Artem Koblyk
e-mail: 170619@student.ue.wroc.pl

Uniwersytet Ekonomiczny we Wrocławiu

Analiza stanu bezpieczeństwa informacyjnego na podstawie *National Cyber Power Index*

JEL Classification: H56, P48, C3
DOI: 10.15611/2022.17.6.04

Streszczenie: W artykule podjęto problematykę funkcjonowania systemu bezpieczeństwa informacyjnego jako podstawy bezpieczeństwa narodowego państwa i społeczeństwa. Przeanalizowano, czy stałe i systematyczne wzmacnianie i rozwój bezpieczeństwa informacyjnego powinny być jednymi z najbardziej priorytetowych kierunków polityki państwa. Głównym celem badania było stwierdzenie, czy system zapewniania bezpieczeństwa informacyjnego zajmuje ważne miejsce w systemie zapewnienia bezpieczeństwa militarnego państwa. Wykorzystano do tego celu analizę kanoniczną. Stwierdzono, że rozwój kraju jest wyjaśniany przez elementy składowe cyberbezpieczeństwa narodowego, tzn. wzrost poziomu bezpieczeństwa informacyjnego, a w szczególności cyberbezpieczeństwa, przyczynia się do rozwoju kraju na płaszczyźnie społecznej, gospodarczej oraz politycznej.

Słowa kluczowe: cyberbezpieczeństwo, NCPI, analiza kanoniczna.

1. Wstęp

Na początku XXI wieku na świecie zaszły radykalne zmiany w prowadzeniu wojen i konfliktów zbrojnych. Istotnie zmieniły się nie tylko ich cele polityczne, ale także sposoby ich prowadzenia oraz używane w tym celu środki walki. W warunkach globalnej integracji i zaciekłej konkurencji międzynarodowej strefa informacyjna staje się głównym obszarem starć i zmagań różnych narodowych interesów państw. Geopolityczna rywalizacja w społeczeństwie informacyjnym wymaga rewizji priorytetów dotyczących organizacji systemu bezpieczeństwa narodowego, nowego spojrzenia na problemy konfrontacji informacyjnej, a także zrozumienia roli oddziaływania informacyjno-psychologicznego na społeczeństwo i jednostki społeczne.

Jak wskazują Khudarkovskyi, Pievtsov, Sidchenko i Zalkin (2020), konfrontacja informacyjna rozumiana jest jako walka w sferze informacyjnej, która zakłada kompleksowe działania wpływające destrukcyjnie na informacje, systemy informacyjne i infrastrukturę informacyjną strony przeciwnej przy jednoczesnej ochronie własnych informacji, systemów informacyjnych i infrastruktury informacyjnej przed tymi działaniami. Ostatecznym celem wojny informacyjnej jest zdobycie i utrzymanie przewagi informacyjnej nad stroną przeciwną.

Biorąc pod uwagę rosnące znaczenie i wpływ jakości informacji na losy konfliktów zbrojnych, konieczne jest przedstawienie zagadnień dotyczących bezpieczeństwa informacyjnego oraz cyberbezpieczeństwa. Cyberbezpieczeństwo charakteryzuje poziom bezpieczeństwa informacyjnego państwa, służy do oceny gotowości kraju do przeciwdziałania różnym zagrożeniom cybernetycznym oraz wzmacniania jego zdolności do zarządzania różnymi incydentami cybernetycznymi.

Pozwoliło to w rezultacie na skonstruowanie celu przeprowadzonego badania, czyli sprawdzenie, czy bezpieczeństwo informacyjne zajmuje czołowe miejsce w strukturze globalnego bezpieczeństwa militarnego konkretnych państw.

2. Bezpieczeństwo informacyjne oraz cyberbezpieczeństwo jako podstawowe elementy systemu bezpieczeństwa narodowego

Sfera informacyjna stała się jednym z czynników systemotwórczych w życiu społecznym i aktywnie wpływa na stan bezpieczeństwa politycznego, gospodarczego, obronnego i innych elementów bezpieczeństwa państwa. Dlatego, wykorzystując informację, należy mieć pewność, że jest ona wiarygodna, a w procesie jej przekazywania i rozpowszechniania nie została zniekształcona. Bezpieczeństwo informacyjne jest zatem ważnym elementem całego systemu bezpieczeństwa narodowego kraju (Zadiraka, 2014).

Bezpieczeństwo informacyjne jest zjawiskiem złożonym, systemowym, wieloaspektowym, na które bezpośredni wpływ mają czynniki zewnętrzne i wewnętrzne, wśród których najważniejszymi są (Havryltsiv, 2020):

- sytuacja polityczna na świecie;
- obecność potencjalnych zagrożeń zewnętrznych i wewnętrznych;
- stan i poziom rozwoju informacyjno-komunikacyjnego w danym państwie;
- wewnętrzna sytuacja polityczna w kraju.

Zgodnie z badaniem Bogdanovicha, Marko i Vorovicha (2018) stan bezpieczeństwa informacyjnego charakteryzuje się wzrostem skali stosowania technologii informacyjnych zarówno przez poszczególne państwa, jak i organizacje międzynarodowe w celach militarno-politycznych. Technologie te mają za zadanie przede wszystkim prowadzenie działań sprzecznych z prawem międzynarodowym, ukierunkowanych na podważanie suwerenności, stabilności politycznej i społecznej, integralności terytorialnej oraz stanowiących zagrożenie dla pokoju światowego, bezpieczeństwa globalnego i regionalnego.

Diorditsa (2016, s. 39) wskazuje, że system bezpieczeństwa cybernetycznego to „zestaw uzgodnionych pod względem zadań elementów bezpieczeństwa cybernetycznego, które są kompletowane i wdrażane zgodnie z jednolitym planem w przestrzeni cybernetycznej w celu zapewnienia bezpieczeństwa cybernetycznego systemów informacyjnych, telekomunikacyjnych oraz informacyjno-telekomunikacyjnych".

Na środowisko cyberprzestrzeni z kolei składają się elementy społeczne, techniczne, telekomunikacyjne, informacyjne, komputerowo-sieciowe. Diorditsa (2016) proponuje postrzegać cyberprzestrzeń jako zestaw wzajemnie połączonych zasobów informacyjnych, oprogramowania, baz danych i banków danych przetwarzanych w sieciach komputerowych i związanej z nimi infrastrukturze, wraz z obiektami znajdującymi się pod ich kontrolą i zarządzaniem.

Cyberprzestrzeń stała się integralną częścią przestrzeni informacyjnej oraz jedną ze sfer walki zbrojnej (Diorditsa i Lipkan, 2017) i może służyć do dezaktywacji systemów komunikacyjnych (Sydorenko, 2018). Nowoczesne technologie pozwalają na wykorzystanie materiałów cyfrowych do tworzenia fałszywych lub niejednoznacznych treści, które mogą być wykorzystywane do oszukiwania i manipulacji (Sydorenko, 2018). Media społecznościowe umożliwiają podmiotom państwowym i niepaństwowym wykorzystywanie fałszywych profili w celu jak najszerszego rozpowszechniania fałszywych informacji. Jako potwierdzenie tego faktu można wymienić celowe wykorzystanie mediów społecznościowych w konfrontacji rosyjsko-ukraińskiej (Lange-Ionatamishvili i Svetoka, 2015).

Warto zwrócić uwagę na interpretację Baranova (2014), który twierdzi, że cyberbezpieczeństwo to taki stan ochrony żywotnych interesów poszczególnych jednostek społecznych, społeczeństwa i państwa w zakresie korzystania z systemów komputerowych i/lub sieci telekomunikacyjnych, przy którym minimalizowane są szkody wynikające z niekompletności, niedotrzymania terminu i nieprawdopodobności wykorzystywanych informacji, negatywny wpływ informacji, negatywne skutki działań technologii informacyjnych, a także nieuprawnione rozpowszechnianie, wykorzystywanie oraz naruszanie integralności, poufności i dostępności informacji.

Podsumowując, należy stwierdzić, że głównym zagrożeniem informacyjnym dla bezpieczeństwa narodowego jest wpływ strony przeciwnej na infrastrukturę informacyjną danego kraju, zasoby informacyjne, społeczeństwo, świadomość i podświadomość poszczególnych osób. Zadaniem bezpieczeństwa informacyjnego jest zatem stworzenie systemu przeciwdziałania zagrożeniom informacyjnym oraz ochrona własnej przestrzeni informacyjnej, infrastruktury informacyjnej i zasobów informacyjnych państwa (Bondarenko i Litvinenko, 1999).

3. Założenia koncepcyjne NCPI

Badanie, którego wyniki będą przedstawione, bazuje na narodowym indeksie potęgi cybernetycznej – *National Cyber Power Index* (NCPI). Indeks ten opracowany jest przez Centrum Nauki i Spraw Międzynarodowych Belfer (Cassidy i in., 2020).

NCPI to podejście do konceptualizacji i pomiaru potęgi cybernetycznej na poziomie krajowym. Indeks jest wielowymiarową i zdezagregowaną miarą. Belfer National Cyber Power Index mierzy zdolności cybernetyczne 30 krajów w kontekście 7 celów narodowych, wykorzystując 32 wskaźniki określające zamiary (*Intent*

indicators) i 27 wskaźników określających zdolności (*Capability indicators*) w zakresie cyberbezpieczeństwa wraz z dowodami zebranymi z publicznie dostępnych danych (Cassidy i in., 2020). Według Cassidy i in. (2020), twórców NCPI, wśród dotychczas istniejących indeksów związanych z cyberprzestrzenią nie istnieje jedna wspólna miara określająca poziom potęgi cybernetycznej. NCPI składa się z wielu komponentów i powinien być rozpatrywany w kontekście celów narodowych danego kraju. W ramach NCPI mierzone są strategie rządowe, zdolności w zakresie działań obronnych i ofensywnych, sposób alokacji zasobów, sektor prywatny, siła robocza oraz innowacje. Ocena NCPI jest pomiarem zarówno sprawdzonej potęgi cybernetycznej, jak i potencjału w zakresie cyberbezpieczeństwa, przy czym ostateczny wynik zakłada, że rząd danego kraju jest w stanie skutecznie dysponować tymi zdolnościami (Cassidy i in., 2020).

Jak już wspomniano wyżej, NCPI identyfikuje 7 podstawowych celów narodowych w zakresie cyberbezpieczeństwa, do których państwa dążą za pomocą środków cybernetycznych (Cassidy i in., 2020). Są to:

1) **inwigilacja i monitorowanie grup krajowych** (S*urveilling and monitoring domestic groups*);

2) **wzmocnienie i usprawnienie krajowej obrony cybernetycznej** (*strengthening and enhancing national cyber defenses*);

3) **kontrolowanie i manipulowanie środowiskiem informacyjnym** (*controlling and manipulating the information environment*);

4) **zbieranie i gromadzenie informacji wywiadowczych w innych krajach na rzecz bezpieczeństwa narodowego** (*intelligence gathering and collection in other countries for national security*);

5) **rozwijanie krajowych kompetencji w dziedzinie cyberbezpieczeństwa i technologii** (*growing national cyber and technology competence*);

6) **niszczenie lub blokowanie infrastruktury i zdolności przeciwnika** (*destroying or disabling an adversary's infrastructure and capabilities*);

7) **zdefiniowanie międzynarodowych norm cybernetycznych i standardów technicznych** (*defining international cyber norms and technical standards*).

Ogólna ocena NCPI mierzy kompleksowość danego kraju jako podmiotu działającego w sferze cyberbezpieczeństwa. Kompleksowość, w kontekście NCPI, odnosi się do wykorzystywania przez dany kraj środków cybernetycznych do osiągania różnorodnych celów. Najbardziej kompleksowo rozwinięte ze względu na potęgę cybernetyczną jest państwo, które dąży do osiągnięcia wielu celów narodowych za pomocą środków cybernetycznych oraz dysponuje odpowiednimi zdolnościami do realizacji tych celów. Dlatego w NCPI dane państwo uzyskuje wysokie wyniki pod względem określonego celu tylko wtedy, gdy ma zarówno sprecyzowane w ramach danego celu zamiary, jak i zdolności niezbędne do jego osiągnięcia. Należy zwrócić uwagę na to, że oszacowanie samych zdolności lub tylko samych zamiarów w ramach konkretnego celu cybernetycznego nie jest wystarczające. NCPI jest połączeniem wskaźników CII (wskaźnik określający zamiary w zakresie cyberbezpieczeń-

stwa) oraz CCI (wskaźnik określający zdolności w zakresie cyberbezpieczeństwa). Przedstawia się on następująco (Cassidy i in., 2020):

$$National\,Cyber\,Power\,Index\left(NCPI\right)=\frac{1}{7}\sum_{x=1}^{7}Capability_{x}\bullet Intent_{x}\ , \tag{1}$$

gdzie: *Capability* – wskaźnik określający zdolności w zakresie cyberbezpieczeństwa (CCI); *Intent* – wskaźnik określający zamiary w zakresie cyberbezpieczeństwa (CII).

Wskaźnik zamiarów (*Intent*) to pomiar jakości i liczby rządowych inicjatyw planistycznych (tj. narodowych strategii bezpieczeństwa cybernetycznego, planów reagowania kryzysowego i innych dokumentów planistycznych o charakterze rządowym). Jest to subiektywna ocena obserwowanego zachowania rządu w kwestiach związanych z cyberbezpieczeństwem. Wskaźnik zdolności (*Capability*) to pomiar jakości i liczby wyników kraju związanych z jednym lub kilkoma celami w zakresie cyberbezpieczeństwa (np. liczba patentów zgłaszanych rocznie, liczba najlepszych globalnych firm zajmujących się bezpieczeństwem, liczba wykwalifikowanych pracowników) (Cassidy i in., 2020).

4. Opis danych i metody badawczej

W badaniu wykorzystano analizę kanoniczną. Celem analizy kanonicznej jest określenie liniowej zależności między grupami zmiennych, co pozwala na dokonanie oceny wpływu jednej grupy czynników na drugą i *vice versa* (Yarovenko, 2020). Innymi słowy, zgodnie z tym, co podaje Halafyan (2007), analiza kanoniczna jest narzędziem umożliwiającym zbadanie zależności pomiędzy dwoma zestawami zmiennych w celu określenia relacji między nimi, co pozwala na dokonanie oceny stopnia wpływu jednego zestawu zmiennych na drugi oraz uzasadnienie jego istotności statystycznej.

W danym przypadku analiza kanoniczna umożliwia zbadanie zależności między zbiorem zmiennych reprezentujących poszczególne elementy składowe narodowego indeksu potęgi cybernetycznej a zbiorem zmiennych reprezentujących wskaźniki odzwierciedlające rozwój gospodarczy, społeczny oraz polityczny 28 państw wybranych do analizy. Celem badania jest udowodnienie lub odrzucenie, za pomocą analizy kanonicznej, hipotezy o obustronnym uwarunkowaniu skuteczności systemu bezpieczeństwa informacyjnego i czynników sprzyjających rozwojowi społeczno-gospodarczo-politycznemu państwa.

Wykorzystano następujące wskaźniki służące do oceny potęgi cybernetycznej:

1) inwigilacji (*surveillance cyber power score*);
2) obrony (*defense cyber power score*);
3) kontroli informacji (*information control cyber power score*);
4) wywiadu (*intelligence cyber power score*);
5) handlu lub wymiany handlowej (*commerce cyber power score*);

6) działań ofensywnych (*offense cyber power score*);
7) ustalonych norm (*norms cyber power score*).

Dane dla powyższych wskaźników pochodzą z 2020 roku (Harvard Dataverse, 2021). Wyniki w powyższych obszarach mierzono na skali przedziałowej od 0 do 100, gdzie 0 oznacza bardzo niski poziom potęgi cybernetycznej, a 100 bardzo wysoki poziom potęgi cybernetycznej.

Badanie przeprowadzono dla państw Sojuszu Północnoatlantyckiego (NATO), państw z regionu Azji i Pacyfiku, Azji Południowej, Bliskiego Wschodu, Afryki Północnej, Ameryki Łacińskiej, Europy Północnej, Europy Wschodniej oraz Europy Centralnej. Do grupy tych państw należą: Australia, Brazylia, Kanada, Chiny, Egipt, Estonia, Francja, Niemcy, Indie, Izrael, Włochy, Japonia, Litwa, Malezja, Holandia, Nowa Zelandia, Korea Południowa, Rosja, Arabia Saudyjska, Singapur, Hiszpania, Szwecja, Szwajcaria, Turcja, Ukraina, Wielka Brytania, USA i Wietnam.

Do analizy wybrano szereg wskaźników odzwierciedlających rozwój gospodarczy, społeczny oraz polityczny w powyższych 28 krajach w latach 2019-2020. Warto zaznaczyć, że w sytuacji, gdy dla poszczególnych zmiennych nie było danych z analizowanego okresu, dane były przyjmowane z najbardziej zbliżonego okresu, ale nie później niż z 2017 roku.

Bazę danych utworzyły następujące wskaźniki odzwierciedlające rozwój gospodarczy (CEIC, 2022; The World Bank, 2022a): eksport towarów i usług (% PKB); bezpośrednie inwestycje zagraniczne, wpływy netto (% PKB); PKB (wartości bieżące w USD); PKB *per capita* (wartości bieżące w USD); wydatki na spożycie finalne sektora instytucji rządowych i samorządowych (% PKB); DNB (dochód narodowy brutto) *per capita*, PPP (wartości bieżące w USD); eksport zaawansowanych technologii (% produkowanego eksportu); przemysł (w tym budownictwo), wartość dodana (% PKB); inflacja, deflator PKB (% rocznie); inwestycje portfelowe netto (bilans obrotów bieżących (BoP), wartości bieżące w USD); dochody podatkowe (% PKB); rezerwy ogółem (w tym złoto, wartości bieżące w USD); bezrobocie ogółem (% całkowitej siły roboczej) (szacunek krajowy).

Wybrano również wskaźniki opisujące poziom rozwoju społeczno-politycznego kraju, takie jak (The World Bank, 2022b): ocena kontroli korupcji; ocena skuteczności rządu; ocena stabilności politycznej i braku przemocy/terroryzmu; ocena jakości organów regulacyjnych; ocena praworządności; ocena sprawności systemu statystycznego danego kraju.

Warto nadmienić, że badania w tym kierunku już wcześniej prowadziła Yarovenko (2020). Według tej autorki o istotności oraz aktualności tego typu analizy może świadczyć fakt, że we współczesnym świecie większość procesów przenosi się do świata cyfrowego lub wirtualnego. Jest to spowodowane między innymi tym, że w różnych obszarach rozwoju społecznego, gospodarczego i politycznego kraju coraz więcej korzyści wynika z posługiwania się technologiami komputerowymi, intelektualnymi oraz cyberfizycznymi do rozwiązywania najistotniejszych problemów społeczeństwa.

Należy zatem sformułować hipotezę, że skuteczność systemu bezpieczeństwa informacyjnego na poziomie państwowym jest uwarunkowana czynnikami rozwoju społeczno-gospodarczo-politycznego kraju, tzn. kraje rozwinięte, o dużym potencjale społeczno-gospodarczym i stabilnej sytuacji politycznej mają podwyższony poziom bezpieczeństwa informacyjnego i odwrotnie, a wzrost poziomu bezpieczeństwa informacyjnego wpływa na rozwój kraju.

5. Wyniki uzyskane w rezultacie przeprowadzonej analizy kanonicznej

Zgodnie z tym, co podaje Yarovenko (2020), ogólną ideę analizy kanonicznej w kontekście danego badania można przedstawić w postaci następującego układu równań:

$$Y = a_1 y_1 + a_2 y_2 + ... + a_n y_n; X = b_1 x_1 + b_2 x_2 + ... + b_n x_n, \quad (2)$$

gdzie: $y_1, y_2 \ldots y_n$ – zbiór zmiennych reprezentujących poszczególne elementy składowe narodowego indeksu potęgi cybernetycznej; $x_1, x_2 \ldots x_n$ – zbiór zmiennych reprezentujących wybrane wskaźniki odzwierciedlające rozwój gospodarczy, społeczny oraz polityczny; Y i X – sumy ważone zmiennych każdego zbioru, które są zmiennymi kanonicznymi i determinują pierwiastek kanoniczny; $a_1, a_2 \ldots a_n$ i $b_1, b_2 \ldots b_n$ – wagi, które są obliczane przy uwzględnieniu maksymalnego skorelowania między dwoma zbiorami zmiennych.

Dzięki zastosowaniu modułu analizy kanonicznej w pakiecie STATISTICA 13.0 otrzymano wyniki przedstawione w tab. 1.

Z tabeli 1 wynika, że wartość współczynnika korelacji kanonicznej R jest równa 0,99955. Wskazuje to na istnienie bardzo silnej korelacji pomiędzy zbiorem zmiennych reprezentujących wybrane wskaźniki odzwierciedlające rozwój społeczno-gospodarczo-polityczny poszczególnych państw a zbiorem zmiennych reprezentujących poszczególne elementy składowe narodowego indeksu potęgi cybernetycznej NCPI. W związku z tym można uznać, że wzrost wpływu czynników opisujących rozwój społeczno-gospodarczo-polityczny powoduje wzrost poziomu cyberbezpieczeństwa kraju, a wzrost poziomu cyberbezpieczeństwa pozytywnie wpływa na rozwój społeczno-gospodarczo-polityczny kraju.

Istotność współczynnika korelacji potwierdza wysoka wartość kryterium Pearsona ($\chi^2 = 225$), którego poziom istotności nie przekracza 0,05. Z tabeli 1 wynika również, że wartość całkowitej redundancji dla zbioru po lewej stronie, który odpowiada zbiorowi zmiennych reprezentujących poszczególne elementy składowe narodowego indeksu potęgi cybernetycznej, wynosi 85,6%, zatem zmienne, które odpowiadają wybranym wskaźnikom odzwierciedlającym rozwój społeczno-gospodarczo-polityczny krajów, w 85,56% wyjaśniają zmienność wskaźników bezpieczeństwa cybernetycznego, co jest dość wysokim rezultatem. Czynniki kształtujące

Tabela 1. Wyniki analizy kanonicznej

N=28		Podsumow. analizy kanon. (NCPI_dataset_2020_canonical_analysis) Kanoniczne R: ,99955 Chi2(133)=225,17 p=,00000 **Lewy zb.**	Prawy zb.
Liczba zmiennych		7	19
Wariancja wyodręb.		100,000%	51,7750%
Całkowita redund		85,5513%	43,6211%
Zmienne:	1	Surveillance Cyber Power	Exports of goods and services (% of GDP)
	2	Defense Cyber Power	Foreign direct investment, net inflows (% of GDP)
	3	Information Control Cyber Power	GDP (current US$)
	4	Intelligence Cyber Power	GDP per capita (current US$)
	5	Commerce Cyber Power	General government final consumption expenditure (% of GDP)
	6	Offense Cyber Power	GNI per capita, PPP (current international $)
	7	Norms Cyber Power	High-technology exports (% of manufactured exports)
	8		Industry (including construction), value added(% of GDP)
	9		Inflation, GDP deflator (annual %)
	10		Portfolio investment, net (BoP, current US$)
	11		Tax revenue (% of GDP)
	12		Total reserves (includes gold, current US$)
	13		Unemployment, total (%of total labor force) (national estimate)
	14		Control of Corruption: Estimate
	15		Government Effectiveness:Estimate
	16		Political Stability and Absence of Violence/Terrorism:Estimate
	17		Regulatory Quality:Estimate
	18		Rule of Law:Estimate
	19		Voice and Accountability:Estimate

Źródło: opracowanie własne z wykorzystaniem pakietu STATISTICA na podstawie badania Yarovenko (2020), a także danych z CEIC i Banku Światowego (CEIC, 2022; The World Bank, 2022a, 2022b).

cyberbezpieczeństwo w 43,6% wyjaśniają zmienność czynników rozwoju społeczno-gospodarczo-politycznego, czyli około 44% rozwoju kraju zależy również od poziomu bezpieczeństwa przestrzeni informacyjnej i cybernetycznej państwa, co jest dość wysokim wynikiem dla tak specyficznej dziedziny, jaką jest bezpieczeństwo informacyjne. Otrzymane rezultaty dają podstawy, by uważać, że uzyskany model kanoniczny jest wystarczająco precyzyjny, ponieważ jedynie 14,45% (100% − 85,5%) wariancji zmiennych reprezentujących poszczególne elementy składowe narodowego indeksu potęgi cybernetycznej NCPI zależy od innych czynników, których nie uwzględniono w analizie.

W dalszej części analizy dokonano wyboru statystycznie istotnych pierwiastków kanonicznych. Na podstawie wartości testu chi-kwadrat ustalono, że w rozważanym przypadku jest tylko jeden statystycznie istotny pierwiastek kanoniczny, co oznacza, że uzasadnione jest rozważenie jednej pary zmiennych kanonicznych.

Po wyznaczeniu wag kanonicznych stwierdzono, że największy wkład w narodowe bezpieczeństwo cybernetyczne wnoszą następujące zmienne: ocena potęgi cybernetycznej w zakresie kontroli informacji, ocena potęgi cybernetycznej inwigilacji oraz ocena potęgi cybernetycznej wywiadu. Najmniejszy wkład natomiast mają: ocena komercyjnej potęgi cybernetycznej, ocena potęgi cybernetycznej w obronie, ocena potęgi norm cybernetycznych oraz ocena potęgi cybernetycznej w działaniach ofensywnych. Wyniki te zaprezentowano w tab. 2.

Tabela 2. Wagi kanoniczne dla zmiennych reprezentujących poszczególne elementy składowe cyberbezpieczeństwa narodowego

Zmienna	Pierw 1
Surveillance Cyber Power	-0,416555
Defense Cyber Power	0,242127
Information Control Cyber Power	0,579710
Intelligence Cyber Power	0,351575
Commerce Cyber Power	0,255081
Offense Cyber Power	-0,190729
Norms Cyber Power	0,221170

Źródło: opracowanie własne z wykorzystaniem pakietu STATISTICA na podstawie badania Yarovenko (2020).

W przypadku czynników rozwoju społeczno-gospodarczo-politycznego największy wkład wnoszą takie zmienne, jak: ocena kontroli korupcji, PKB (bieżące USD), ocena stabilności politycznej i braku przemocy/terroryzmu, ocena skuteczności rządu, ocena sprawności systemu statystycznego danego kraju, PKB *per capita* (bieżące USD). Najmniejszy wkład natomiast mają następujące zmienne: bezpośrednie inwestycje zagraniczne, wpływy netto (% PKB); inwestycje portfelowe netto (bilans obrotów bieżących (BoP), bieżące USD); dochody podatkowe (% PKB); rezerwy ogółem (w tym złoto, bieżące USD). Wyniki zamieszczono w tab. 3.

Tabela 3. Wagi kanoniczne dla zmiennych reprezentujących wybrane wskaźniki rozwoju społeczno-gospodarczo-politycznego

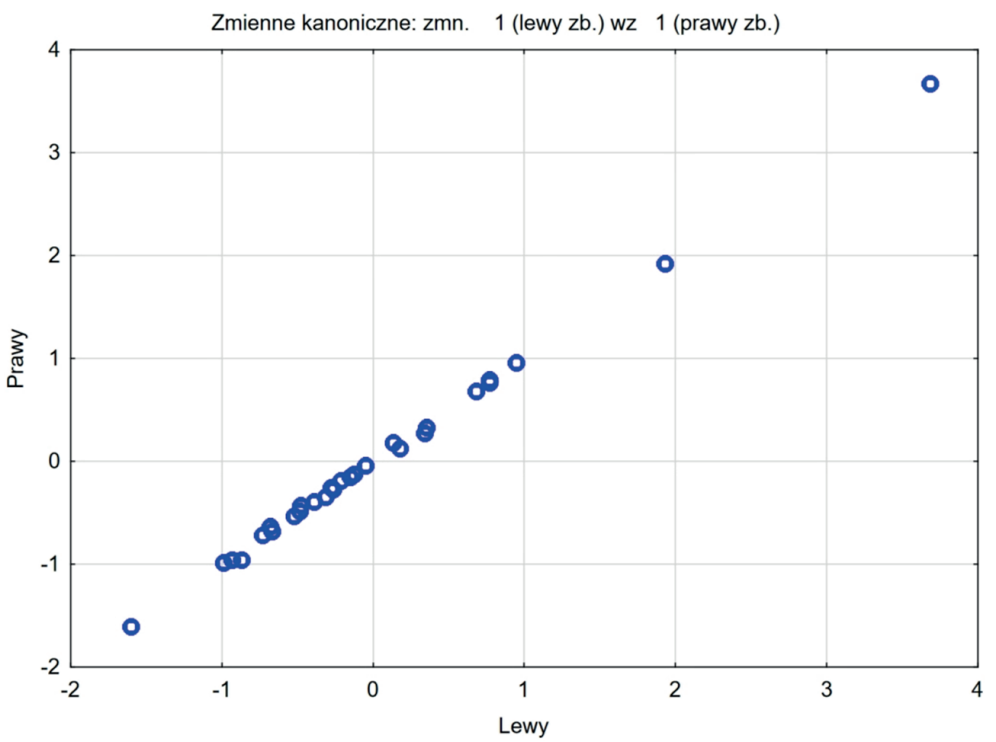
Zmienna	Wagi kanoniczne, prawy zbiór (NCPI_dataset_2020_canonical_analysis)						
	Pierw 1	Pierw 2	Pierw 3	Pierw 4	Pierw 5	Pierw 6	Pierw 7
Exports of goods and services (% of GDP)	-0,25345	-0,16039	-0,12426	-0,84295	0,06694	-0,14267	0,16752
Foreign direct investment, net inflows (% of GDP)	-0,01565	-0,02816	0,49927	0,36202	0,25542	-0,14929	-0,02027
GDP (current US$)	0,69368	-0,18885	0,63348	-0,00705	-0,16285	-0,18001	-0,68329
GDP per capita (current US$)	0,44905	0,57307	0,89951	-1,38008	0,33884	0,19942	-1,70287
General government final consumption expenditure (% of GDP)	0,26606	0,34972	-0,91404	-0,63849	-0,09104	-0,64752	0,60148
GNI per capita, PPP (current international $)	-0,23564	-0,40275	0,06268	1,68405	0,81025	-0,12305	1,70445
High-technology exports (% of manufactured exports)	0,17919	-0,34064	-0,21229	0,91871	0,07433	0,11242	-0,45613
Industry (including construction), value added(% of GDP)	-0,41681	-1,02083	0,57404	-0,10274	0,10706	0,37007	-0,06373
Inflation, GDP deflator (annual %)	0,21381	0,18534	-0,55715	0,04682	0,20797	0,37719	0,47660
Portfolio investment, net (BoP, current US$)	-0,05859	-0,19984	0,54434	0,30046	-0,08122	-0,44386	-1,18853
Tax revenue (% of GDP)	-0,05903	-0,25081	0,57282	-0,60273	0,09896	0,50081	-0,66719
Total reserves (includes gold, current US$)	-0,02220	-0,36849	-0,05615	-0,32125	0,75963	0,32167	0,36284
Unemployment, total (%of total labor force) (national estimate)	-0,22582	-0,29278	-0,15683	-0,32333	0,36943	-0,16321	-0,73223
Control of Corruption: Estimate	-1,13813	-2,82803	-1,15130	2,49187	-2,14048	-0,53813	-0,59449
Government Effectiveness:Estimate	0,51654	1,04348	-0,48277	-1,42758	0,10197	0,35424	1,01019
Political Stability and Absence of Violence/Terrorism:Estimate	0,52060	1,10164	-0,29601	-0,80501	1,73074	1,84874	1,48592
Regulatory Quality:Estimate	0,20215	-0,53798	-0,87754	-0,09665	-0,15654	-2,68485	-1,07447
Rule of Law:Estimate	0,24586	1,35050	0,89607	-1,40877	-1,10092	1,62592	-0,73247
Voice and Accountability:Estimate	-0,48017	-0,91239	0,60511	1,59478	1,07719	0,02661	0,30603

Źródło: opracowanie własne z wykorzystaniem pakietu STATISTICA na podstawie badania Yarovenko (2020).

Wartości wag kanonicznych umożliwiły skonstruowanie równań regresyjnych dla zmiennych kanonicznych dla pierwszego pierwiastka kanonicznego:

$$
\begin{aligned}
Y &= -0,42y_1 + 0,24y_2 + 0,58y_3 + 0,35y_4 + 0,26y_5 + (-0,19y_6) + 0,22y_7; \\
X &= -0,25x_1 + (-0,02x_2) + 0,69x_3 + 0,45x_4 + 0,27x_5 + (-0,24x_6) + \\
&0,18x_7 + (-0,42x_8) + 0,21x_9 + (-0,06x_{10}) + (-0,06x_{11}) + (-0,02x_{12}) + \\
&(-0,23x_{13}) + (-1,14x_{14}) + 0,52x_{15} + 0,52x_{16} + 0,20x_{17} + 0,25x_{18} + (-0,48x_{19}).
\end{aligned} \tag{3}
$$

W ostatnim etapie skonstruowano wykres rozrzutu wartości kanonicznych dla pierwszej pary pierwiastków kanonicznych, co zwizualizowano na rys. 1. Na wykresie oś pozioma to elementy składowe narodowego indeksu potęgi cybernetycznej, a oś pionowa to wskaźniki rozwoju społeczno-gospodarczo-politycznego.



Rys. 1. Wykres rozrzutu wartości kanonicznych

Źródło: opracowanie własne z wykorzystaniem pakietu STATISTICA na podstawie badania Yarovenko (2020).

Ułożenie na wykresie (rys. 1) obserwacji w sposób liniowy wskazuje na istnienie dość ścisłej zależności pomiędzy zmiennymi reprezentującymi poszczególne elementy cyberbezpieczeństwa narodowego a czynnikami rozwoju społeczno-gospodarczo-politycznego. Poziom cyberbezpieczeństwa narodowego, a co za tym idzie – bezpieczeństwa informacyjnego, zależy od poziomu rozwoju danego pań-

stwa. Ponadto poziom bezpieczeństwa może również wpływać na stopień rozwoju danego kraju.

Uzyskane w trakcie prowadzenia analizy kanonicznej wyniki potwierdzają słuszność hipotezy mówiącej o tym, że czynniki rozwoju społeczno-gospodarczo-politycznego państwa determinują poziom jego bezpieczeństwa informacyjnego i odwrotnie, poziom bezpieczeństwa informacyjnego ma decydujący wpływ na rozwój kraju. Innymi słowy, sprawnie funkcjonujący system zapewnienia bezpieczeństwa informacyjnego państwa jest jednym z czynników stymulujących rozwój nowoczesnego państwa.

6. Podsumowanie oraz kierunek dalszych badań

Rezultat analizy kanonicznej wskazał na istnienie bardzo silnej zależności pomiędzy zbiorem zmiennych reprezentujących wybrane wskaźniki odzwierciedlające rozwój społeczno-gospodarczo-polityczny poszczególnych państw a zbiorem zmiennych reprezentujących poszczególne elementy składowe narodowego indeksu potęgi cybernetycznej NCPI.

Ze względu na to, że czynniki z zakresu cyberbezpieczeństwa oceniają zdolność danego kraju do przeciwdziałania różnym zagrożeniom cybernetycznym, kraje o wysokim potencjale gospodarczym mają większe możliwości przeciwdziałania takim zagrożeniom. Poza tym państwa takie mają większe możliwości finansowe w zakresie organizowania dodatkowych przedsięwzięć, wykorzystywania nowoczesnych technologii i wykwalifikowanych specjalistów w dziedzinie cyberbezpieczeństwa.

Ustalono również, że jeśli rozwój kraju powiązany z elementami składowymi cyberbezpieczeństwa narodowego, tzn. wzrostem poziomu bezpieczeństwa informacyjnego, a w szczególności cyberbezpieczeństwa, to przyczynia się do rozwoju kraju na płaszczyźnie społecznej, gospodarczej oraz politycznej. Na przykład im wyższy poziom ochrony danych osobowych, tym większe zaufanie społeczeństwa do państwa i różnych instytucji. Im bardziej chronione są dane finansowe obywateli, tym większa jest niezawodność systemu bankowego i tym mniejsze są straty spowodowane działalnością cyberprzestępców.

O ważności badania świadczy fakt, że uzyskane w ramach przedstawionej analizy wyniki mogą przyczynić się do opracowywania szeregu działań o charakterze strategicznym między tymi obszarami bezpieczeństwa cybernetycznego i do rozwoju społeczno-gospodarczo-politycznego państwa. W konsekwencji może to doprowadzić do wzmocnienia państwowych instytucji bezpieczeństwa, wdrożenia nowych metod i podjęcia odpowiednich środków w zakresie zapewnienia bezpieczeństwa, w szczególności w zakresie bezpieczeństwa informacyjnego. To z kolei może pozytywnie wpłynąć na stabilność polityczną w kraju, ochronę socjalną ludności przed cyberprzestępczością, zmniejszenie liczby szkód dla gospodarki pań-

stwowej i podmiotów gospodarczych wynikających z nielegalnego wykorzystania posiadanych zasobów.

Na podstawie przeprowadzonych studiów literaturowych i wyników badania można stwierdzić, że stałe i systematyczne wzmacnianie i rozwój bezpieczeństwa informacyjnego powinny być jednymi z najbardziej priorytetowych kierunków polityki państwa.

W trakcie dalszych analiz poruszonej tematyki należałoby skupić się na konstrukcji modelu ekonometrycznego w celu zbadaniu zbadania związku narodowego indeksu potęgi cybernetycznej (NCPI) ze zmiennymi objaśniającymi, które charakteryzują 7 podstawowych celów w zakresie cyberbezpieczeństwa.

Literatura

Baranov, O. (2014). Pro tlumachennia ta vyznachennia poniattia «kiberbezpeka». *Pravova Informatyka*, (2), 54–62.

Bogdanovich, V. Y., Marko, E. I. i Vorovich, B. A. (2018). *Informatsiina bezpeka yak osnova voiennoi bezpeky derzhavy ta suspilstva* [Information security as a basis for military security of the company]. Kyiv: Central Research Institute of the Armed Forces of Ukraine, Center for Military and Strategic Studies of the National Defence University of Ukraine named after Ivan Cherniakhovskyi.

Bondarenko, V. i Litvinenko, O. (1999). Information security of the modern state: conceptual reflections. *Stratehichna Panorama*, (1-2), 127–133.

Cassidy, D., DeSombre, W., Hemani, I., Jones, S, Schwarzenbach, A. i Voo, J. (2020). *National Power Index 2020. methodology and analytical considerations.* Pobrane 3 listopada 2021 z https://www.belfercenter.org/sites/default/files/2020-09/NCPI_2020.pdf

CEIC. (2022). *Indicators*. Pobrane 20 maja 2022 z https://www.ceicdata.com/en/indicators

Diorditsa, I. (2016). Poniattia ta zmist natsionalnoi systemy kiberbezpeky. *Jurnalul Juridic Naţional: Teorie Şi Practică,* (6), 37–42. Pobrane z http://www.jurnaluljuridic.in.ua/archive/2016/6/part_1/9.pdf

Diorditsa, I. i Lipkan, V. (2017). Natsionalna systema kiberbezpeky yak skladova chastyna systemy zabezpechennia natsionalnoi bezpeky Ukrainy [National cyber security system as an integral part of the system of ensuring national security]. *Pidpryiemnytstvo, Hospodarstvo i Prawo,* 5, 174–180.

Halafyan, A. (2007). *STATISTICA 6. Statisticheskiy analiz dannyih* [STATISTICA 6. Statistical data analysis]. Moscow: LLC "Binom-Press".

Harvard Dataverse. (2021). *Harvard belfer national Cyber Power Index 2020.* Pobrane 6 listopada 2021 z https://dataverse.harvard.edu/dataset.xhtml?persistentId=doi:10.7910/DVN/LT55JY

Havryltsiv, M. (2020). State information safety in the system national security of Ukraine. *Juridical Scientific and Electronic Journal*, (2), 200–203. doi: https://doi.org/10.32782/2524-0374/2020-2/52

Khudarkovskyi, K. I., Pievtsov, H. V., Sidchenko, S. O. i Zalkin, S. V. (2020). *Informatsiino-psykholo-hichni operatsii: planuvannia, protydiia, tekhnolohii: monohrafiia.* Kharkiv: Ivan Kozhedub National Air Force University.

Lange-Ionatamishvili, E. i Svetoka, S. (2015). Strategic communications and social media in the Russia Ukraine conflict. *NATO Strategic Communications Centre of Excellence.* doi: 10.3233/978-1-61499-699-6-86

Sydorenko, I. (2018). Strategic communications of Ukraine. *European Political and Law Discourse*, *5*(2), 273–279.

The World Bank. (2022a). *World development indicators*. Pobrane 20 maja 2022 z https://databank.worldbank.org/source/world-development-indicators#

The World Bank. (2022b). *Worldwide Governance Indicators*. Pobrane 20 maja 2022 z https://databank.worldbank.org/source/worldwide-governance-indicators/preview/on

Yarovenko, H. (2020). Canonical analysis of relationship between information security and socio-economic-political development of the country. *International Economic Relations and World Economy*, (31), 165–172. doi: https://doi.org/10.32782/2413-9971/2020-31-26

Zadiraka, V. (2014). Suchasni metody rozviazannia zadach informatsiinoi bezpeky. *Visnyk Natsionalnoyi Akademiyi Nauk Ukrainy*, (5), 65–69.

Analysis of the State of Information Security Based on the National Cyber Power Index

Abstract: This article undertakes the study on the problematic aspects of the functioning of the information security system as a foundation of national security of the state and society. It was analyzed whether the constant and systematic strengthening and development of information security system should be among the highest priorities of a state policy. The main purpose of the study is to determine whether the information security system assurance must hold one of the key places in the overall system of ensuring the military security of the state. A canonical analysis was used in the research. It was concluded that the development of the country is explained by the components of national cybersecurity, i.e. the increase in the level of information security, and cybersecurity in particular, contributes to the development of the country at the social, economic and political dimensions.

Keywords: cybersecurity, NCPI, canonical analysis.