Uniwersytet Pedagogiczny im. Komisji Edukacji Narodowej w Krakowie
Wydział Humanistyczny
Instytut Politologii

Agnieszka Warchoł

Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku

Praca doktorska

STRESZCZENIE

Tytuł dysertacji doktorskiej to *Wpływ cyberprzestrzeni na bezpieczeństwo państwa na początku XXI wieku*. Celem rozprawy doktorskiej jest przedstawienie, w ujęciu kompleksowym, wpływu cyberprzestrzeni na politykę bezpieczeństwa państwa u progu XXI wieku, a więc systematyzacja informacji w tym zakresie, zawartych zarówno w źródłach tradycyjnych, jak i internetowych. Dodatkowo, poprzez zestawienie zagadnień teoretycznych z praktycznymi aspektami funkcjonowania państwa w cyberprzestrzeni, praca ma się przyczynić do pogłębienia stanu badań nad oddziaływaniem cyberprzestrzeni na politykę bezpieczeństwa państwa. Z racji aktualności tematu, informacje zawarte w rozprawie doktorskiej mogą być przydatne do zgłębiania wiedzy nie tylko przez studentów i naukowców, ale także wszystkich użytkowników cyberprzestrzeni.

Ramy czasowe dysertacji doktorskiej to lata 2007-2015. Za początek rozważań został uznany 2007 rok. Ma on wymiar symboliczny, gdyż odnosi się do ataku cybernetycznego wymierzonego w Estonię. To wydarzenie spowodowało zwrócenie międzynarodowej uwagi na problem cyberbezpieczeństwa. Cezurę czasową niniejszej pracy zamyka 2015 rok, jednakże zakres rozważań zostanie rozszerzony o bieżące wydarzenia, których jesteśmy świadkami. Ponadto, w rozprawie znajdą się również odniesienia do incydentów sprzed 2007 roku, co ma na celu wprowadzenie do aktualnych problemów.

Wybór tematu uzasadniam chęcią przyczynienia się do wzrostu świadomości społeczeństwa w zakresie zagrożeń dla państwa w cyberprzestrzeni. Państwo to my – obywatele, więc jego skuteczna ochrona zależy bezpośrednio od nas.

Głowna teza dysertacji zawiera się w stwierdzeniu, że na początku XXI wieku, cyberbezpieczeństwo jest podstawowym wyzwaniem dla polityki bezpieczeństwa państwa.

Do jej zweryfikowania i realizacji postawionego celu przyjęłam holizm metodologiczny. Pozwala on łączyć różne metody analizy, charakterystyczne dla nauk społecznych. W niniejszej pracy zastosowałam następujące metody badawcze:

- metoda porównawcza,
- analiza i krytyka źródeł,
- analiza i krytyka piśmiennictwa,
- metoda historyczna.

Bezpieczeństwo cyberprzestrzeni oraz pojawiające się w niej zagrożenia są tematem niezwykle aktualnym. Jest to stosunkowo nowy obszar badawczy. Brakuje w tym zakresie kompleksowych opracowań, zwłaszcza będących owocem pracy polskich naukowców. Na naszych oczach zmienia się sposób postrzegania bezpieczeństwa, a celem politologów powinna być szybka reakcja i opis problemu. Podjęłam próbę charakterystyki cyberprzestrzeni jako politycznego zagrożenia, szansy i wyzwania, by podkreślić, iż rozwój nauki i nowoczesnych technologii wpływa kompleksowo na politykę bezpieczeństwa państwa.

Niniejsza rozprawa doktorska składa się z pięciu rozdziałów, aneksów, zakończenia, bibliografii, spisów: tabel, wykresów, rysunków i map.

Rozdział pierwszy *Istota cyberprzestrzeni* ma charakter wprowadzający i ilustruje istotę cyberprzestrzeni. W pierwszym fragmencie dysertacji znajduje się także próba prezentacji siatki pojęciowej wykorzystanej w dalszych częściach rozprawy doktorskiej. Po niej następuje charakterystyka cyberprzestrzeni oraz specyfikacja problemu badawczego. Niezwykle ważne jest spojrzenie na kwestie wpływu cyberprzestrzeni na politykę bezpieczeństwa państwa przez pryzmat teorii stosunków międzynarodowych, teorii socjologicznych i rozwoju społecznego. Tej tematyce poświęcona jest ostatnia część wprowadzającego rozdziału.

Rozdział drugi *Państwo w cyberprzestrzeni* stanowi część rozważań, poświęconą trzem kategoriom poznania naukowego, które determinują bezpieczeństwo państwa:

- wyzwania,
- szanse,
- zagrożenia.

Ten rozdział traktuje o zagrożeniach w cyberprzestrzeni dla polityki bezpieczeństwa państwa. Wymieniam w nim podmioty odpowiedzialne za kreowanie zagrożeń w

cyberprzestrzeni, i stawiam następujące pytania: jak państwo może pozytywnie wykorzystać cyberprzestrzeń? przed jakimi wyzwaniami współcześnie stoją państwa, by zapewnić swoim obywatelom bezpieczeństwo?

Rozdział trzeci *Prawne aspekty ochrony cyberprzestrzeni* został poświęcony prawnym aspektom ochrony cyberprzestrzeni. Rozpoczynam go od rozważań dotyczących prawa międzynarodowego. Na podstawie dokumentów wiążących wiele stron, podejmuję próbę udzielenia odpowiedzi na następujące pytania badawcze: czy istnieją międzynarodowe normy traktatowe dotyczące operacji militarnych w cyberprzestrzeni? czy agresja w cyberprzestrzeni może prowadzić do zastosowania konwencjonalnych środków odwetowych przez poszczególne państwa?

Po rozważaniach dotyczących prawnego aspektu ochrony cyberprzestrzeni o zasięgu międzykontynentalnym, skupiłam się na zagadnieniu dotyczącym dbałości o cyberbezpieczeństwo przez organizacje o charakterze regionalnym. W tej części pracy starałam się omówić najważniejsze regulacje Unii Europejskiej i Rady Europy. Ostatni fragment rozdziału poświęcony jest kwestii ochrony cyberprzestrzeni na gruncie prawa krajowego.

W rozdziale czwartym pt. *Bezpieczeństwo cyberprzestrzeni Rzeczypospolitej Polskiej w latach 2011-2015* podejmuję kwestie związane z ochroną infrastruktury krytycznej, w tym rodzimych systemów teleinformatycznych. Pomimo ustalonych ram czasowych, w celu dokładniejszego ujęcia problemu, sięgam do 2001 roku, kiedy strona polska podpisała Konwencję Rady Europy o cyberprzestępczości. W kolejnej części omawiam wydarzenia z lat 2011-2015. Dolna cezura czasowa określa moment ukazania się definicji „cyberprzestrzeń" w polskim prawie. Pojawienie się „cyberprzestrzeni" w języku prawnym, i zarazem prawniczym, wyznacza jedną z granic niniejszych rozważań, ponieważ umożliwiło to tworzenie aktów prawnych dotyczących *expressis verbis* cyberprzestrzeni. Kończąc ten fragment podjęłam charakterystykę podmiotów odpowiedzialnych za cyberbezpieczeństwo Rzeczypospolitej Polskiej.

Rozdział piąty dysertacji doktorskiej *Ochrona cyberprzestrzeni w wybranych państwach i inicjatywy międzynarodowe* obejmuje analizę empirycznych przykładów funkcjonowania państw w cyberprzestrzeni. Korzystając z rozwiązań zastosowanych w państwach takich jak: Estonia, Stany Zjednoczone Ameryki, Federacja Rosyjska, Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej oraz Turcja, starałam się odpowiedzieć na następujące pytania badawcze: czy ww. państwa posiadają strategie i

doktryny ochrony cyberprzestrzeni? czy posiadają wykwalifikowanych specjalistów do prowadzenia działań w cyberprzestrzeni, których można nazwać cyberżołnierzami?

W końcowym fragmencie rozdziału zajęłam się tematem aktywności ponadnarodowej w zakresie utrzymania globalnego cyberbezpieczeństwa. Swoje rozważania kończę odpowiedzią na pytanie: czy powstają ponadnarodowe inicjatywy w zakresie zwiększenia świadomości oraz pogłębiania umiejętności w zakresie rozpoznawania zagrożeń w cyberprzestrzeni?

W dysertacji doktorskiej została wykorzystana głównie literatura polsko- i anglojęzyczna. Problemem jaki napotkałam podczas pracy nad rozprawą doktorską był z jednej strony nadmiar informacji, i co za tym idzie *attention crash,* z drugiej strony – niedostateczna ilość źródeł wiarygodnych, państwowych. Te, do których posiadam dostęp są jawne. Mowa tu o ustawach, doktrynach, strategiach, itd. Reszta jest utajniona. Wbrew pozorom to dobra wiadomość. Im więcej danych dotyczących bezpieczeństwa państwa nie jest ujawnianych, tym lepiej jesteśmy chronieni, gdyż informacje nie dostają się do osób nieuprawnionych.

The impact of cyberspace on state security at the beginning of the 21st century

ABSTRACT

The title of the dissertation is *The impact of cyberspace on state security at the beginning of the 21st century*. The intent of this thesis is to explore the topic of the state functioning in cyberspace. The purpose of the dissertation is to present, in a comprehensive perspective, the impact of cyberspace on the state security policy at the turn of the 21st century. The time frame is 2007-2015. The beginning of the discussion (2007) has a symbolic dimension. It refers to the cyberattack targeted at Estonia. This incident has brought international attention to the issue of cyber security. The timing of this work closes in 2015, but the scope of the discussion will be extended to the current events. In addition, there will be references to pre-2007 ways, which are intended to prelude current matters.

The choice of the topic is justified by the desire to contribute to increasing public awareness of cyber threats. The state is us, citizens, thefore effective protection depends directly on us.

The main thesis of the dissertation is that at the beginning of the 21st century cyber security is a fundamental challenge for the state security policy.

I have chosen methodological holism to verify and achieve this goal. It allows to combine different methods of analysis, specific to social sciences. In this dissertation I applied the following research methods:

- the comparative method,
- analysis and criticism of sources,
- analysis and criticism of literature,
- the historical method.

The security of cyberspace and its emerging threats are extremely topical. This is a relatively new research area. There are no comprehensive studies in this field, especially as a result of the work of Polish scientists. The way of security perception is changing, so the goal of political analysts should be quick reaction to describe the problem.
I have attempted to characterize cyberspace as a political threat, chance, and challenge, in order to emphasize that the development of science and modern technology has complex impact on the state security policy.

This dissertation consists of five parts: the first chapter is introductory and illustrates the essence of cyberspace. In the first part of the dissertation I also attempted to present a conceptual framework used in later parts of the dissertation. It follows the characteristics of cyberspace and the specification of the research problem. It is extremely important to look at the impact of cyberspace on the state security policy through international relations, sociological and social development theories. This topic is in the last part of the introductory chapter.

The second part of the dissertation is entitled *State in cyberspace*. This is a comprehensive passage containing three categories of scientific knowledge that determine the security of the state:

- challenges,
- chances,
- threats.

This chapter concerns the cyber threats for state security policy. I mention the entities responsible for creating threats in cyberspace, and I ask the following questions: How can the state positively benefit from cyberspace? What challenges do the state face today to ensure safety for citizens?

The third chapter relates to the legal aspects of cybersecurity. I started with the considerations of the international law. Based on documents, binding many signatories, I try to answer the following research questions: are there international treaties for military operations in cyberspace? Can aggression in cyberspace prompt the usage of conventional retaliatory measures by individual states?

After discussing the legal aspect of protection the intercontinental cyberspace, I focused on the issue of cyber security by regional organizations. In this part of the dissertation, I tried to discuss the most important regulations of the European Union and the Council of Europe. The last section of this chapter is devoted to protection of cyberspace under the national law.

Cyber security is the part of the information security of the state. I wrote more about it in the fourth chapter of the dissertation, which is titled *Security of cyberspace of the Republic of Poland in 2011-2015*. In this section I discuss issues related to protection of critical infrastructure, including vernacular IT systems. In spite of the established timeframe, in order to accurate the identification of the problem, I return to 2001, when the Polish side signed the Convention on Cybercrime. In the next section I discuss the events of 2011-2015. The beginning of the time frame determines the moment when the definition of ‘cyberspace’

appeared in Polish law. The arrival of term ‘cyberspace’ in the legal language sets one of the limits of the present considerations, because it has enabled the creation of legislation regarding cyberspace. At the end of this section, I take into account the characteristics of entities responsible for cyber security of Poland.

The last chapter of the dissertation dissertation includes an analysis of the empirical examples of states functioning in cyberspace. I have discussed the solutions used in countries like Estonia, the United States of America, the Russian Federation, the United Kingdom of Great Britain and Northern Ireland, and Turkey, and on this basis I have tried to answer the following research questions: Do these countries have strategies and doctrines for cybersecurity? Do they have qualified cyber-professionals who can be called cyber-soldiers?

In the final section of the chapter I discuss the topic of transnational activity in the field of global cyber security. My reflection ends with the answer to the question: are there transnational initiatives to increase awareness and deepen cybercrime skills? Does the international environment create initiatives to increase awareness and skills for the identification of cyber threats?

While working on my dissertation I used mainly Polish and English literature. The problem I encountered, at the time of writing, was, on the one hand, the excess of information, and consequently the *attention crash*, on the other hand, insufficient number of credible, state sources. The ones, which I have access, are open. The rest of information is classified. Contrary as it seems, this is good news. The more data regarding state security is not disclosed, the better we are protected, because the information is not accessible for the unauthorized.