KD 0076/2013

Przedmiotem zainteresowania Autora rozprawy pt. „Wykorzystanie internetu jako środka zagrożenia bezpieczeństwa w konflikcie asymetrycznym" stały się obecne i przyszłe starcia w cyberprzestrzeni. Celem Autora było wykazanie podobieństw pomiędzy metodami walki stosowanymi w wirtualnym świecie do metod walki asymetrycznej widocznej we współczesnych konfliktach oraz taktyce militarnej.

Dysertacja została podzielona na pięć rozdziałów. Każdy z nich zawiera wprowadzenie do omawianej w nim problematyki eksponując tezy i kończy się podsumowaniem syntetycznie przedstawiając wnioski płynące z poruszonej problematyki cząstkowej.

W pierwszym rozdziale pracy wskazano i przeanalizowano ewolucję zjawiska, z jakim mamy do czynienia obecnie – ewolucji Internetu od zapotrzebowania na niezawodny system komunikacji w warunkach wojny jądrowej po jego dzisiejszą formę. Omówione zostały również procesy, które doprowadziły m.in. do powstania złośliwego oprogramowania oraz opisane postaci kilku znanych hakerów, co pozwoliło lepiej zrozumieć analizowaną tematykę. Całość procesów została skompresowana do najważniejszych faktów, w celu wskazania podstawowych procesów kształtujących analizowane zjawisko i ich współczesnych przejawów.

W drugim rozdziale przedstawiono listę czynników wpływających na poziom bezpieczeństwa czy też zagrożenia państwa. Analizie poddano zarówno czynniki stałe, takie jak wojny czy katastrofy naturalne, jak i czynniki wynikające z ewolucji i dynamiki społeczeno-ekonomiczno-politycznej, które obecnie wpływają na strukturę państw na świecie. Wskazane zostały czynniki szczególnie w obszarze ładu miedzynarodowego oraz ewolucji społecznej mające bezpośredni i negatywny wpływ na poziom bezpieczeństwa tradycyjnych struktur państwowych. Jednocześnie te zjawiska okazały się być silnie powiązane z rewolucją technologiczną w obszarze IT, w szczególności społeczeństwa informacyjnego. Centralnym elementem w tej nowej społeczności okazał się Internet. Powyższe czynnniki pokazały, iż konflikt w cyberprzestrzeni w sposób naturalny stał się konfliktem asymetrycznym, gdyż obecne zmiany ewolucyjne w ładzie światowym sprzyjają działaniom niekonwencjonalnym i nieprowadzącym do bezpośrednego starcia ani dużych zniszczeń mogących zagrozić wytworzonej międzynarodowej sieci powiązań społecznych, ekonomicznych i politycznych.

W trzecim rozdziale zostały poddane analizie obecne kierunki rozwoju badanego zjawiska. Przedstawiono kwestię wojny informacyjnej, wskazując jednocześnie, iż jest ona niezwykle ważnym aspektem działań w konflikcie w cyberprzestrzeni. Przeanalizowano również opracowania teoretyczne – dorobek naukowy – w obszarze badanego zjawiska. Zwrócono uwagę na szczególnie rozwinięte analizy badaczy rosyjskich. Przedstawiono

również powody i analizy wskazujące, że w przyszłości, aspekt działań w cyberprzestrzeni będzie stałym elementem holistycznej taktyki w tradycyjnym konflikcie zbrojnym. Równocześnie wskazano na wciąż trudne do algorytmicznego ujęcia zagrożenie badawcze wynikające z wprowadzenia nowych technologii, które w sposób istotny mogą wpłynąć na badane zjawisko, m.in. sztuczna inteligencja, komputery kwantowe czy rozwój kryptowalut.

W czwartym rozdziale została przedstawiona struktura czterech państw rozwijających swoje metody walki w cyberprzestrzeni: Stanów Zjendoczonych, Chińskiej Republiki Ludowej, Wielkiej Brytanii i Federacji Rosyjskiej. Zdaniem Autora niezwykle istotne w tym ujęciu są nie tyle możliwości technologiczne, lecz przede wszystkim rozwinięcie odpowiedniego zaplecza teoretycznego i intelektualnego przed budową zdolności do działań w cyberprzestrzeni. Widoczne jest to przede wszystkim w przypadku Federacji Rosyjskiej, w której stworzono bogate zaplecze teoretyczne nt. wykorzystania działań poniżej progu wojny, gdzie ważnym elementem operowania stała się cyberprzestrzeń. Punktem wyjścia w tym przypadku była chęć oddziaływania na przeciwnika na wszelkich dostępnych płaszczyznach uniemożliwiając mu jednocześnie działania obronno-odwetowe przy użyciu konwencjonalnych wojskowych środków. W tym aspekcie wydaje się, że Państwa Zachodu we wstępnym etapie eksploracji cyberprzestrzenii nie do końca dotrzymały tempa rozwoju własnych narzędzi obronnych względem Federacji Rosyjskiej i Chińskiej Republiki Ludowej. Stało się tak też ze względów na odmienne pojmowanie ochrony własnych interesów przez ww. państwa, a przede wszystkim różnic w wolności dostępu i wykorzystania cyberprzestrzeni dla własnych społeczeństw.

The main subject of the author`s dissertation is titled: "Using the Internet as a security threat in asymetric warfare" and that has become the current and future cyberspace clash. The main purpose of the author was to present the similiarities between the methods of war applied within a virtual world, to methods of conflict in an asymetric warfare that are currently observed and applied in a virtual world, seen in todays conflicts and military tactics.

This dissertation was divided into five chapters. Every one of them contains an introduction that discussed the exposing thesis and ended with a summary which presented the conclusion of the partial issues.

The first chapter indicates and analyzes the evolution of the internet due to demands necessary for a reliable communication system in the conditions of nuclear war to its present form. The processes that led to the creation of malicious software and figures of famous hackers were presented which allowed the reader to better understand the analyzed topic. All processes were compressed to the most significant facts in order to outline the basic changes in the analyzed phenomenom and its modern signs.

The list of factors that influence the security level or threat to the country were presented in the second chaper. Constant wars or natural catastrophes, factors resulting from evolution and social-economic-political dynamics that currently influence countries structure all over the world were taken into the consideration and analyzed. The outlined factors in international order and social evolution were presented that have a direct and negative impact on traditional state structures. At the same time, these phenomena were proven to be highly tied with both the technological revolution in the area of IT, and information in the society. The central element of the new community proved to be the Internet. All above factors showed that the conflict in cyberspace naturally became the asymetric conflict. In addition, the current evoluationary changes in world order favored unconventional actions preventing direct clashes leading to massive damages that might endanger the existance of formed international net of social, economic and political ties.

The third chapter focused on the analysis of the current development of the examined case. Information about warfare was presented, indicating that it is an extremeley important aspect of actions in cyberspace conflict. Theoretical academic achievements were analyzed remaining in the scope of this topic. Great focus was highlighted on the Russian researchers analysis. Methods and analysis presented the future aspects of cyberspace operations which will be a inevitable element of holistic tactics in the traditional military conflict. At the same time, new technologies introduced such as: artificial intelligence, quantum computers and cryptocurrency evolution are still difficult be taken into the reasearchers algorythmic

assessment of the examined cases.

Four countries listed: United States of America, People`s Republic of China, Great Britain and the Russian Federation, building its potential in cyberspace, were presented in the fourth chapter. From the author`s perspective it is most crucial to build a theoretical and intellectual basis in order to conduct actions in cyberspace versus gaining technological abilities. This can be observed in the case of the Russian Federation, where the theroetical background for the use of actions in cyberspace under the threshold of war are the important element. The main point is to gain an advantage over the enemy in all the possible areas. At the same time disables the enemy and its chance to conduct defence-retaliatory actions with the use of conventional military means. It seems that western countries are still in the initial phase of cyberspace exploitation. They did not manage to keep up with the pace of their own developments in the defense tools in comparision to the Russian Federation or People`s Republic of China. Furthermore, it became obvious that the mentioned above countries have different understandings of the protection of their own interests. Societies in each individual country have different permission, and access to cyberspace.