokich rangą generałów. Zamachowcy, nazywający się Radą Rewolucyjną, ogłosili że przejmują władzę w państwie, aby zapobiec kolejnemu przewrotowi, planowanemu przez prawicowych generałów wspieranych przez Stany Zjednoczone. Ich plany udaremnił generał Suharto, który przybył na miejsce wydarzeń i aresztował zaangażowanych w porwanie. Prezydent Sukarno został aresztowany w swojej rezydencji w Dżakarcie – oficjalnie ze względów bezpieczeństwa. Faktyczną władzę w państwie przejął Suharto. Winą za przeprowadzenie zamachu stanu oraz zamordowanie generałów obarczono członków Indonezyjskiej Partii Komunistycznej (*Partai Komunis Indonesia*, PKI) – trzeciej co do wielkości komunistycznej partii na świecie, liczącej nawet 3,5 mln członków[1]. Jedną z pierwszych decyzji gen. Suharto była delegalizacja PKI oraz eksterminacja jej członków i sympatyków.

[1] R. Mortimer, *Indonesian Communism Under Sukarno: Ideology and Politics, 1959–1965*, Jakarta 2006, s. 366.

Regularne masowe egzekucje rozpoczęły się w drugiej połowie października i trwały do połowy marca 1966 r. Nie jest znana dokładna liczba ofiar, eksperci najczęściej szacują ją na między 500 tys. a 1 mln. Kolejny milion osób aresztowano i przez lata poddawano torturom[2]. Sprawcami były specjalne eskadry armii indonezyjskiej, wyszkolone w tym celu cywilne bojówki i lokalni gangsterzy. Ofiarami padali członkowie PKI, ich rodziny, osoby związane z wieloma organizacjami stowarzyszonymi z PKI (np. związkami zawodowymi), etniczni Chińczycy. Czasem palono całe wioski. Sankcjonowane przez armię pogromy komunistów stawały się również pretekstem do rozwiązywania prywatnych konfliktów. Ta systemowa przemoc stała się fundamentem trwającego ponad trzy dekady reżimu *Orde Baru* (ind. Nowy Porządek). Wydarzenia te to jedna z najsłabiej zbadanych i opisanych zbrodni na masową skalę w dwudziestowiecznej historii świata. Nawet sama kwestia nazewnictwa, użycia adekwatnej terminologii przy opisie tych wydarzeń, budzi pewne kontrowersje.

Zbrodnia bez nazwy?

Termin „ludobójstwo" został stworzony przez Rafała Lemkina, polskiego prawnika żydowskiego pochodzenia, jeszcze w trakcie II wojny światowej, przez połączenie greckiego *genos* (lud, rasa, szczep, klan, rasa, plemię) z łacińskim przyrostkiem *cide* (morderstwo)[3]. Twórca pojęcia definiuje je jako „zniszczenie narodu lub grupy etnicznej"[4], a szerzej jako „skoordynowany plan różnorodnych działań, mających na celu unicestwienie grupy samej w sobie"[5].

[2] G. Wandita, *PREMAN NATION: Watching The Act of Killing in Indonesia*, „Critical Asian Studies" 2014, nr 1 (46), s. 168.

[3] R. Lemkin, *Rządy państw Osi w okupowanej Europie*, Warszawa 2013, s. 110.

[4] Ibidem.

[5] Ibidem.

Choć motywem do ukucia nowego terminu była potrzeba precyzyjnego opisania zbrodni dokonanych w czasie II wojny światowej, zjawisko to znane jest ludzkości od zarania dziejów. Jak słusznie zauważył Leo Kuper, pionier socjologii ludobójstwa – „słowo jest nowe, zbrodnia prastara"[6].

Do terminologii prawniczej pojęcie ludobójstwa zostało wprowadzone w 1948 r. za sprawą uchwalonej przez Zgromadzenie Ogólne Narodów Zjednoczonych Konwencji w sprawie zapobiegania i karania zbrodni ludobójstwa. Art. II tego dokumentu zawiera następującą definicję:

> „W rozumieniu Konwencji niniejszej ludobójstwem jest którykolwiek z następujących czynów, dokonany w zamiarze zniszczenia w całości lub części grup narodowych, etnicznych, rasowych lub religijnych, jako takich:
> a) zabójstwo członków grupy,
> b) spowodowanie poważnego uszkodzenia ciała lub rozstroju zdrowia psychicznego członków grupy,
> c) rozmyślne stworzenie dla członków grupy warunków życia, obliczonych na spowodowanie ich całkowitego lub częściowego zniszczenia fizycznego,
> d) stosowanie środków, które mają na celu wstrzymanie urodzin w obrębie grupy,
> e) przymusowe przekazywanie dzieci członków grupy do innej grupy"[7].

Na szczególną uwagę zasługuje brak kategorii „grupy politycznej", której zagłada mogłaby być zakwalifikowana jako ludobójstwo, co w przypadku indonezyjskiej masakry ma kluczowe znaczenie. To „poważne zaniedbanie"[8] czy wręcz „martwy

---

[6] L. Kuper, *Genocide. Its Political Use in the Twentieth Century*, New Haven 1982, s. 11.

[7] Dz.U. 1952, nr 2, poz. 9, art. 2.

[8] J.S. Morton, N.V. Singh, *The international legal regime on genocide*, „Journal of Genocide Research" 2003, nr 5 (1), s. 56.

punkt"[9] prawnej definicji zjawiska powstało wskutek wzmożonej debaty towarzyszącej procesowi powstawania i uchwalania Konwencji. Wśród argumentów przeciwników pojawiały się opinie, że charakter grup politycznych jest mniej stabilny i bardziej niejednorodny, a ich tło historyczne nie jest ugruntowane równie mocno, jak w przypadku grup narodowych, etnicznych czy religijnych. Zwracano również uwagę na dobrowolny i subiektywny charakter członkostwa w grupie o charakterze politycznym[10]. Te, wydawać by się mogło, merytoryczne argumenty, były w istocie częścią sporu o charakterze politycznym. W obawie przed fiaskiem całego projektu kategoria „grupy politycznej" została wykreślona z treści Konwencji, mimo że większość delegacji, z przedstawicielami Stanów Zjednoczonych na czele, była początkowo zwolennikami jej włączenia.

Podjęte po 1948 r. próby wprowadzenia szerszej definicji ludobójstwa do prawa międzynarodowego zostały udaremnione[11], kilka państw (Etiopia, Bangladesz, Kostaryka, Peru, Słowenia i Litwa) wprowadziło natomiast pojęcie ludobójstwa na tle politycznym do krajowych Kodeksów karnych[12].

Definicja ukuta wskutek politycznego konfliktu interesów wzbudziła ożywioną dyskusję wśród przedstawicieli nauk społecznych i humanistycznych – socjologii, politologii czy antropologii kultury – dotyczącą jej użyteczności i kompletności. Kwestia pominięcia grup politycznych w prawnej definicji i zasadność jej włączenia do pojęcia „ludobójstwa" definiowanego przez przedstawicieli nauk społecznych stała się jednym z głównych tematów debaty naukowej w obrębie tzw.

---

[9] B. Van Schaack, *The Crime of Political Genocide: Repairing the Genocide Convention's Blind Spot*, „Yale Law Journal" 1997, nr 7, t. 106, s. 2259.

[10] W.A. Schabas, *Genocide in International Law: The Crime of Crimes*, Cambridge 2009, s. 154–157.

[11] Więcej na ten temat: ibidem, s. 160–165.

[12] Ibidem, s. 161–162.

genocide studies. Definicja ukuta przez prawnika Rafała Lemkina i wprowadzona do języka prawa decyzją gremium o charakterze politycznym okazała się nieużyteczna wobec wyzwań i celów nauk społecznych – między innymi komparatywnych badań nad ludobójstwami. Powstało więc wiele nowych definicji, często bardziej inkluzywnych, włączających ludobójstwa na grupie o charakterze politycznym, ekonomicznym, społecznym czy też tzw. ludobójstwa kulturowe. Kwestia granic inkluzywności tego pojęcia jest jednak niezwykle wrażliwa – zbytnie rozszerzenie definicji prowadzić mogłoby do trywializacji tego zjawiska. ONZ-owska konwencja bywa również zawężana poprzez postrzeganie tego fenomenu wyłącznie przez pryzmat masowych mordów.

Leo Kuper, jeden z pierwszych badaczy uczestniczących w dyskusji nad potrzebą stworzenia nowej definicji, zauważa:

> „Będę postępować zgodnie z definicją ludobójstwa podaną w Konwencji. Nie oznacza to, że zgadzam się z tą definicją. Wręcz przeciwnie, uważam, że wykluczenie grup politycznych z listy grup chronionych jest poważnym pominięciem. We współczesnym świecie różnice polityczne są co najmniej tak samo istotną podstawą masakry i unicestwienia, jak różnice rasowe, narodowe, etniczne lub religijne. Ponadto, ludobójstwa przeciwko grupom rasowym, narodowym, etnicznym lub religijnym są na ogół konsekwencją konfliktów politycznych, lub są ściśle z nimi związane. Nie wydaje mi się jednak, aby pomocne było tworzenie nowych definicji ludobójstwa, gdy istnieje międzynarodowa definicja oraz Konwencja o ludobójstwie, która może stać się podstawą dla niektórych skutecznych działań, mimo że ogranicza ona podstawową koncepcję. Ponieważ jednak wykluczenie grup politycznych mogłoby wypaczyć moją analizę, będę swobodnie odnosić się (…) do działań likwidacyjnych lub eksterminacyjnych przeciwko nim”[13].

[13] „I shall follow the definition of genocide given in the Convention. This is not to say that I agree with the definition. On the contrary, I believe

Wielu badaczy, bez oporów, jakie wyrażał Kuper, zaproponowało nowe definicje ludobójstwa, które wbrew brzmieniu Konwencji uznają grupę polityczną jako możliwy cel ludobójstwa. Dla przykładu Jack Nusun Porter, w wydanej po raz pierwszy w 1982 r. *Genocide and Human Rights: A Global Anthology*, komentując prawną definicję pojęcia ludobójstwa zaznacza:

> „Nie zgadzam się z tą wąską definicją i wierzę, że ludobójstwo może obejmować eksterminację grup z przyczyn ściśle politycznych"[14].

Jeffrey S. Bachman w *The United States and Genocide. (Re) Defining the Relationship* postuluje następującą definicję:

> „Ludobójstwo to próba wyeliminowania, w całości lub w części, grupy narodowej, politycznej, społecznej, rasowej, kulturowej lub społeczno-ekonomicznej w celu zniszczenia jej jako takiej lub osiągnięcia określonego celu politycznego, społecznego lub gospodarczego. Członkostwo w którejkolwiek z wyżej wymienionych grup może być przypisane przez członków grupy lub sprawców. Metody, za pomocą których można popełnić ludobójstwo, obejmują zabijanie członków grupy; celowe narzucanie warunków, które mogą spowo-

a major omission to be in the exclusion of political groups from the list of groups protected. In the contemporary world, political differences are at the very least as significant a basis for massacre and annihilation as racial, national, ethnic or religious differences. Then too, the genocides against racial, national, ethnic or religious groups are generally a consequence of, or intimately related to, political conflict. However, I do not think it helpful to create new definitions of genocide, when there is an internationally recognized definition and a Genocide Convention which might become the basis for some effective action, however limited the underlying conception. But since it would vitiate the analysis to exclude political groups, I shall refer freely (...) to liquidating or exterminatory actions against them". L. Kuper, *Genocide. Its Political...*, op.cit., s. 39. Wszystkie przekłady cytatów zostały wykonane przez autora.

[14] „I disagree with this narrow definition and believe genocide can include the extermination of groups for strictly political beliefs". J.N. Porter, *What is Genocide? Notes Toward a Definition*, [w:] *Genocide and Human Rights: A Global Anthology*, red. idem, Lanham 1982, s. 9.

> dować śmierć członków grupy; oraz wprowadzanie zasad mających na celu usunięcie tożsamości kulturowej grupy, znanej również jako ludobójstwo kulturowe. Ludobójstwo może mieć miejsce w czasach pokoju i wojny, podczas gdy wojna agresywna łączy się ze zbrodnią ludobójstwa. Co więcej, zarówno nieuzbrojeni, jak i uzbrojeni – niewalczący i walczący – członkowie grupy docelowej kwalifikują się jako ofiary ludobójstwa"[15].

Ta dość szeroka definicja, jedna z wielu włączających grupy polityczne, została przytoczona nie bez powodu. W dalszej części swojej pracy Bachman jednoznacznie i stanowczo stwierdza, że indonezyjskie masakry można zaliczyć do kategorii ludobójstwa. Podrozdział zatytułowany „Did Indonesia commit genocide?" kończy krótkim i dobitnym zdaniem: „To jest ludobójstwo"[16].

Inne teorie nie starają się wyszczególnić poszczególnych typów grup, które mogą potencjalnie paść ofiarą ludobójstwa, kładąc nacisk na sam proces wyodrębnienia społeczności ofiar, który dokonywany jest arbitralną decyzją sprawców. Przykładem może być definicja proponowana przez Franka Chalka i Kurta Jonassohna:

---

[15] „I define genocide as the attempt to eliminate, in whole or in part, a national, political, social, ethnic, racial, cultural, or socioeconomic group with the purpose of destroying it as such or achieving a particular political, social or economic objective. Membership in any of the aforementioned groups may be assigned by the group's members or by the perpetrators. The methods by which genocide can be inflicted include killing members of the group; deliberately imposing conditions that are likely to cause the deaths of members of the group; and enacting policies that seek to erase the group's cultural identity, also known as cultural genocide. Genocide may occur in times of peace and war, with aggressive war sharing a nexus with the crime of genocide. Furthermore, both unarmed and armed – noncombatant and combatant – members of the targeted group qualify as victims of genocide". J.S. Bachman, *The United States and Genocide: (Re)Defining the Relationship*, Londyn–Nowy Jork 2018, s. 6.

[16] „This is genocide". Ibidem, s. 83.

> „Ludobójstwo jest formą jednostronnego masowego zabijania, w którym państwo lub inny organ zamierza zniszczyć grupę, której istnienie i członkostwo w niej określone jest przez sprawcę"[17].

Inne podejście do problemu wykluczenia grup politycznych z definicji prawnej ludobójstwa przyjęli Barbara Harff i Ted R. Gurr. Zamiast przekształcać istniejącą definicję, stworzyli nowy termin – *politicide*[18]. Pojęcie to ma jednak swoje niedoskonałości. Po pierwsze, jego użycie ograniczone jest do dyskursu akademickiego. Po drugie, jak zauważa Robert Cribb, jego forma może sugerować, że odnosi się ono do różnorakich przypadków morderstw politycznych, np. do zamachu (*assassination*)[19]. Zdaniem Martina Shawa wyodrębnienie masowych mordów na tle politycznym z kategorii ludobójstwa jest nieuzasadnione:

> „Jeśli »grupa polityczna« staje się celem zniszczenia w taki sam sposób, jak inne rodzaje grup, to z pewnością jest to również ludobójstwo"[20].

W swojej argumentacji Shaw wskazuje nie tylko na istotę procesu wyodrębniania grupy ofiar. Zauważa również, że elity polityczne wielokrotnie stawały się ofiarą ludobójstw, nawet jeśli ich tło nie było *stricte* polityczne:

---

[17] „Genocide is a form of one-sided mass killing in which a state or other authority intends to destroy a group, as that group and membership in it are defined by the perpetrator". F. Chalk, K. Jonassohn, *The History and Sociology of Genocide: Analyses and Case Studies*, New Haven–Londyn 1990, s. 23.

[18] B. Harff, T.F. Gurr, *Toward Empirical Theory of Genocides and Politicides: Identification and Measurement of Cases since 1945*, „International Studies Quarterly" 1988, vol. 32, nr 3, s. 359–371.

[19] R. Cribb, *Political Genocides in Postcolonial Asia* [w:] *The Oxford Handbook of Genocide Studies*, red. D. Bloxham, A.D. Moses, Oxford 2010, s. 446.

[20] "If a 'political group' is targeted for destruction in the same way as other kinds of group, then surely this is, likewise, genocide". M. Shaw, *What is Genocide?*, Cambridge 2015, s. 91.

> „Naziści zniszczyli opozycyjne organizacje polityczne, takie jak partie komunistyczne i socjalistyczne oraz związki zawodowe, eliminując je jako organizacje, więżąc, a nawet zabijając ich aktywistów, zanim wyeliminowali społeczność żydowską w Niemczech. Podczas okupacji Polski na celowniku nazistów znaleźli się najpierw polscy oficjele, a zwłaszcza klasa oficerska armii. Podczas inwazji na Związek Radziecki atakowali komunistów, a także jeńców wojennych i Żydów. Podczas ludobójstwa w Rwandzie nacjonaliści Hutu najpierw zabili polityków opozycji (w tym Hutu), zanim zaatakowali masę ludności Tutsi. W Bośni serbscy nacjonaliści wyeliminowali działaczy politycznych z chorwackich i bośniacko-muzułmańskich partii nacjonalistycznych jako pierwszy krok w eliminacji ludności chorwackiej i muzułmańskiej”[21].

Shaw wskazuje również, że w historii masowej przemocy istniały jednostkowe przypadki, w których eliminacja wspólnoty politycznej miała kluczowe znaczenie, definiując tym samym charakter całego zdarzenia. Jako przykład podaje między innymi indonezyjskie masakry z lat 1965–1966. Jak podkreśla, nawet te nieliczne przypadki nie powinny być rozpatrywane w oderwaniu od innych ludobójstw:

> „W pełni rozwinięte *politicide*, w których partia polityczna i otaczająca ją społeczność stają się głównym celem polityki destrukcji, nie różnią się jakościowo od innych ludobójstw, jako że klasa polityczna i inne elity zazwyczaj padają ofiarą ludobójstw. W tym sensie najlepiej wydaje się postrzegać *politicide* jako wariant ludobójstwa, a przemoc na tle poli-

[21] “The Nazis destroyed opposing political organizations like the Communist and Socialist parties and trade unions, eliminating them as organizations, imprisoning and even killing their activists, before they eliminated the Jewish community in Germany. In their occupation of Poland, the Nazis first targeted Polish officialdom, and especially the officer class of the army. In their invasion of the Soviet Union, they targeted Communists as well as prisoners of war and Jews. In Rwandan genocide, the Hutu nationalists first killed opposition politicians (including Hutus) before attacking the mass of the Tutsi population. In Bosnia, Serbian nationalists eliminated political activists of the Croatian and Bosnian-Muslim nationalist parties as the first step in the elimination of Croat and Muslim populations”. Ibidem, s. 91.

> tycznym jako ogólny wymiar ludobójstwa, w którym wrogowie polityczni są atakowani obok lub jako główny element etnicznych, klasowych lub innych wrogów społecznych"[22].

Wśród przekrojowych publikacji naukowych z zakresu socjologii i historii ludobójstwa można znaleźć takie pozycje, które wyraźnie stwierdzają, że indonezyjskiej zbrodni z lat 1965–1966 nie można zaklasyfikować jako ludobójstwo[23]. Wiele tego typu opracowań nie wspomina o tych wydarzeniach wcale. Jednym z wyjątków jest *The History and Sociology of Genocide. Analyses and Case Studies* Franka Chalka i Kurta Jonassohna. Proponowana przez nich definicja nie wyklucza ludobójstwa na tle politycznym, co więcej, wskazują oni na bardziej złożony charakter indonezyjskiej zbrodni:

> „Podczas gdy ludobójstwo to było skierowane przeciwko partii politycznej, miało osobliwy wydźwięk o charakterze etnicznym, religijnym i ekonomicznym. Etnicznym, ponieważ ataki rozprzestrzeniły się na wielu Chińczyków, którzy byli postrzegani nie tylko jako obcokrajowcy, ale także jako przedstawiciele komunistycznych Chin; religijnym, ponieważ muzułmanie, a także niektórzy chrześcijanie postrzegali komunistów jako wrogów Boga; ekonomicznym, ponieważ z jednej strony chińscy kupcy byli oskarżani o bogacenie się poprzez wykorzystywanie biednych mas, a z drugiej strony dlatego, że PKI opowiadała się za konfiskatą dóbr ziemskich i ich redystrybucją wśród biednych chłopów"[24].

---

[22] „Fully fledged politicides, in which a political party and the community that surrounds it becomes the prime target of a policy of destruction, are not qualitatively different from other genocides, while political and other elites are commonly targeted in genocides. In this sense it seems best to view *politicide* as a variant of genocide and *political targeting* as a general dimension of genocide, where political enemies are targeted alongside, or as the leading element of, ethnic, class or other social enemies". Ibidem, s. 92.

[23] Np. S. Totten, P.R. Bartrop (red.), *The Genocide Studies Reader*, Londyn–Nowy Jork 2009 lub L.M. Nijakowski, *Rozkosz zemsty: socjologia historyczna mobilizacji ludobójczej*, Warszawa 2013.

[24] „While this genocide was directed at a political party, it had curious overtones of an ethnic, religious, and economic character. Ethnic because the

To że wyraźne odróżnienie ludobójstw na tle religijnym, etnicznym, rasowym czy w końcu politycznym nie jest możliwe, podkreślał również Leo Kuper. Jak zauważa, nawet niemieckie zbrodnie z lat 30. i z czasu II wojny światowej stanowiły połączenie masowych mordów politycznych z masakrami na tle etnicznym i religijnym:

> „[…] Niemieckie okrucieństwa w latach 30. XX wieku i podczas II wojny światowej, które stały się impulsem do Konwencji o Ludobójstwie, były połączeniem masowych mordów politycznych z masakrami etnicznymi i religijnymi. Przeplatanie się elementu politycznego z masakrami rasowymi, etnicznymi lub religijnymi jest obecne w wielu współczesnych ludobójstwach. Przeplatanie to jest szczególnie widoczne w społeczeństwach pluralistycznych, to znaczy społeczeństwach składających się z różnych ras, grup etnicznych i/lub religijnych, charakteryzujących się przeszłymi gwałtownymi konfliktami i obecnymi wszechobecnymi podziałami”[25].

Czemu więc społeczność naukowa studiów nad ludobójstwem tak często pomijała indonezyjskie masakry w swoich pracach? Adam Jones, który w III wydaniu *Genocide: A Com-*

attacks spread to many Chinese, who were seen not only as foreigners, but also as representatives of communist China; religious because the Muslims and also some Christians saw the Communists as enemies of God; an economic because on the one hand Chinese traders were accused of growing rich by exploiting the poor masses and on the other hand because the PKI advocated the confiscation of landed estates and their redistribution to poor peasants”. F. Chalk, K. Jonassohn, op.cit., s. 382.

[25] „[…] the German atrocities in the 1930s and during the Second World War, which provided the stimulus for the Genocide Convention, combined political mass murder with ethnic and religious massacres. And the interweaving of the political with the racial, ethnic, or religious massacres persists in many of the contemporary genocides. The interweaving is especially marked in plural societies, that is to say, societies comprising people of different racial, ethnic, and/or religious groups and characterized by past violent conflicts and present pervasive cleavages”. L. Kuper, *The Prevention of Genocide*, New Haven–Londyn 1985, s. 126–127.

prehensive Introduction[26] zamieszcza tekst dotyczący omawianych wydarzeń (i sam określa je mianem ludobójstwa) podaje trzy możliwe przyczyny, dlaczego wydarzenia te zajmowały do niedawna (a po trosze wciąż zajmują) „co najwyżej marginalną pozycję w porównawczych studiach nad ludobójstwem"[27]. Po pierwsze, tzw. pryzmat zimnej wojny; po drugie, skupienie się społeczności *anti-genocide* w latach 80. i 90. na indonezyjskiej przemocy w Timorze Wschodnim; po trzecie, brak dostępu do dokumentacji świadczącej o charakterze i rozmiarach tej masakry. Na szczególną uwagę zasługuje argument dotyczący zimnej wojny. Nie jest tajemnicą, że wzmocnienie PKI, czy wręcz możliwość przekształcenia Indonezji w państwo komunistyczne, nie leżało w interesie tzw. bloku zachodniego. Jak pokazują odtajnione w 2017 r. dokumenty z archiwów amerykańskiej dyplomacji i wywiadu, dotyczące indonezyjskiej masakry z lat 1965–1966, Stany Zjednoczone miały szczegółową wiedzę na temat okoliczności dojścia do władzy generała Suharto i towarzyszącej temu eksterminacji członków i sympatyków PKI, jej brutalnego charakteru i skali[28]. Mimo tego zachodnie mocarstwa aktywnie wspierały nowy reżim, między innymi poprzez pomoc finansową udzielaną Indonezji przez Bank Światowy czy Międzynarodowy Fundusz Walutowy[29]. Wsparcie polityczne, ekonomiczne, logistyczne i militarne reżimu Suharto przez państwa bloku zachodniego szło w parze z charakterem

[26] A. Jones, *Genocide: A Comprehensive Introduction*, Londyn–Nowy Jork 2017.

[27] „[…] at best a marginal position in comparative genocide studies". Ibidem, s. 419.

[28] Więcej na ten temat: *U.S. Embassy Tracked Indonesia Mass Murder* 1965, National Security Archive, https://nsarchive.gwu.edu/briefing-book/indonesia/2017-10-17/indonesia-mass-murder-1965-us-embassy-files [dostęp: 12. 09.2019].

[29] Ł. Bonczol, *Zrozumieć Indonezję. Nowy Ład generała Suharto*, Warszawa 2012, s. 169–169.

doniesień medialnych czołowych tytułów prasy amerykańskiej. Noam Chomsky i Edward S. Herman w wydanym w 1988 r. *Manufacturing Consent: The Political Economy of the Mass Media* analizują język i treść artykułów prasowych na temat indonezyjskiej przemocy z 1965 r. oraz późniejszych wydarzeń w Timorze Wschodnim, porównując go do innych przypadków masowej przemocy, np. reżimu Pol Pota. Jak konkludują:

> „Pomoc militarna i ekonomiczna oraz ochrona dyplomatyczna ze strony Stanów Zjednoczonych trwała przez lata dyktatury Suharto, media zaś uznawały go za dobrego ludobójcę"[30].

Najbardziej pogłębioną argumentację na rzecz zaklasyfikowania omawianej zbrodni jako ludobójstwa przedstawili ci badacze, którzy zakwestionowali oczywisty na pozór fakt – że wydarzenia te należy traktować jako mordy na tle politycznym. Chronologicznie pierwszym i jednym z najgłośniejszych orędowników włączenia masakr indonezyjskich do kategorii ludobójstwa, również w świetle obowiązującej definicji prawnej, jest Robert Cribb, wybitny znawca współczesnej Indonezji. W artykule zatytułowanym *Genocide in Indonesia, 1965–1966*[31] wnikliwie analizuje kwestię czy te na pozór jednoznacznie polityczne mordy mogą być uznane za ludobójstwo. W swoich rozważaniach cofa się do czasów kolonialnych i do procesu kształtowania się nowego bytu państwowego – niepodległej Indonezji. Cribb zauważa, że u podstaw indonezyjskich ruchów nacjonalistycznych leży przekonanie o politycznym, a nie etnicznym charakterze nowego państwa. W indonezyjskim procesie naro-

[30] „U.S. military and economic aid and diplomatic protection continued throughout the years of the Suharto dictatorship, and the media's finding him a good genocidist followed accordingly". N. Chomsky, E. Herman, *Manufacturing Consent. The Political Economy of the Mass Media*, New York 1988, s. XL.

[31] R. Cribb, *Genocide in Indonesia, 1965–1966*, „Journal of Genocide Research" 2001, nr 3 (2), s. 219–239.

dowotwórczym wyróżnić można trzy główne nurty – islamizm, komunizm oraz nurt głoszący potrzebę stworzenia państwa opartego na zbudowanym przez Holendrów aparacie państwowym, z tą różnicą, że tym razem przynosić miał on korzyści obywatelom nowego państwa, a nie kolonialnym zarządcom[32]. Wszystkie trzy obozy dążyły do utworzenia nowoczesnego niepodległego państwa indonezyjskiego, które jednak miało działać według każdego z nich na innych zasadach. Ogłoszona w 1956 r. przez prezydenta Sukarno ideologia NASAKOM (*nasionalisme, agama, komunisme* – nacjonalizm, religia, komunizm) była próbą połączenia tych trzech nurtów. Wierzył on bowiem, że Indonezja przyszłości to nie efekt zwycięstwa jednego z nich, lecz raczej współistnienie różnych elementów indonezyjskiej tożsamości. Swoją rolę Sukarno upatrywał w kształtowaniu indonezyjskiej polityki tak, aby żaden z nurtów nie zdobył znaczącej przewagi. Wydaje się jednak, że to właśnie PKI była „największym beneficjentem demokracji sterowanej"[33], w kolejnych latach przechylając szalę wpływów na stronę ideologii komunistycznej. Siła tej masowej organizacji stopniowo wzrastała aż do momentu kulminacyjnego, czyli do 1965 r. Przedstawiając taką genezę ruchu komunistycznego w Indonezji, Cribb argumentuje, że masakry na indonezyjskich komunistach nie były zwykłą walką o władzę, lecz raczej o kształt nowego bytu państwowego. Czyni tym samym z grupy ofiar quasi-narodową społeczność:

> „Zabicie pół miliona komunistów było nie tylko intensywnym konfliktem politycznym, ale zubożeniem ideału narodowego, eksterminacją narodu, jaki istniał w umysłach milionów Indonezyjczyków"[34].

[32] Nurt ten określany jest przez Cribba jako *developmentalism*.

[33] Ibidem, s. 229.

[34] „The killing of half a million communists was not merely an intense political conflict, it was the impoverishment of a national ideal, the extermination of a nation as it has existed in the minds of millions of Indonesians". Ibidem, s. 237.

W wydanym w 2010 r. *The Oxford Handbook of Genocide Studies*[35] pod red. Donalda Bloxhama i A. Dirka Mosesa, Cribb kontynuuje rozważania nad zaliczeniem masakry w Indonezji do kategorii ludobójstwa, również w świetle treści Konwencji (obok masowych mordów w Chinach i Kambodży). W swojej argumentacji zwraca uwagę na fakt, że współczesna nauka odchodzi od jednoznacznego rozumienia etniczności jako zjawiska pierwotnego (a przynajmniej historycznego), w stronę rozumienia etniczności jako swoistej kreacji społecznej oraz wskazuje wiele podobieństw między tożsamością etniczną a polityczną. Tym samym definiowanie tożsamości etnicznej lub narodowej jako tej przyrodzonej, historycznej czy pierwotnej w opozycji do tożsamości politycznej, czyli tej, która pozostaje wyłącznie w kwestii osobistego wyboru, wydaje się nieadekwatne:

> „Te masowe mordy były próbą pozbycia się z ciała politycznego szerokiej grupy ludzi, których samo istnienie wydawało się zagrożeniem dla narodu w takim kształcie, jaki wyobrażali sobie sprawcy. Masowe mordy wydarzyły się w wyniku fundamentalnych konfliktów o charakter narodów Związku Radzieckiego, Indonezji, Chin i Kambodży. W każdym przypadku zwolennicy różnych frakcji uzgodnili fizyczne ramy w postaci granic państw, angażując się jednocześnie w walkę o przekształcenie podstaw charakteru narodu istniejącego w tych granicach. Zniszczenie politycznych wrogów w tych przypadkach nie było tylko przejęciem władzy lub interesów ekonomicznych, ale eksterminacją alternatywnego narodu wewnątrz państwa. Pod tym względem ofiary rzeczywiście stanowiły grupę »narodową« w rozumieniu konwencji ONZ"[36].

---

[35] R. Cribb, *Political Genocides in Postcolonial Asia,* [w:] *The Oxford Handbook of Genocide Studies*, red. D. Bloxham, A.D. Moses, Oxford 2010.

[36] „These mass killings were attempts to rid the body politics of a vast group of people, whose very existence seemed inimical to the nation the perpetrators conceived it. The mass killings arose from fundamental conflicts over the nation character of the Soviet Union, Indonesia, China and Cambodia. The protagonists in each case agreed on the physical framework

Z kolei Jess Melvin sugeruje, że indonezyjska przemoc może zostać nazwana ludobójstwem nawet w świetle definicji prawnej wyznaczonej przez Konwencję – jako masakra na tle religijnym. Po pierwsze, dlatego że duża część ofiar (komuniści *per se*) określana była przez wojsko jako ateiści. To oskarżenie było niejednokrotnie używane, aby rozbudzić niechęć społeczeństwa wobec grupy ofiar. Po drugie, ze względu na autoidentyfikację tej grupy – jako spadkobierców tzw. czerwonego islamu, czyli ideologii głoszącej kompatybilność islamu z komunizmem[37].

O tym, że charakter grupy ofiar trudno jednoznacznie określić mianem politycznego, świadczyć może również fakt, że przynależność do tej grupy była, a w pewnym stopniu wciąż jest, cechą dziedziczną. Wraz z mordowanymi członkami PKI czy organizacji z nią utożsamianych ginęły niejednokrotnie całe rodziny. Co więcej, stygmatyzacja rodzin osób zamordowanych lub uwięzionych (określanych w Indonezji mianem *ex-tapol* – *ex-tahanan politik,* byłych więźniów politycznych), nawet tych urodzonych po 1965 r., miała miejsce przez cały okres rządów gen. Suharto, a nawet po jego obaleniu w 1998 r. Członkowie rodzin o „komunistycznej przeszłości" nie byli dopuszczani do pracy w administracji publicznej, mediach, edukacji i innych sektorach kluczowych z punktu widzenia rządu – było to skutkiem wprowadzonej pod koniec lat 80. zasady *bersih lingkungan* (czystość środowiskowa)[38]. O dziedzicznym charakterze dyskryminacji wspominają niejednokrotnie byli więźniowie polityczni

provided by national borders, but they were engaged in a struggle to reshape the fundamentals of national character within those borders. The destruction of political enemies in these cases was not just a grab for factional power or economic interest, but the extermination of an alternative nation within the state. In these respect, the victims indeed constituted a 'national' group in the terms of UN Convention". Ibidem, s. 449–450.

[37] J. Melvin, *The Army and the Indonesian Genocide*, Londyn–Nowy Jork 2018, s. 45.

[38] R. Cribb, *Political Genocides…*, op.cit., s. 236.

i ich potomkowie, często określający swoje rodziny jako *keluarga PKI* (rodzina PKI)[39].

W samej Indonezji aż do upadku reżimu gen. Suharto[40] otwarta i merytoryczna dyskusja o masakrach z początku *Orde Baru* była niemożliwa – każda próba kwestionowania oficjalnej narracji grozić mogła poważnymi reperkusjami. Choć pierwsze, pojedyncze próby publicznego przełamania tabu miały miejsce jeszcze przed końcem reżimu, to dopiero tuż po jego zakończeniu nastąpiła znacząca zmiana. Początkowe lata okresu *reformasi* (okres po upadku dyktatury gen. Suharto) charakteryzowały się płynącą z wielu kręgów krytyką poprzedniego systemu oraz szerzej rozumianą demokratyzacją indonezyjskiego życia politycznego i społecznego. Tendencja ta nie trwała jednak długo. Jak zauważa jeden z czołowych indonezyjskich badaczy mordów z lat 1965–1966, Baskara T. Wardaya, już w kilka lat po upadku reżimu Suharto sytuacja wraca niemalże do stanu rzeczy charakterystycznego dla czasów *Orde Baru*[41]. Dynamikę zmian oficjalnej narracji obrazuje chociażby usunięcie nazwy partii z popularnego skrótu G30S/PKI w początkowej fazie okresu *reformasi*, a następnie w 2007 r. dodanie go z powrotem do szkolnego sylabusa[42]. Powołana w 2004 r. Komisja Prawdy i Pojednania została uznana przez indonezyjski Sąd Konstytucyjny za niekonstytucyjną[43]. W ostatnich latach miało miejsce wiele mniejszych incydentów, mających na celu utrzymanie *sta-*

[39] Autor w latach 2017–2018 przeprowadził szereg wywiadów z byłymi więźniami politycznymi i członkami ich rodzin oraz uczestniczył w wielu nieformalnych spotkaniach osób pokrzywdzonych.

[40] Suharto ustępuje z urzędu dopiero w 1998 r.

[41] B.T. Wardaya, wystąpienie na seminarium *1965 and the Indonesian Coup: Fifty Years on*, organizator: Australian Institute of international Affairs, nagranie dostępne: https://www.youtube.com/watch?v=56YJLxNKBGs [dostęp: 20.10.2019].

[42] J. Melvin, op.cit., s. 32.

[43] Ibidem.

tus quo oficjalnej narracji. W 2015 r. organizatorzy największego festiwalu literackiego w Azji Południowo-Wschodniej – *Ubud Writers and Readers Festival* – odwołali serię planowanych wydarzeń związanych z tematem masakry komunistów, między innymi projekcji głośnego dokumentu *Scena Ciszy*. Powodem podjęcia takiej decyzji miały być naciski ze strony władz[44]. W tym samym roku obywatel Szwecji pochodzenia indonezyjskiego został zatrzymany na ponad dobę, a następnie deportowany za odwiedzenie miejsca masowego pochówku ofiar antykomunistycznej rzezi, w tym swojego ojca[45]. W grudniu 2015 r. w Dżakarcie policja zabroniła organizacji publicznego odczytu i dyskusji nad dramatem pt. *Family Album: #50years1965* w ramach *Jakarta Theater Festival*[46]. W kwietniu 2016 r. rząd Republiki zorganizował dwudniowe ogólnonarodowe sympozjum zatytułowane *Dissecting the 1965 Tragedy*. Otwierający spotkanie minister-koordynator do spraw polityki, prawa i bezpieczeństwa Luhut Binsar Pandjaitan w dosadny sposób wyraził stosunek rządu Indonezji do często poruszanej kwestii oficjalnych przeprosin wystosowanych przez władze Republiki:

> „Nie jesteśmy aż tacy głupi. Nawet nie myślcie, że rząd będzie przepraszał za to czy tamto. Wiemy, że to, co robimy, jest najlepsze dla tego narodu"[47].

---

[44] Ni Komang Erviani, *Ubud cancels sessions on 1965 massacre*, „The Jakarta Post", https://www.thejakartapost.com/news/2015/10/24/ubud-cancels-sessions-1965-massacre.html [dostęp: 10.09.2019].

[45] S.Jb. Bachyul, *Man deported for visiting 1965 tragedy mass grave*, „The Jakarta Post", https://www.thejakartapost.com/news/2015/10/19/man-deported-visiting-1965-tragedy-mass-grave.html [dostęp: 11.10.2019].

[46] *Jakarta Police ban discussion of 1965 drama*, „The Jakarta Post", https://www.thejakartapost.com/news/2015/12/08/jakarta-police-ban-discussion-1965-drama.html [dostęp: 10.09.2019].

[47] „We are not that stupid. Don't even think that the government will apologize for this and that. We know what we are doing that is best for this nation". *Government will not apologize for 1965 massacre: Luhut*, „The Jakarta Post", https://www.thejakartapost.com/news/2016/04/18/government-will-not-apologize-for-1965-massacre-luhut.html [dostęp: 10.09.2019].

W czasie tego samego sympozjum za nieprawdziwą uznał opinię znakomitej większości ekspertów dotyczącą liczby ofiar, szacowanej zazwyczaj pomiędzy 500 tys. a 1 mln. „Nie wierzę, że liczba ofiar przekroczyła tysiąc. Prawdopodobnie było ich mniej”[48] – skomentował.

Zaplanowane na październik 2018 r. seminarium naukowe pt. *Historical Change and Continuity in a Scientific and Learning Perspective*, mające odbyć się na Malang State University, zostało odwołane w niejasnych okolicznościach. Według dziennika „The Jakarta Post” odwołanie konferencji nastąpiło wskutek nacisku dowództwa wojskowego miasta Malang, a powodem miała być obecność wśród mówców Asviego Warmana Adama – historyka prowadzącego badania nad masakrami z lat 1965–1966[49].

W świetle tak napiętej atmosfery nawet postępowi indonezyjscy badacze zachowują szczególną ostrożność. Poruszając temat masakr z lat 1965–1966 często określają je potocznym (używanym przez większość Indonezyjczyków, niejednokrotnie również przez pokrzywdzonych) określeniem *tragedi ’65* (tragedia ’65) czy też *peristiwa ’65* (wydarzenia ’65). Trudno nie zgodzić się z Jess Melvin, która zwraca uwagę, że popularyzacja terminu *tragedi* przyczynia się do ponownego kwestionowania tożsamości sprawców[50].

[48] „I don’t believe the number was more than 1,000; probably fewer”. *Open wounds*, „The Economist”, https://www.economist.com/asia/2016/04/23/open-wounds [dostęp: 10.09.2019].

[49] K.M. Tehusijarana, Putra Nedi AW, *Malang history seminar canceled after ‘discussion’ with military*, „The Jakarta Post”, https://www.thejakartapost.com/news/2018/10/11/malang-history-seminar-canceled-after-discussion-with-military.html [dostęp: 11.10.2019].

[50] J. Melvin, op.cit., s. 33.

Indonezyjska zbrodnia w polskich studiach nad ludobójstwem

Polskie studia nad ludobójstwem zdominowane są przez badania dotyczące Holocaustu. Jednym z niewielu polskich badaczy zajmujących się szeroko rozumianymi *genocide studies* czy też komparatystyką ludobójstw jest Lech Nijakowski. W *Rozkoszy zemsty*, przy okazji omówienia innego indonezyjskiego ludobójstwa – rzezi w Timorze Wschodnim w latach 1975–1999 – wspomina o wydarzeniach z początku rządów gen. Suharto. Nie zalicza ich jednak do kategorii ludobójstwa, lecz określa jako „terror polityczny na ludobójczą skalę"[51]. Wydaje się jednak, że wydarzenia z lat 1965–1966 spełniają wszystkie z kluczowych cech ludobójstwa, odróżniających je od innych masowych mordów, które sam Nijakowski wymienia, definiując to zjawisko:

„1. Dążenie do anihilacji wyróżnionej kategorii społecznej"[52].

Nijakowski zauważa, że podział na grupy „naturalne" (czyli np. rasowe, etniczne czy narodowe) oraz polityczne „wydaje się wątpliwy", bo nawet kategorie „naturalne" są „wynikiem specyficznego procesu definiowania społecznego" i „powstają w następstwie długiego procesu spontanicznego i celowego konstruowania"[53]. Jako przykład podaje kategorię Żydów w III Rzeszy. Jak zaznacza, „nie byli [oni] oczywistą, narzucającą się kategorią naturalną, ale specyficznym konstruktem, powstałym w czasie konfliktowego procesu, w którym ścierały się

[51] L.M. Nijakowski, op.cit., s. 179.

[52] Ibidem, s. 73.

[53] Ibidem.

racje nazistowskich ideologów rasowych, prawników i urzędników"[54], którzy arbitralnie decydowali o tym, kogo i na jakiej podstawie (wyznawanej religii, pochodzenia, wyników badań rasowych, danych gmin żydowskich) zaliczyć do tej kategorii. Kolejnym przykładem świadczącym o ułomności reguły podziału na grupy naturalne i polityczne, jaki podaje Nijakowski, są właśnie komuniści. Uważam, że przytoczona przez niego argumentacja doskonale opisuje grupę społeczną, która padła ofiarą indonezyjskiej rzezi:

> „Podobnie »komuniści« – wydaje się, że jest to kategoria jednoznacznie polityczna, łącząca działaczy wyznających ideologię komunistyczną i dążących do rewolucji. Tymczasem w praktyce za komunistów uznawano osoby, które nie miały pojęcia o podstawach marksizmu-leninizmu, maoizmu czy innej ideologii komunistycznej. Co więcej, uważano te jednostki za wrogie z natury – komunisty nie dało się „nawrócić" na właściwe poglądy, pozostawał on wiecznym buntownikiem, społecznym dewiantem, którego należało trwale usunąć ze społeczeństwa w imię jego dobrostanu"[55].

Znacząca część ofiar omawianej masakry nie miała bowiem dogłębnej lub żadnej wiedzy na temat ideologii komunistycznej. Jak zauważa Greg Barton, nawet ci aktywnie działający w PKI „nie byli zaznajomieni ze wszystkimi, poza najbardziej elementarnymi ideami komunizmu"[56]. Wielu z tych, którzy należeli do PKI czy też do innych organizacji z nią stowarzyszonych lub kojarzonych, byli często bardzo słabo wykształconymi, czasem niepiśmiennymi mieszkańcami wsi. Wiele ofiar nie było członkami żadnej z powyższych organizacji. Postrzegani byli jako „komuniści" wskutek arbitralnej decyzji sprawców,

---

[54] Ibidem, s. 74.

[55] Ibidem.

[56] „(…) were unfamiliar with all but the most basic ideas of Communism". G. Barton, *Abdurrahman Wahid: Muslim democrat, Indonesian president*, Sydney 2002, s. 90.

często nieznajdującej potwierdzenia w rzeczywistości. Nie dawano też ofiarom szansy na „nawrócenie" – partia miała być zlikwidowana „do samych korzeni" (termin ten użyty został po raz pierwszy przez gen. Suharto już pierwszego października 1965 r., na antenie rządowej stacji radiowej, potem wielokrotnie powtarzany przez czołowych indonezyjskich wojskowych i duchownych[57]). Ofiarami padały niejednokrotnie również rodziny „komunistów", a stygmatyzacja miała charakter dziedziczny.

„2. Niedyskryminacyjne zabijanie"[58].

Wśród ofiar byli dorośli, dzieci, osoby wykształcone i niepiśmienne, zamożne i ubogie. Bywało, że sprawcy palili całe wioski.

„3. Zanegowanie możliwości zmiany kategorii społecznej"[59].

PKI została zdelegalizowana tuż po zamachu stanu z przełomu września i października 1965 r. Mordy rozpoczęły się praktycznie bezzwłocznie i trwały zazwyczaj kilka miesięcy. Wystąpienie z partii (która faktycznie już nie istniała) nie było możliwe. Deklaratywna zmiana poglądów nie skutkowała ocaleniem. Osoby zakwalifikowane przez sprawców do kategorii ofiar nie miały możliwości „odwołania się" od tej decyzji[60].

„4. Lekceważenie indywidualnych zasług ofiar dla zbiorowości sprawców"[61].

W przypadku omawianej masakry nie jest łatwo precyzyjnie

[57] Więcej na temat języka używanego przez liderów oprawców i jego zbieżności z typową dla zjawiska ludobójstwa retoryką patrz: G. Robinson, *Down to the Very Roots: The Indonesian Army's Role in the Mass Killings of 1965–66*, „Journal of Genocide Research" 2017, nr 19 (4), s. 465–486.

[58] L.M. Nijakowski, op.cit., s. 74.

[59] Ibidem.

[60] J. Melvin, op.cit., s. 44.

[61] L.M. Nijakowski, op.cit., s. 75.

zdefiniować zbiorowość sprawców w opozycji do zbiorowości ofiar. Wynika to między innymi z tego, że zarówno ofiary, jak i sprawcy to obywatele Indonezji. W obu grupach znajdowały się osoby pochodzące z najróżniejszych grup etnicznych, różnych wyznań, mówiące różnymi językami, wykonujące różne zawody. Choć masakry zostały zaplanowane i zainicjowane przez indonezyjskie wojsko, które również wiodło prym w przeprowadzaniu mordów, także cywile brali udział w pogromach. I tak sąsiedzi zabijali sąsiadów, niejednokrotnie zasłużonych dla lokalnych społeczności. Nauczyciele oraz intelektualiści szczególnie często padali ofiarą przemocy[62]. Wśród ofiar znajdowali się również przedstawiciele indonezyjskiej elity politycznej, kulturalnej, naukowej i artystycznej.

„5. Zamknięcie drogi ucieczki"[63].

Nie jest znana liczba osób, które zdołały opuścić Indonezję w obawie przed reperkusjami, ale była ona z pewnością nieznaczna. Sprawcy zainteresowani byli jak najszybszym ujęciem wszystkich członków i sympatyków PKI. Lotniska kontrolowane były przez wojsko[64]. Ambasady monitorowały indonezyjskich obywateli przebywających za granicą – wielu indonezyjskich obywateli, którzy uznani zostali za sprzymierzonych z PKI, utraciło indonezyjskie paszporty[65].

Wydaje się, że używając tej samej, zaproponowanej przez Nijakowskiego definicji ludobójstwa, doszliśmy do przeciwnych wniosków. Uważam, że wydarzenia z Indonezji z lat

---

62 R. Cribb, *Political Genocides…*, op.cit., s. 233.

63 L.M. Nijakowski, op.cit., s. 75.

64 K. McGregor, *Heads from the North: Transcultural Memorialization of the 1965 Indonesian Killings at the National Gallery of Australia*, [w:] *The Indonesian Genocide of 1965: Causes, Dynamics and Legacies*, red. K. McGregor, J. Melvin, A. Pohlman, Londyn 2017, s. 238.

65 V. Herman, *The last men in Havana: Indonesian exiles in Cuba*, „Review of Indonesian and Malaysian Affairs" 2010, vol. 44, nr 1, s. 85–87.

1965–1966 spełniają wszystkie z wyżej wymienionych kryteriów. Nijakowski konkluduje jednak, że indonezyjską przemoc określić można jako „zbrodniczą walkę o władzę"[66]. Z pewnością nie zgodziłby się z tą opinią Robert Cribb, który stanowczo stwierdza, że uwięzienie lub zamordowanie kilku tysięcy najważniejszych działaczy PKI przyniosłoby armii pewne zwycięstwo[67]. Żądza przejęcia władzy nie wyjaśnia zatem wyczerpująco skali i charakteru tej masakry.

Według Nijakowskiego niespełnione zostały dwie z przytoczonych powyżej głównych cech ludobójstwa: „lekceważenie indywidualnych zasług ofiar dla zbiorowości sprawców" i „zanegowanie możliwości zmiany kategorii społecznej". Nijakowski pisze, że w przypadku indonezyjskich masakr istniała możliwość „politycznej konwersji" oraz że zasługi wrogów politycznych dla sprawców były uznawane. Nie podaje jednak konkretnych przykładów lub źródeł potwierdzających tę tezę, trudno więc się do niej odnieść.

Podsumowanie

Czy to, co wydarzyło się w Indonezji w latach 1965–1966 było ludobójstwem? Prosta odpowiedź na tak postawione pytanie nie jest możliwa, głównie dlatego, że zjawisko ludobójstwa nie ma jednej powszechnie uznawanej definicji. Ponadto nie jest łatwo „zrozumieć Indonezję". Wydaje się, że do najciekawszych wniosków doszli ci nieliczni badacze, którzy szeroką znajomość różnorakich aspektów ludobójstwa jako zjawiska, łączą z pogłębioną wiedzą dotyczącą współczesnej Indonezji, jej historii, sceny politycznej i społeczeństwa. Istotna wydaje się również refleksja nad udziałem państw trzecich w tej zbrodni. Rzuca ona cień nie

[66] L.M. Nijakowski, op.cit., s. 178.

[67] R. Cribb, *Political Genocides…*, op.cit., s. 235.

tylko na jej charakter, ale również na to, w jakich kategoriach jest ona postrzegana/definiowana. Uważam, że użycie terminu ludobójstwa w odniesieniu to tej zbrodni, jednej z największych w powojennej historii świata, jest nie tylko słuszne i zasadne w świetle wielu teorii, a jak argumentują niektórzy badacze również pod względem prawnym, ale przede wszystkim użyteczne i pomocne w trwającym procesie rozliczania tej trudnej przeszłości.

Bibliografia

Bachman J.S., *The United States and Genocide: (Re)Defining the Relationship*, Londyn 2018.

Bachyul S. Jb., *Man deported for visiting 1965 tragedy mass grave*, „The Jakarta Post", https://www.thejakartapost.com/news/2015/10/19/man-deported-visiting-1965-tragedy-mass-grave.html.

Barton G., *Abdurrahman Wahid: Muslim democrat, Indonesian president*, Sydney 2002.

Bonczol Ł., *Zrozumieć Indonezję. Nowy Ład genera*ła Suharto, Warszawa 2012.

Chalk F., Jonassohn K., *The History and Sociology of Genocide: Analyses and Case Studies*, New Haven–Londyn 1990.

Chomsky N., Herman E., *Manufacturing Consent. The Political Economy of the Mass Media*, New York 1988.

Cribb R., *Genocide in Indonesia, 1965–1966*, „Journal of Genocide Research" 2001, nr 3 (2).

Cribb R., *Political Genocides in Postcolonial Asia*, [w:] *The Oxford Handbook of Genocide Studies*, red. D. Bloxham, A.D. Moses, Oxford 2010.

Government will not apologize for 1965 massacre: Luhut, „The Jakarta Post", https://www.thejakartapost.com/news/2016

/04/18/government-will-not-apologize-for-1965-massacre--luhut.html.

Harff B., Gurr T.F., *Toward Empirical Theory of Genocides and Politicides: Identification and Measurement of Cases since 1945*, „International Studies Quarterly" 1988, vol. 32, nr 3.

Herman V., *The last men in Havana: Indonesian exiles in Cuba,* „Review of Indonesian and Malaysian Affairs" 2010, vol. 44, nr 1.

Jakarta Police ban discussion of 1965 drama, „The Jakarta Post", https://www.thejakartapost.com/news/2015/12/08/jakarta-police-ban-discussion-1965-drama.html.

Jones A., *Genocide: A Comprehensive Introduction*, Londyn––Nowy Jork 2017.

Konwencja w sprawie zapobiegania i karania zbrodni ludobójstwa, uchwalona przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 9 grudnia 1948 r. (ratyfikowana zgodnie z ustawą z dnia 18 lipca 1950 r.). Dz.U. 1952, nr 2, poz. 9, art. 2.

Kuper L., *Genocide. Its Political Use in the Twentieth Century*, New Haven 1982.

Kuper L., *The Prevention of Genocide*, New Haven–Londyn 1985.

Lemkin R., *Rządy państw Osi w okupowanej Europie*, Warszawa 2013.

McGregor K., *Heads from the North: Transcultural Memorialization of the 1965 Indonesian Killings at the National Gallery of Australia*, [w:] *The Indonesian Genocide of 1965: Causes, Dynamics and Legacies*, red. K. McGregor, J. Melvin, A. Pohlman, Londyn 2017.

Melvin J., *The Army and the Indonesian Genocide*, Londyn––Nowy Jork 2018.

Mortimer R., *Indonesian Communism Under Sukarno: Ideology and Politics, 1959–1965*, Jakarta 2006.

Morton J.S., Singh N.V., *The international legal regime on genocide*, „Journal of Genocide Research" 2003, nr 5 (1).

Ni Komang Erviani, *Ubud cancels sessions on 1965 massacre*, „The Jakarta Post", https://www.thejakartapost.com/news/2015/10/24/ubud-cancels-sessions-1965-massacre.html.

Nijakowski L.M., *Rozkosz zemsty: socjologia historyczna mobilizacji ludobójczej*, Warszawa 2013.

Open wounds, „The Economist", https://www.economist.com/asia/2016/04/23/open-wounds.

Porter J.N., *What is Genocide? Notes Toward a Definition*, [w:] *Genocide and Human Rights: A Global Anthology*, red. J.N. Porter, Lanham 1982.

Robinson G., *Down to the Very Roots: The Indonesian Army's Role in the Mass Killings of 1965–66*, „Journal of Genocide Research" 2017, nr 19 (4).

Schabas W.A., *Genocide in International Law: The Crime of Crimes*, Cambridge 2009.

Shaw M., *What is Genocide?*, Cambridge 2015.

Tehusijarana K.M., Putra Nedi AW, *Malang history seminar canceled after 'discussion' with military*, „The Jakarta Post", https://www.thejakartapost.com/news/2018/10/11/malang-history-seminar-canceled-after-discussion-with-military.html.

Totten S., Bartrop P.R. (red.), *The Genocide Studies Reader*, Londyn–Nowy Jork 2009.

U.S. Embassy Tracked Indonesia Mass Murder 1965, National Security Archive, https://nsarchive.gwu.edu/briefing-book/indonesia/2017-10-17/indonesia-mass-murder-1965-us-embassy-files.

Van Schaack B., *The Crime of Political Genocide: Repairing the Genocide Convention's Blind Spot*, „Yale Law Journal" 1997, vol. 106, nr 7.

Wandita G., *PREMAN NATION: Watching The Act of Killing in Indonesia*, „Critical Asian Studies" 2014, nr 1 (46).

Wardaya B.T., Wystąpienie na seminarium „1965 and the Indonesian Coup: Fifty Years on", organizator: Australian Institute of International Affairs, nagranie dostępne: https://www.youtube.com/watch?v=56YJLxNKBGs.

Abstrakt

Indonezyjska przemoc z lat 1965–1966 to jedna z największych „tragedii", jakie wydarzyły się na świecie po II wojnie światowej. Słowo „tragedia" nie oddaje jednak precyzyjnie charakteru ani skali tych wydarzeń. W zaledwie kilka miesięcy ginie około pół miliona ludzi, nawet milion osób zostaje uwięzionych. W skutek wzmożonego ostatnimi czasy zainteresowania badaczy tą masakrą, często określaną mianem „przemilczanej", wiedza na jej temat jest dziś znacznie większa, niż jeszcze kilka lat temu. Wciąż nie istnieje jednak pełna zgoda czy „ludobójstwo" to właściwy termin do opisu tych wydarzeń. W poniższym artykule wskazane zostaną rozmaite przyczyny, dla których takiego konsensusu nie udało się osiągnąć. Źródła części z nich można dopatrywać się w różnicach między definicją prawną terminu a alternatywnymi definicjami postulowanymi przez badaczy. Kolejne wątpliwości wywodzą się z pewnych przekonań, będących pozostałością utrzymującego się przez dziesięciolecia ubogiego stanu wiedzy na temat przebiegu masakr. Autor pokazuje jednak, że niezależnie od kształtu przyjętej definicji, pogłębiona analiza wydarzeń pozwala ten konflikt rozstrzygnąć na korzyść stosowania terminu „ludobójstwo" w kontekście wydarzeń z lat 1965–1966.

Słowa kluczowe: Indonezja, ludobójstwo, PKI, 1965

Abstract

The Indonesian violence of 1965–1966 is one of the biggest atrocities of post World War II history. However, the term „atrocity" does not

precisely reflect the nature and scale of those events. Within just a few months, about half a million people were killed. As much as a million were imprisoned. Due to recent intensification of researchers' interest in this massacre, often referred to as „silent" one, knowledge about it is much deeper today than it was a few years ago. However, there is still no full agreement as to whether „genocide" is the right term to describe these events. The following article will indicate the various reasons why such a consensus has not been achieved. The sources of some of them can be seen in the differences between the legal definition of the term and alternative definitions postulated by scholars. Further doubts come from certain beliefs, which are the remains of a poor state of knowledge about the course of the massacres that persisted for decades. Nonetheless, the author shows that regardless of the adopted definition, an in-depth analysis of that violence allows this conflict to be resolved in favor of the term „genocide" as the legitimate one in that case.

Keywords: Indonesia, genocide, PKI, 1965