V. Herasymchuk, Student
V. Shadura, Senior Lecturer
Zhytomyr Polytechnic State University

OSINT IN INFORMATION WARFARE

In the current digital era, information warfare has become a critical tool for governments, organizations, and individuals to obtain an advantage over their opponents. A key aspect of information warfare is the use of OSINT. Open-source intelligence is a type of intelligence gathering that focuses on utilizing publicly available information. This information is collected, analyzed, and shared in a timely manner with the relevant audience to satisfy a specific intelligence or information requirement. Moreover, OSINT also encompasses the intelligence produced by this discipline. This definition is in accordance with FM 2-0. [1]

Using OSINT in information warfare has become more popular in recent years, especially as more and more information is available on the internet. OSINT sources include social media, public records, and online forums. These sources can help to understand an enemy's actions. For example, OSINT allows identification of an opponent's location, communication methods, and personnel. Hence, different tools and techniques are used to collect, analyze, and disseminate information. Data mining is used to search and analyze large amounts of data to identify patterns and trends. Sentiment analysis is a technique that uses natural language processing to detect the emotions and opinions expressed in online content. Geolocation involves identifying the physical location of an individual or object using data from GPS devices or other sources.[2]

However, the use of OSINT in information warfare is not without its challenges and ethical considerations. False information and disinformation can spread rapidly online, and it is hard to confirm the accuracy of OSINT data. Additionally, using personal data can infringe on people's privacy and civil liberties. Therefore, it is important for those using OSINT in information warfare to be aware of these risks and take steps to mitigate them.

OSINT has been used in various situations such as cyber operations, geopolitical conflicts, and terrorism. For example, OSINT was used in the investigation of the 2014 downing of Malaysia Airlines Flight MH17 crash in eastern Ukraine. OSINT was also applied to identify the Russian «Buk» missile launcher believed to have been used in the attack, as well as the individuals responsible for transporting and operating it.[3][4]

In conclusion, OSINT is a valuable tool in information warfare as it can provide insights into an adversary's activities, intentions, and vulnerabilities. However, those who use OSINT must be aware of the ethical concerns and challenges involved, such as false information, disinformation, and violations of privacy and civil liberties. By using OSINT effectively and ethically, those involved in information warfare can gain a significant advantage over their adversaries.

REFERENCES

1. US Army. Open-Source Intelligence: ATP 2-22.9 / US Army., 2012. – 91 c.

2. https://www.researchgate.net/publication/353806347_Open_Source_Intelligence_and_its_Applications_in_Next_Generation_Cyber_Security_-_A_Literature_Review
3. https://en.wikipedia.org/wiki/Malaysia_Airlines_Flight_17
4. https://www.bellingcat.com/news/uk-and-europe/2015/10/08/mh17-the-open-source-evidence/