Streszczenie

W dysertacji scharakteryzowano podstawy walki informacyjnej, odnosząc się do jej sposobów realizacji w cyberprzestrzeni. Wskazano kluczowe znaczenie informacji we współczesnym świecie, wykazując przy tym, że jest ona zasobem strategicznym dla państwa. Omówiono ewolucję wojny informacyjnej, wskazując problem, z jakimi borykają się współczesne organizacje w jej przetwarzaniu. Przedstawiono analizę działań informacyjnych, z wykorzystaniem różnorodnych modeli walki, które wykorzystane razem, pozwalają na wieloaspektową ocenę prowadzonych operacji informacyjnych, na współczesnym polu walki.

Scharakteryzowano cyberprzestrzeń, jako specyficzne środowisko walki, w którym zachodzą skomplikowane relacje pomiędzy podmiotami, prowadzącymi działania w cyberprzestrzeni. Analizie poddano proste techniki ataków cyfrowych oraz omówiono, na czym polegają wysoce skorelowane, wysoce ustrukturyzowane ataki, których egzemplifikacją jest cyberwojna. Analiza literaturowa raportów stanu bezpieczeństwa cyberprzestrzeni oraz pozycji poświęconych konfliktom zrealizowanym, w tym specyficznym środowisku walki (w formie case study), pozwoliła wysunąć tezy dotyczące dominujących trendów w cyberprzestrzeni, podatności celów, oraz wykorzystywanej w tych atakach cyberbroni. Dysertacja zawiera opis samodzielnej eksploracji autora w sieci TOR, która skoncentrowana była na uzyskaniu dostępu do stron hackerskich i oprogramowania złośliwego używanego do ataków w cyberprzestrzeni.

W rozprawie ocenie poddano metody prognozowania, zarówno ilościowe, jak i jakościowe. Przedstawiono analizę szeregów czasowych, popartą własnymi badaniami oraz omówiono metody prognozowania, pozwalające nadążyć za dużą dynamiką zmienności cyberprzestrzeni, w tym analizę systemową i metody scenariuszowe.

Dysertacja zawiera wyniki badań analizy otoczenia cyberprzestrzeni, które pozwoliły na sformułowanie czterech scenariuszy stanów jej otoczenia. Przedstawione wyniki analizy zagrożeń, w postaci ataków cyfrowych na elementy infrastruktury krytycznej, predysponowały do stworzenia scenariusza zdarzeń (zagrożeń), w którym ujęto prognozy dotyczące ewolucji ataków. Zespolenie obu scenariuszy pozwoliło ukonstytuować „scenariusz bezpieczeństwa Rzeczypospolitej Polskiej w cyberprzestrzeni na lata 2021-2022”. Stał się on podstawą do analizy obowiązującej strategii cyberbezpieczeństwa RP i sformułowania wniosków dotyczących określenia nowej strategii.

Abstract

The dissertation describes the basics of information warfare, referring to its methods of implementation in cyberspace. The key importance of information in the contemporary world has been indicated, showing that it is a strategic resource for the state. In paper the evolution of information warfare was discussed, pointing to the problem faced by contemporary organizations in its processing. An analysis of information activities is presented, with the use of various combat models, which, when used together, allow for a multi-faceted assessment of information operations carried out on the contemporary battlefield.

Cyberspace has been characterized as a specific combat environment in which there are complex relationships between entities operating in cyberspace. The simple techniques of digital attacks were analysed and the meaning of highly correlated, highly structured attacks exemplified by cyber warfare was discussed. Literature analysis of cyberspace security status reports and items devoted to realized conflicts, in this specific combat environment (in the form of a case study), made it possible to put forward theses about the dominant trends in cyberspace, the vulnerability of targets, and the cyber weapons used in these attacks. The dissertation describes the author's independent exploration of the TOR network, which was focused on gaining access to hacker sites and malware used for attacks in cyberspace.

In the dissertation, forecasting methods, both quantitative and qualitative, were assessed. The analysis of time series is presented, supported by own research, and forecasting methods are discussed, allowing to keep up with the large dynamics of cyberspace variability, including system analysis and scenario methods.

The dissertation contains the results of research into the cyberspace environment analysis, which allowed for the formulation of four scenarios of its surroundings. The presented results of threat analysis, in the form of digital attacks on elements of critical infrastructure, predisposed to the creation of an event (threat) scenario, which includes forecasts of the evolution of attacks. Combining the two scenarios allowed to constitute the "scenario of the security of the Republic of Poland in cyberspace for the years 2021-2022". It became the basis for the analysis of the current cybersecurity strategy of the Republic of Poland and the formulation of conclusions regarding the definition of a new strategy.