Robert Siudak

CYBERBEZPIECZEŃSTWO W POLSCE

OD DYSKURSÓW DO POLITYK PUBLICZNYCH

CYBERBEZPIECZEŃSTWO W POLSCE. OD DYSKURSÓW DO POLITYK PUBLICZNYCH

Robert Siudak

Cyberbezpieczeństwo w Polsce. Od dyskursów do polityk publicznych

Kraków 2022

Robert Siudak
Uniwersytet Jagielloński
https://orcid.org/0000-0001-7902-6163
robert.siudak@uj.edu.pl

Recenzent
dr hab. Marek Górka

Opracowanie redakcyjne
Justyna Wójcik

Projekt okładki
Lesław Sławiński

ISBN (druk) 978-83-8138-709-5
ISBN (PDF) 978-83-8138-710-1
https://doi.org/10.12797/9788381387101

Na okładce wykorzystano grafikę z serwisu Pixabay

Publikacja została sfinansowana ze środków Narodowego Centrum Nauki przyznanych na podstawie Umowy nr UMO-2017/27/N/HS5/00871 do projektu badawczego nr 2017/27/N/HS5/00871 pt. „Dyskursy cyberbezpieczeństwa w świetle zagrożeń związanych z technologiami informacyjno-komunikacyjnymi w Polsce"

WYDAWNICTWO KSIĘGARNIA AKADEMICKA
ul. św. Anny 6, 31-008 Kraków
tel.: 12 421-13-87; 12 431-27-43
e-mail: publishing@akademicka.pl

Księgarnia internetowa: https://akademicka.com.pl

Spis treści

Wykaz skrótów

ABW	– Agencja Bezpieczeństwa Wewnętrznego
AI	– *artificial intelligence*
APT	– *advanced persistant threat*
ARPA	– Advanced Research Projects Agency
AS	– aktor sekurytyzujący
B+R	– badania i rozwój
BBN	– Biuro Bezpieczeństwa Narodowego
C.A.S.E	– Critical Approaches to Security in Europe
C2	– *command and control*
C3	– *command, control and communication*
C4I	– *command, control, communication, computing and intelligence*
CERT	– zespół reagowania na incydenty komputerowe
CIA	– Central Intelligence Agency
CII	– *critical information infrastructures*
CMM	– *cybersecurity capacity maturity model for nations*
CPU	– *central processing unit*
CRI	– Cyber Readiness Index
CRP	– Cyberprzestrzeń Rzeczypospolitej Polski
CSIRT	– Computer Security Incident Response Team
CSIRT GOV	– Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego
CSIRT MON	– Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej
CSIRT NASK	– Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy
CTF	– *capture the flag*
DARPA	– Defense Advanced Research Projects Agency
DDoS	– *distributed denial of service*
DHS	– Department of Homeland Security
DNC	– Democratic National Committee
DOD	– Department of Defense
DRAM	– *dynamic random-access memory*

DUC – dostawca usług cyfrowych
ECSO – European Cyber Security Organization
EDA – European Defence Agency
ENISA – Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji
EPBiO – Europejska Polityka Bezpieczeństwa i Obrony
EW – *electronic warfare*
FBI – Federal Bureau of Investigation
FININT – *financial intelligence*
FIRST – Forum of Incident Response and Security Teams
FSB – Federalna Służba Bezpieczeństwa Federacji Rosyjskiej
GCI – Global Cybersecurity Index
GCSC – Global Commission on the Stability of Cyberspace
GCSCC – Global Cyber Security Capacity Centre
GFCE – Global Forum on Cyber Expertise
GGE – Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security
GRU – Główny Zarząd Wywiadowczy Sztabu Generalnego Sił Zbrojnych Federacji Rosyjskiej
HDD – *hard disk drive*
HTTPS – Hypertext Transfer Protocol Secure
HUMINT – *human intelligence*
Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats
IA – *information assurance*
ICANN – Internet Corporation for Assigned Names and Numbers
IGF – Internet Governance Forum
IK – infrastruktura krytyczna
INCB – Israel National Cyber Bureau
IO – *information operations*
IoT – Internet of Things
IP – *Internet protocol*
IRA – Internet Research Agency
ISO – International Organization for Standardization
IT – *information technologies*
ITRs – International Telecommunication Regulations
ITU – International Telecommunication Union
ITU-T – International Telecommunication Union – Telecommunication Standardization Sector
IW – *information warfare*
IXP – punkt wymiany ruchu internetowego
JCPA – *Joint Comprehensive Plan of Action*
KNF – Komisja Nadzoru Finansowego
KNZ – Karta Narodów Zjednoczonych
KPRM – Kancelaria Prezesa Rady Ministrów
LAN – *local area network*
MAEA – Międzynarodowa Agencja Energii Atomowej

MAiC – Ministerstwo Administracji i Cyfryzacji
MC – Ministerstwo Cyfryzacji
MON – Ministerstwo Obrony Narodowej
MSWiA – Ministerstwo Spraw Wewnętrznych i Administracji
MŚP – małe i średnie przedsiębiorstwa
NASK – Naukowa i Akademicka Sieć Komputerowa
NATO – North Atlantic Treaty Organisation
NATO CCDCOE – NATO Cooperative Cyber Defence Centre of Excellence
NATO StratCom COE – NATO Strategic Communications Centre of Excellence
NCBC – Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni
NCIRC – NATO Computer Incident Response Capability
NCK – Narodowe Centrum Kryptologii
NIK – Najwyższa Izba Kontroli
NIST – National Institute of Standards and Technology
NSA – National Security Agency
NSD – National Security Directive
NSDD – National Security Decision Directive
NSPD – National Security Presidential Directive
OBWE – Organizacja Bezpieczeństwa i Współpracy w Europie
OEWG – Open-Ended Working Group
OSI – Open Systems Interconnection
OSINT – *open-source intelligence*
OUK – operator usług kluczowych
OWASP – Open Web Application Security
P2P – *peer-to-peer*
PCCIP – President's Commission on Critical Infrastructure Protection
PESCO – Permanent Structured Cooperation
PLC – *programmable logic controllers*
PSYOPS – *psychological operations*
RAM – *random-access memory*
RB ONZ – Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych
RCB – Rządowe Centrum Bezpieczeństwa
RFN – Republika Federalna Niemiec
RMA – *revolution in military affairs*
ROM – *read-only memory*
SBN – Strategia bezpieczeństwa narodowego
SCADA – *supervisory control and data acquisition*
SDGs – Sustainable Development Goals
SEO – *search engine optimization*
SG ONZ – Sekretarz Generalny Organizacji Narodów Zjednoczonych
SHAPE – Supreme Headquarters Allied Powers Europe
SOW – Szanghajska Organizacja Współpracy
SQL – Structured Query Language
SSD – *solid-state drive*
TCP – *transmission control protocol*
TIK – technologie informacyjno-komunikacyjne

TLS – *transport layer security*
UE – Unia Europejska
UKE – Urząd Komunikacji Elektronicznej
UNIDIR – United Nations Institute for Disarmament Research
UNODC – United Nations Office on Drugs and Crime
UoKSC – Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa
USA – United States of America
VC – *venture capital*
WOC – Wojska Obrony Cyberprzestrzeni
WWW – World Wide Web
XSS – *cross-site-scripting*
ZO ONZ – Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych

Profesorowi Arturowi Gruszczakowi
za drogowskazy stawiane na szlaku badawczym

Wstęp

Co my mamy na myśli pod pojęciem cyberbezpieczeństwa? Bo też z rozmów z różnymi ludźmi mam wrażenie, że często mówimy o czymś innym. To znaczy, że to pojęcie jest też na tyle nowe i na tyle szerokie, że ono może dotyczyć i kwestii indywidualnych bardzo, ale też kwestii systemowych. (...) I też wydaje mi się, że to wpływa na debatę publiczną, że mówimy podobne rzeczy wszyscy, ale nie zawsze mam wrażenie, że o tym samym.

Krzysztof Izdebski,
dyrektor programowy Fundacji ePaństwo
Wywiad badawczy, 8.02.2019

W ciągu ostatnich dwóch dekad cyberbezpieczeństwo stało się jednym z kluczowych wyzwań w zakresie polityk publicznych[1]. Od dokumentów, przez strategie wojskowe i opracowania naukowe, aż po regulacyjne rynkowe komponent *cyber* jest prezentowany jako niezbędny element bezpieczeństwa indywidualnego, krajowego i międzynarodowego. Z czysto technicznego punktu widzenia daleko posunięta homogenizacja systemów komputerowych – zarówno na poziomie oprogramowania, jak i sprzętu – sprawia, że zestaw możliwych zagrożeń jest bardzo podobny, a wręcz uniwersalny na całym świecie. Niemniej, jak pokazują zróżnicowane odpowiedzi, model intersubiektywnego budowania bezpieczeństwa cyfrowego uwzględnia szereg innych czynników poza technicznymi, w tym społeczne, kulturowe, gospodarcze, a nawet

[1] Zob. R.A. Clarke, R. Knake, *Cyberwar: The Next Threat to National Security and What to Do about It*, Ecco, New York 2010; R.J. Deibert, R. Rohozinski, *Risking Security: Policies and Paradoxes of Cyberspace Security*, „International Political Sociology" 2010, Vol. 4, No. 1, s. 15-32; N. Shafqat, A. Masood, *Comparative Analysis of Various National Cyber Security Strategies*, „International Journal of Computer Science and Information Security" 2016, Vol. 14, No. 1, s. 129-136.

ideologiczne[2]. Postrzeganie bezpieczeństwa technologii informacyjno-komunikacyjnych (TIK), a także rola cyberprzestrzeni w szerszej dziedzinie bezpieczeństwa nie tylko ewoluują w czasie[3], ale są też stale kształtowane przez trwające spory pomiędzy różnymi dyskursami. To właśnie proces społecznego kształtowania sposobów rozumienia problemów cyberbezpieczeństwa stanowi obiekt dociekań w niniejszej pracy.

Problematyka badań

Rozprawa podnosi zatem kwestię społecznej konstrukcji niebezpieczeństw wynikających ze wzrastającej zależności wszelkich sfer aktywności ludzkiej od sprawnego funkcjonowania TIK. Problem jednoznacznego określenia zakresu przedmiotowego oraz funkcjonalnego pojęcia cyberbezpieczeństwa stanowi punkt wyjścia do dociekań na temat odmiennych dyskursów o cyberbezpieczeństwie obecnych w polskiej debacie publicznej. Prześledzenie dynamiki negocjowania odmiennych znaczeń określonych problemów bezpieczeństwa technologii informacyjno-komunikacyjnych w różnych dyskursach o cyberbezpieczeństwie stanowi jeden z kluczowych elementów rozprawy. Zastosowanie w pracy teorii rozwijanych w ramach krytycznych studiów nad bezpieczeństwem do analizy tematyki cyberbezpieczeństwa pozwoliło z kolei na poszerzenie badań poza tradycyjne wymiary: technologiczny oraz strategiczny. Problematyzacja społecznego wymiaru bezpieczeństwa TIK uzupełni badania dotyczące polskich polityk publicznych wobec wyzwań cyberbezpieczeństwa. Rzeczpospolita Polska wciąż tkwi w fazie określania swoich strategicznych oraz technologicznych wymagań odnośnie do krajowej cyberprzestrzeni oraz mechanizmów mających zabezpieczyć kluczowe interesy społeczne, polityczne i ekonomiczne kraju. Ewolucja podejścia do kwestii bezpieczeństwa TIK w polskich politykach publicznych także stanowi przedmiot badań niniejszej pracy.

---

[2] Zob. L.C. Lobato, K.M. Kenkel, *Discourses of Cyberspace Securitization in Brazil and in the United States*, „Revista Brasileira de Política Internacional" 2015, Vol. 58, s. 23-43; C. Haddad, C. Binder, *Governing through Cybersecurity: National Policy Strategies, Globalized (In-)Security and Sociotechnical Visions of the Digital Society*, „Österreichische Zeitschrift für Soziologie" 2019, Vol. 44, s. 115-134; S. Boeke, *National Cyber Crisis Management: Different European Approaches*, „Governance" 2018, Vol. 31, No. 3, s. 449-464.

[3] R. Kaiser, *The Birth of Cyberwar*, „Political Geography" 2015, Vol. 46, s. 11-20.

Celem ogólnym pracy jest zatem analiza społecznych procesów konstruowania problematyki cyberbezpieczeństwa w polskiej przestrzeni publicznej. Cele szczegółowe (pośrednie) to natomiast:

- Identyfikacja głównych dyskursów o cyberbezpieczeństwie w Polsce polegająca na określeniu ich liczby, charakterystyki, obecnych w nich ram, a także aktorów promujących je w przestrzeni publicznej.
- Zbadanie warunków wewnętrznych oraz zewnętrznych wpływających na dynamikę procesów sekurytyzacji, ryzyfikacji, polityzacji oraz prywatyzacji zagrożeń wynikających z technologii informacyjno-komunikacyjnych w Polsce.
- Analiza wpływu badanych dyskursów na rozwiązania legislacyjne, proceduralne oraz certyfikacyjno-technologiczne w dziedzinie cyberbezpieczeństwa.
- Badanie oraz systematyzacja szeregu różnic pojęciowych obecnych w polskiej debacie publicznej na temat cyberbezpieczeństwa. Analiza problemu odmiennego definiowania tożsamych terminów, takich jak między innymi „cyberbezpieczeństwo", „cyberprzestrzeń" czy „cyberobrona", przez różnych aktorów społecznych.
- Stworzenie ramy teoretycznej opartej na założeniach sekurytyzacji, ryzyfikacji, polityzacji oraz prywatyzacji uzupełnionych o teorię framingu, mogącej stanowić podstawę teoretyczną badań nad problematyką społecznego konstruowania różnorakich problemów bezpieczeństwa.

Główne pytania badawcze postawione w rozprawie brzmią: *Jakie dyskursy obecne są w polskiej debacie publicznej na temat cyberbezpieczeństwa? Jak wpłynęły one na proces tworzenia oraz implementacji polityk publicznych w Polsce w odniesieniu do cyberbezpieczeństwa?* Sformułowano także następujące pytania uzupełniające:

- Jakich głównych aktorów oraz obiekty bezpieczeństwa można wyróżnić w ramach omawianych procesów społecznych?
- Jakie uwarunkowania zewnętrzne oraz wewnętrzne miały kluczowy wpływ na dynamikę badanych procesów?
- Jakie zasoby społeczne oraz symboliczne wykorzystywane były przez aktorów?
- Które z dyskursów w największej mierze wpłynęły na kształt uregulowań prawnych, instytucjonalnych oraz certyfikacyjno-technicznych cyberbezpieczeństwa w Polsce?

Jako główną hipotezę przyjęto, iż polską debatę na temat cyberbezpieczeństwa kształtowało pięć dyskursów: technologiczny, bezpieczeństwa

narodowego, obywatelski, stosunków międzynarodowych oraz ekonomiczny. **Dyskurs technologiczny** koncentruje się na problemie nieodłącznego ryzyka związanego z wykorzystywaniem TIK. Odpowiedzią na nie jest analiza ryzyka oraz budowanie odporności (*resilience*) określonego urządzenia, sieci, organizacji czy systemu ekonomiczno-społecznego. **Dyskurs bezpieczeństwa narodowego** skupia się na działaniach realizowanych w cyberprzestrzeni lub za jej pośrednictwem, będących zagrożeniami egzystencjonalnymi dla wspólnoty narodowej lub jej poszczególnych instytucji. Zaciera on granice pomiędzy określonymi kategoriami zagrożeń w świecie cyfrowym – kryminalnymi, terrorystycznymi, militarnymi. **Dyskurs obywatelski** przyjmuje optykę bezpieczeństwa jednostki (*human security*), w tym ochrony jej praw i wolności. **Dyskurs stosunków międzynarodowych** analizuje cyberprzestrzeń jako nową domenę rywalizacji państw. **Dyskurs gospodarczy** koncentruje się na szansach rynkowych mogących wynikać z inteligentnej specjalizacji krajowej gospodarki w sektorze cyberbezpieczeństwa.

Założenia metodologiczne

Pole badawcze pracy determinuje zastosowanie podejścia interdyscyplinarnego. Projekt badawczy osadzony jest w obszarze oraz dziedzinie nauk społecznych, w dyscyplinie nauk o polityce i administracji, a częściowo także nauk o bezpieczeństwie. Bazuje na dorobku wypracowanym w badaniach nad stosunkami międzynarodowymi, a w szczególności koncepcji opisująco-wyjaśniających określanych mianem teorii bezpieczeństwa. Praca osadzona jest w paradygmacie konstruktywistycznym. Kluczową rolę w przyjętej ramie badawczej odgrywa teoria sekurytyzacji, uzupełniona przez propozycje teoretyczne zwracające uwagę na możliwość odmiennej dynamiki społecznego konstytuowania problemów cyberbezpieczeństwa – ryzyfikację, polityzację oraz prywatyzację. W ramach szerzej rozumianych nauk społecznych kluczowym elementem pozwalającym na uchwycenie badanych zjawisk pierwotnych i wtórnych (epifenomenów) jest teoria aktu mowy, uzupełniona przez koncepcję framingu. Szczegółowy opis założeń teoretycznych oraz konceptualizację formalną zawarto w rozdziale pierwszym rozprawy.

W głównej części badań wykorzystano metodę monograficzną, której celem była przekrojowa analiza procesów społecznych odpowiedzialnych za kształtowanie obecności zagrożeń wynikających z TIK w Polsce. Została ona uzupełniona metodą historyczną, która posłużyła

do prześledzenia ewolucji polityk publicznych względem cyberbezpieczeństwa w Polsce. Wykorzystano cztery metody badawcze:

1. **Analiza dyskursu** – na podstawie źródeł pierwotnych: oficjalnych przemówień oraz wypowiedzi, oficjalnych stanowisk, aktów prawnych, dokumentów strategicznych, raportów, materiałów promocyjnych firm oferujących rozwiązania dla cyberbezpieczeństwa. Zastosowano przy tym następujące techniki badawcze: analizę treści, analizę semiotyczną, analizę kontekstową, analizę intertekstualną, analizę ram (*frame analysis*), charakterystykę dyskursu.
2. **Wywiady badawcze** – 31 wywiadów pogłębionych przeprowadzonych z aktorami mającymi wpływ lub biorącymi bezpośredni udział w badanych procesach, między innymi ministrem cyfryzacji, pełnomocnikiem rządu ds. cyberbezpieczeństwa, doradcą Prezydenta RP i innymi (pełną listę zamieszczono w Aneksie 1). Obraną techniką badawczą były wywiady częściowo strukturyzowane.
3. **Ankiety** – 374 ankiety zebrane podczas dwóch wydarzeń związanych z cyberbezpieczeństwem: Europejskiego Forum Cyberbezpieczeństwa CYBERSEC 2018 (Kraków, 8-9.10.2018) oraz Mega Sekurak Hacking Party 2019 (Kraków, 25.02.2019). Dobór dwóch odmiennych grup respondentów zastosowano celowo. Założono, iż uczestnicy CYBERSEC Forum, zgodnie z formatem oraz zakresem merytorycznym wydarzenia, reprezentują grupę badanych zajmujących się cyberbezpieczeństwem z perspektywy strategii państwa oraz firm, realizacji polityk publicznych, a także tworzenia oraz implementacji regulacji i ram prawnych. Druga grupa respondentów, obecna na Mega Sekurak Hacking Party, zgodnie z tematyką oraz formatem wydarzenia, objęła osoby zainteresowane technicznym wymiarem bezpieczeństwa TIK, szczególnie administratorów sieci, pentesterów, programistów oraz innych pracowników działów IT. W trakcie CYBERSEC Forum zebrano odpowiedzi od 200 badanych w czasie rozmów prowadzonych przez 11 ankieterów[4]. W trakcie Mega Sekurak Hacking Party

[4] Ankieterami byli studenci socjologii Uniwersytetu Jagiellońskiego realizujący w ten sposób obóz badawczy. W tym miejscu chciałbym podziękować zarówno samym uczestnikom obozu, jak i dr. Witowi Hubertowi za współpracę. Podziękowania należą się także organizatorowi wydarzenia, Instytutowi Kościuszki, za możliwość przeprowadzenia badań.

zebrano łącznie 174 arkusze ankietowe, które rozdawano w formie wydruku do samodzielnego wypełnienia przez uczestników[5].

4. **Obserwacja uczestnicząca** – łącznie w latach 2017-2020 wykonano ponad 9 tysięcy godzin obserwacji uczestniczącej podczas 21 konferencji i wydarzeń branżowych (pełną listę zamieszczono w Aneksie 2) oraz pracy trzech podmiotów:
   a) Instytutu Kościuszki – think tanku będącego jednym z kluczowych interesariuszy tematyki cyberbezpieczeństwa w Polsce;
   b) Polskiego Klastra Cyberbezpieczeństwa #CyberMadeInPoland – podmiotu zrzeszającego firmy sektora cyberbezpieczeństwa w Polsce;
   c) Grupy Roboczej ds. Cyberbezpieczeństwa działającej przy Ministerstwie Cyfryzacji / Cyfryzacja KPRM.

Stan badań

Problematyka społecznej konstrukcji zagrożeń wynikających z TIK stanowi temat dociekań naukowych zwłaszcza w badaniach nad procesami sekurytyzacji oraz militaryzacji cyberprzestrzeni. Próbę wpisania omawianego zagadnienia w ramy teorii stworzonej przez szkołę kopenhaską stanowi artykuł Lene Hansen oraz Helen Nissenbaum *Digital Disaster, Cyber Security, and the Copenhagen School*, opublikowany w „International Studies Quarterly"[6]. Badaczki postulują w nim konceptualizację cyberbezpieczeństwa jako bezpośredniego wyniku sekurytyzacji bezpieczeństwa komputerów (*computer security*). Pogłębioną analizę omawianej problematyki znaleźć można w pracach Myriam Dunn Cavelty. Zarówno w monografii *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*[7], jak i szeregu artykułów oraz referatów naukowych analizuje ona procesy sekurytyzacji TIK w określonych wspólnotach narodowych bądź też na poziomie międzynarodowym. Militaryzacja dyskursu dotyczącego cyberprzestrzeni stanowi także jeden z kluczowych tematów prac badaczki. Należy zwrócić uwagę, że

[5] W tym miejscu chciałbym podziękować portalowi Sekurak za możliwość przeprowadzenia badań podczas wydarzenia.

[6] L. Hansen, H. Nissenbaum, *Digital Disaster, Cyber Security, and the Copenhagen School*, „International Studies Quarterly" 2009, Vol. 53, No. 4, 1155-1175.

[7] M. Dunn Cavelty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, Oxon–New York 2008.

Bibliografia

Dokumenty

98th U.S. Congress, Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, P.L. 98-473, 98 Stat. 2190, [on-line:] https://www.congress.gov/bill/98th-congress/house-bill/5112.

100th U.S. Congress, Computer Security Act of 1987, H.R.145, [on-line:] https://www.congress.gov/bill/100th-congress/house-bill/145.

104th U.S. Congress, National Information Infrastructure Protection Act of 1996, S.982, [on-line:] https://www.congress.gov/bill/104th-congress/senate-bill/982.

107th U.S. Congress, Cyber Security Research and Development Act. Communications and telecommunications, Nov. 27, 2002, H.R. 3394, [on-line:] https://www.govinfo.gov/app/details/PLAW-107publ305.

107th U.S. Congress, Federal Information Security Management Act of 2002, Mar. 5, 2002, H.R.3844, [on-line:] https://www.congress.gov/bill/107th-congress/house-bill/3844.

107th U.S. Congress, Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot Act) Act of 2001, Oct. 26, 2001, H.R.3162, [on-line:] https://www.congress.gov/bill/107th-congress/house-bill/3162/text/enr.

114th U.S. Congress, Countering Foreign Propaganda and Disinformation Act, July 14, 2016, S. 3274, [on-line:] https://www.congress.gov/bill/107th-congress/house-bill/3844.

116th U.S. Congress, Ending Forced Arbitration for Victims of Data Breaches Act of 2019, H.R. 327, Indtroduced Jan. 8, 2019, [on-line:] https://www.govtrack.us/congress/bills/116/hr327.

116th U.S. Congress, Ending Forced Arbitration for Victims of Data Breaches Act of 2019, H.R.327, Indtroduced Jan. 8, 2019.

BBN, *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, 2014, [on-line:] https://www.bbn.gov.pl/ftp/SBN%20RP.pdf.

BBN, *Strategia bezpieczeństwa narodowego Rzeczypospolitej Polskiej*, 2020, [on-line:] https://www.bbn.gov.pl/ftp/dokumenty/Strategia_Bezpieczenstwa_Narodowego_RP_2020.pdf.

Commission of the European Communities, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions: Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime*, COM(2000)

890 final, 26.01.2001, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52000DC0890&from=CS.

Commission of the European Communities, *Communication from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions: Network and Information Security: Proposal for A European Policy Approach*, COM(2001) 298 final, 6.06.2001, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52001DC0298&from=EN.

Council of Europe, *Enhanced international cooperation on cybercrime and electronic evidence: Towards a Protocol to the Budapest Convention*, 19.03.2018, [on-line:] https://rm.coe.int/t-cy-pd-pubsummary-v6/1680795713.

Cyberbezpieczeństwo i obrona. Rezolucja Parlamentu Europejskiego z dnia 22 listopada 2012 r. w sprawie bezpieczeństwa cybernetycznego i cyberobrony (2012/2096 (INI)), Dz. Urz. UE C 419/145, 16.12.2015.

Decyzja Nr 17/MON Ministra Obrony Narodowej z dnia 5 lutego 2019 r. w sprawie powołania Pełnomocnika Ministra Obrony Narodowej do spraw utworzenia wojsk obrony cyberprzestrzeni, Dz.U. MON 2019, poz. 23.

Deklaracja końcowa szczytu NATO w Warszawie. Wydana przez Szefów Państw i Rządów uczestniczących w posiedzeniu Rady Północnoatlantyckiej w Warszawie w dniach 8 i 9 lipca 2016 r., „Bezpieczeństwo Narodowe" 2016, nr 37-40, s. 205-242, [on-line:] https://www.bbn.gov.pl/ftp/dok/03/37-40_KBN_Deklaracja_szczytu.pdf.

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, 19.07.2016.

Dyrektywa Parlamentu Europejskiego i Rady 2013/40/UE z dnia 12 sierpnia 2013 r. dotycząca ataków na systemy informatyczne i zastępująca decyzję ramową Rady 2005/222/WSiSW, Dz. Urz. UE L 218/8, 14.08.2013.

European Commission, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: The European Agenda on Security*, COM(2015) 185 final, 28.04.2015, [on-line:] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0185&from=GA.

European Commission, *Growth, competitiveness, and employment: The challenges and ways forward into the 21st century*, White Paper, COM(93) 700 final, 5.12.1993.

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council and the Council: Increasing resilience and bolstering capabilities to address hybrid threats*, JOIN(2018) 16 final, 13.06.2018, [on-line:] https://eeas.europa.eu/sites/eeas/files/joint_communication_increasing_resilience_and_bolstering_capabilities_to_address_hybrid_threats.pdf.

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action Plan against Disinformation*, JOIN(2018) 36 final, 5.12.2018, [on-line:] https://eeas.europa.eu/sites/eeas/files/action_plan_against_disinformation.pdf.

European Commission, High Representative of the European Union for Foreign Affairs and Security Policy, *Joint Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions:*

Streszczenie

Rozprawa podnosi kwestię społecznej konstrukcji niebezpieczeństw wynikających ze wzrastającej zależności wszelkich sfer aktywności ludzkiej od sprawnego funkcjonowania technologii informacyjno-komunikacyjnych. Celem ogólnym pracy jest analiza społecznych procesów konstruowania problematyki cyberbezpieczeństwa w polskiej przestrzeni publicznej w latach 2017-2021. Jest to realizowane przez identyfikację głównych dyskursów o cyberbezpieczeństwie obecnych w Polsce. Zgodnie z wynikami przeprowadzonych badań zagrożenia związane z funkcjonowaniem technologii informacyjno-komunikacyjnych były postrzegane w Polsce przez pryzmat pięciu dyskursów o cyberbezpieczeństwie: technologicznego, bezpieczeństwa narodowego, obywatelskiego, stosunków międzynarodowych i gospodarczego. Najbardziej rozpowszechnione oraz wpływowe, także pod kątem kształtowania polityk publicznych, okazały się dyskursy dotyczące technologii i bezpieczeństwa narodowego, odpowiednio, z ramami: *bezpieczeństwo sieci i systemów informatycznych* oraz *bezpieczeństwo cyberprzestrzeni*.

Słowa kluczowe: cyberbezpieczeństwo, dyskurs, sekurytyzacja, Polska

Summary

The dissertation focuses on the social construction of dangers resulting from increasing dependence on the continuous functioning of information and communication technologies. The author's aim is to analyze the social processes of constructing cybersecurity issues in the Polish public debate between 2017 and 2021. This is carried out by identifying the main cybersecurity discourses in Poland. The results suggest that threats related to the functioning of information and communication technologies were perceived through the prism of five types of cybersecurity discourse: technological, civic, international, economic and discourse on national security. The most widespread and influential types of discourse, also in terms of shaping public policies, turned out to be technological and national security discourses.

Keywords: cybersecurity, discourse, securitization, Poland

Książka opisuje kwestię społecznej konstrukcji niebezpieczeństw wynikających ze wzrastającej zależności wszelkich sfer aktywności ludzkiej od sprawnego funkcjonowania cyberprzestrzeni. Przeprowadzone badania pokazują, że zagrożenia związane z bezpieczeństwem technologii informacyjno-komunikacyjnych są postrzegane w Polsce przez pryzmat różnych dyskursów o cyberbezpieczeństwie: dotyczących technologii, bezpieczeństwa narodowego, stosunków międzynarodowych, a także gospodarki.

Publikacja stanowi wstęp do problematyki cyberbezpieczeństwa i ukazuje problem na podstawie badań dotyczących Polski. Z pewnością będzie cennym źródłem informacji dla osób zainteresowanych bezpieczeństwem narodowym oraz IT.

WYDAWNICTWO KSIĘGARNIA AKADEMICKA Sp. z o.o. Kraków

https://akademicka.pl

ISBN 978-83-8138-709-5