
AN ANALYSIS OF ICT IMPACT ON UKRAINE AND RUSSIA CONFLICT

Sabaria Catharin Debora

International Relations Study Program, Faculty of Humanities, Bina Nusantara
University

sabaria.debora@binus.ac.id

Abstract : This research discusses the impact of information and communication technology (ICT) on the conflict between Ukraine and Russia that led to the annexation of Crimea by Russia in 2014. This study uses qualitative approach to analyze the selected issue. The data were taken from case study articles and official websites. The analysis of the formulated problem is carried out by combining hegemony theory, agenda setting theory and securitization theory. The agenda setting theory of Maxwell E. McCombs and Donald L. Shaw is used to analyze the use of ICT, Antonio Gramsci's hegemony theory is used to analyze the hegemony of ICT in Ukraine and Russia, while Barry Buzan's theory of securitization is used to analyze the negative effects of the abuse of ICT during the duration of the conflict. The research found that ICT has significant impact and influence in Ukraine and Russia conflict and is a clear example of the use of ICT abuse in Eastern Europe. The information war between Russia and Ukraine led to the annexation of Crimea by Russia. The success of Russia in annexing Crimea without armed contact and casualties is a clear evidence of how ICT can be an effective and efficient weapon to achieve national interests. From the analysis, it can be concluded that the development of ICT not only bring a positive impact on the society, but also negatively affect modern conflict, such as seen in the conflict between Ukraine and Russia.

Keyword: ICT, conflict, Ukraine, Russia, information war

Submission	:	Aug 11 th 2021
Revision	:	Sept 18 th 2021
Publication	:	Nov 28 th 2021

INTRODUCTION

Technological globalization has brought humanity into a new chapter of information and communication technology (ICT), which has become one of the factors in shaping global governance. The advancement of ICT has shifted the communication model from conventional to digital so that it can be done anytime and anywhere. Advances in ICT have also enabled humans to digitally access information and carry out activities in various fields digitally. The definition of ICT in general is a broad term of information technology that refers to communication technologies such as the internet, wireless networks, cellular phones, computers, software, social networks, and other applications that enable users to access, retrieve, store, transmit and manipulate information in the form of digital (ICT, 2021). Another definition of ICT is the various

types of technological devices and resources that are used as tools to transmit, store, create, share, or exchange information (ICT, 2021).

Humans who are ICT users are referred to as the information society. There is no standard definition of what is meant by the information society. Abdul Waheed Khan, UNESCO's Assistant Director-General for Communication and Information said that "information society is the building block for knowledge societies". However, in general, information society could be defined as a situation where every individual can use the internet. The purpose of the information society is to gain competitive advantage internationally using information technology in creative and productive ways. There are three main characteristics of the information society. First, information is used as an economic resource. An organization can maximize the use of information to increase efficiency and effectiveness, as well as innovate. Second, to identify the main uses of information because people generally use information in their activities as consumers. Third, development of the information industry which is usually related to technology infrastructure (Moore, 2020). The information industry can develop if it is balanced with the development of technology infrastructure. In the end when the infrastructure is built, there will be a technology-based information society. Therefore, technological innovation with economic dimension will always be implicit in the life of the information society. Thus, it can also be said that information technology is a product or result of an information society.

Positively, the advancement of ICT makes human life easier. However, advances in information and communication technology can also have various negative impacts because they are vulnerable to misuse. This study will analyze how the impact of ICT application on the conflict between Ukraine and Russia that led to the annexation of Crimea in 2014. The rift between Ukraine and Russia began at the end of 2013 under the leadership of Viktor Yanukovich. Yanukovich's decision to withdraw from signing the Association Agreement (AA) and the Deep and Comprehensive Free Trade Agreement (DCFTA) with the European Union sparked the anger of the Ukrainian people (Ukraine, 2020). Russia is suspected to be influencing Yanukovich's decision. A wave of massive protests led to the removal of Yanukovich from the presidency by the Ukrainian Parliament Verkhovna Rada. Tensions between the two countries reached the peak during Russia's annexation of Crimea. The dismissal of Yanukovich raised concerns among Crimean, the majority of whom speak Russian and are supporters of the former president. On March 16, 2014, after undergoing a referendum, Crimea joined Russia (Ukraine, 2021). The result of the referendum sees as many as 96.8% of Crimean people said they wanted to join Russia (Ukraine, 2021). Russia officially annexed Crimea after President Vladimir Putin signed the decree "on the recognition of the Republic of Crimea" (Ukraine, 2021). The annexation of Crimea by Russia surprised the international

community because Russia did not use excessive military force and used more advances in ICT.

Tensions between Ukraine and Russia back then led to conflicts that continues to this day. The conflict between the two countries does not only use military force but also concrete evidence of the misuse of ICT to fulfill political agendas and ultimately has an impact on the life of the information society in Ukraine and Russia. Russia's use of ICT in its conflict with Ukraine is known as an information war. Aki-Mauri Huhtine defines information warfare as the use of technology in the midst of a crisis or conflict to achieve specific goals against an opponent or enemy (Huhtinen, 2007). According to Aki-Mauri Huhtine, there are two types of information warfare. The first type is more of a psychological warfare because it involves the media to have a psychological impact and influence people's perception. The second type is war related to electronics and the internet (cyber warfare). This type can be done using a personal computer, sending viruses to damage information systems and a country's defense, disinformation, electronic warfare, hackers or using electromagnetic waves with the aim of damaging ICT infrastructure.

This study combines the hegemony theory of Antonio Gramsci, the agenda setting theory popularized by Maxwell E. McCombs and Donald L. Shaw, and the securitization theory of Barry Buzan. Hegemony theory holds that the foundation of society plays a role in shaping culture, values, and ideology. The ruling class is not only able to control the economic structure and institutions in society, but also to control ideology and politics (Altheide , 1984). Through research conducted by Maxwell E. McCombs and Donald L. Shaw, it is proven that the media can contain certain agendas, especially political agendas with the aim of influencing the audience's political stance. In general, the definition of agenda setting as quoted from *Mass Media, Mass Culture* by James R. Wilson, and Roy S. Wilson, is the process of mass media determining what audiences should think and worry about (seeting, nd). On the other hand, according to Barry Buzan, the types of threats to a country consist of military, political, social, economic, and environmental (Buzan , 1983). The application of hegemony theory to this research can be seen in the hegemony of ICT in Ukraine and Russia. Meanwhile, the Agenda Setting theory is used to analyze how ICT can be used to convey certain purposes from parties who have political interests. Securitization theory looks at how the misuse of ICT can threaten the security of a country.

LITERATURE REVIEW

This research refers to several scientific articles. The first article is taken from the writings of Keir Giles who is an expert in information warfare and the Russian military. In his article "The Next Phase of Russia Information Warfare", Keir Giles describes the information warfare methods used by Russia in an effort to control Crimea and confront

Ukraine. The methods used include using social media to influence public opinion and carrying out personal attacks on military personnel as well as sabotaging telecommunications networks and internet infrastructure in Ukraine and Crimea (Giles, 2016).

The second literature that became a reference for this research is also written by Keir Giles. In *Handbook of Russian Information Warfare*, Keir Giles describes the concept of information warfare strategy, its objectives and history of development, implementation, and prospects in the future. Keir Giles wrote it because the information war that arose in the midst of the political crisis of Ukraine and Russia became a concern of Western countries (Giles, 2015).

The third literature is taken from the writings of Andrew S. Weiss, "New Tools, Old Tricks: Emerging Technologies and Russia's Global Tool Kit". In his writings, Weiss explained that the decline of Russian weapons technology was one of the backgrounds that changed Western countries' perception of Russia's military capabilities. Western countries tend to no longer see Russia as a threat because of the declining technological developments in the country. In the same article, Weiss also tries to explain how Cyber Russia, in the midst of obstacles in innovation in research and development, is able to pose a threat and cause damage which is shown through the annexation of Crimea and the election of Donald Trump as president of the United States (Weiss, 2021). Furthermore, this study also analyzes how Russia has managed to take traditional cyber operations to a more modern level. In realizing its ambition to increase its influence in global level, Russia is maximizing the use of propaganda, disinformation, high politics, high-level diplomacy, and intelligence tactics by involving all sectors, both private and state-owned. Though imprudent at times, Russia's use of information technology has tremendous destructive power. According to Weiss, the reason is that the Russian side has innovative and aggressive capabilities. In general, it can conclude from this scientific article that this tactic is not new to Russia, as it used in the Cold War era.

The fourth literature is taken from the writings of Bettina Renz and Hanna Smith titled "Russia and Hybrid Warfare - Going Beyond the Label". In their writings, Renz and Smith describe how Russia is fully aware of how behind they are in weapons technology. Therefore, Russia developed a strategy called hybrid war (Gibridnaya Voina). One strategy of hybrid war is to use media and social media as weapons with the aim of influencing public perception of Russia (Renz, 2016). By using this strategy, Russia is considered by Western countries to have succeeded in taking over Crimea without resorting to violence or using military means. A Russian figure who has an important role in developing the "hybrid war" strategy is Valery Gerasimov. He argues that changes in military strategy need to be made because of the increasing role of the economy and information in modern conflicts.

METHOD

This research uses qualitative research method. In *Introduction to Qualitative Research*; Beverly Hancock et al. wrote that “qualitative research focuses on reports of experience or on data which cannot be adequately expressed numerically” (Hancock, et al, 2007). The method is used because the data sources come from the analysis of scientific articles and official websites.

RESULTS & DISCUSSION

Russia's use of ICT in the conflict with Ukraine was motivated by the country's experience when it was involved in a conflict with Georgia. Russia realizes that its military equipment is far behind compared to Western countries, especially the United States. Therefore, Russia has switched to a war strategy that does not only rely on military equipment, but also maximizes the use of ICT. Russia's success in annexing Crimea without using armed force shows that the country has succeeded in utilizing ICT measurers to achieve its political interests. It is proof that the advancement in ICT can also have a negative impact. The International Telecommunication Union (ITU), a specialized UN agency operating in the field of information technology, regularly measures the ICT Index of a country. This measurement aims to determine the level and ICT development in a country yearly; to find out the development of ICT in developed and developing countries; to find out the digital divide in a country; and to uncover potential development in the field of ICT. The measurement component of the ICT Index includes ICT access, use and skills. Some of the indicators included in the measurement are the use of cellular phones, internet bandwidth, computer and internet use, the percentage of individuals who use the internet and literacy rate (Union, 2015). The last measurement of the ICT Index was in 2017. The measurement in the following year could not be carried out due to several obstacles. Comparatively in terms of the ICT index, Ukraine, and Russia both have weaknesses compared to other European countries. Both countries have low rankings compared to Eastern, Western and Scandinavian countries. The 2017 ICT Index data shows Russia is ranked 45th and Ukraine is ranked 79th (ICT, 2017). In terms of internet penetration, Statista data for 2020 shows that Russia is still better than Ukraine. Internet penetration in Russia reaches 76%, while Ukraine is still around 57%. The data above is evidence of why when there was a conflict, Russia was superior and dominant than Ukraine(Statistica, 2020).

Russia's superiority in internet penetration makes it easier for the country to use ICT as part of its information warfare strategy against Ukraine. The higher percentage of internet penetration indicates that the information society in Russia uses the internet more than in Ukraine. The limitations of Ukrainian people in accessing the internet have resulted in Russia being relatively more advantaged in the use of information warfare strategies. In terms of skills in the field of ICT, the difference in the percentage of Russians

living in rural and urban areas is not much of a difference. From 2017 to 2020, the percentage of the Russian information society living in urban areas is around 94 – 96%. Meanwhile, the percentage of Russian information society living in rural areas who have ICT skills is around 86 – 88%. From these data it can be analyzed that thanks to high internet penetration, Russia has superior ICT skills than Ukraine (ICT, 2020).

Based on the data above, it can be seen how Russia uses its advantages in terms of ICT to deal with the conflict with Ukraine. Russia uses its widely accessible news site to spread propaganda related to the conflict with Ukraine. ICT also allows Russia to limit the information that can be accessed by the people from Crimea. Another impact of ICT related to the Ukraine and Russia conflict is the use of social media. The percentage of Russian people who use social media as of 2020 reaches 72 million of the total population of 145 million (Statistica, 2020). Meanwhile, social media users in Ukraine by 2021 will reach 25 million out of 44 million population (Digital, 2021). The difference in the number of users who are not balanced, has an impact on Russia's dominance in the information war by using social media platforms.

One of the paradoxes of the information society is the condition in which information can be reproduced very easily which in turn leads to various problems, including violations of intellectual property rights. In a UNESCO publication related to the World Summit on the Information Society, through the Fifth International Conference on Adult Education Declaration on Adult Learning held in Hamburg, Germany on July 1997, it was stated that the development of information and communication technology (ICT) brought new risks to social life both for individuals and even the business world. Therefore, it is necessary to establish ethics in the life of the information society where piracy is included in the discussion. From the results of the 2014 World Summit on the Information Society publication, there are 9 things that need to be considered in the ethics of the information society, namely: principles, participation, people, profession, privacy, piracy, protection, power, and policy (Geneva, 2013).

Principles relate to ethical values in the information society. The point is that knowledge in society can continue to be sustainable, coherent, innovative, and integrative if they are not only based on practical opportunities or political or financial interests but are also based on ethical values. Participation means that access to information, communication, education, and knowledge is open to all, both free of charge and at affordable prices for all economic groups. Meanwhile, People relates to community, identity, gender, generation, and education. This means that people here are the key figures who act as senders and recipients in the process of transferring information, communication, and knowledge. Therefore, it is emphasized how their role in carrying out their function to filter the information given or received, and how to respect differences and uphold equality.

Profession means ethics in professions related to information. Those who have professions in the field of information and communication have a special responsibility in implementing the basic values in the ethics of the information society. Meanwhile, privacy is how to ensure the protection of the private life of the information society. On the other hand, piracy is an ethics that is often violated because it involves protection of copyright or intellectual property. Piracy can also be categorized as cybercrime. The next ethics is protection or protection for children and adolescents. Internet access that can be done through computers, smartphones, and tablets where young people are connected, make them vulnerable to dangers such as sexual exploitation. Therefore, protection is a violation of ethics. Next is power, which emphasizes economic and political power, they must not show power or control each other, but share and use them for the benefit of the wider community. Lastly is the policy that emphasizes how the government in a country ensures that there are rules that support the life of the information society. The use of ICT in the Ukraine-Russia conflict shows a violation of information society ethics related to power. Under the leadership of Vladimir Putin, Russia is known as a country that has freedom of expression that is limited by the government. The majority of media outlets are controlled by the government. This control makes it easier for Russia to carry out its information warfare strategy in dealing with Ukraine. Russian news portals have changed from being a source of information to being a tool for government propaganda. In terms of the use of media outlets, Russia can be said to be superior. The popularity of Russian media outlets such as TASS, Sputnik International, Ria Novosti and Interfax far exceeds that of Ukrainian media outlets such as UNIAN and Ukrayinska Pravda. The control of the Russian government is not only limited to news portals, but also on social media. The conflict with Ukraine, which is still ongoing today, also uses social media channels. The misuse of ICT in the Ukraine-Russia conflict is one of the negative impacts related to the advancement of ICT in the political field.

Another impact of ICT, if it is related to the ethics of the information society, is related to policy. In this ethic, it is hoped that the government has clear rules to ensure the guarantee of freedom of expression, freedom of association in terms of ICT, and freedom to seek, receive and provide information without any restrictions. In terms of freedom of expression, Ukraine is slightly better off than Russia. Based on data from freedomhouse.org, freedom of speech and internet access in Ukraine is half free. Meanwhile, in Russia freedom of speech is very limited (Freedom, nd). Although internet penetration and social media users are much higher than in Ukraine, the government's supervision of the Russian information society is still very tight.

From the perspective of Hegemony theory, an analysis can be made on how ICT dominates various aspects of the Ukrainian and Russian information society. Humans consciously and unconsciously become part of the influence of ICT hegemony. From the perspective of Agenda Setting theory, it can be seen how ICT becomes a tool or media to

convey certain intentions from Ukraine and Russia with the aim of influencing public opinion. In the end, Ukraine uses ICT not only to defend its sovereignty, but also aims to attract the sympathy of the international community. Russia uses ICT in information warfare because it is fully aware that in defending its sovereignty, it cannot rely on conventional weapons. Russia uses ICT as a new weapon because it is relatively cheaper, has a wide range of utilities and has a greater impact. In terms of political interests, Russia uses ICT to gain international recognition for its existence. In terms of securitization theory, the hegemony of ICT against humans, which is then used for political purposes, has the potential to threaten the security of a country, in this case Ukraine and Russia.

CONCLUSION

From the analysis above, it can be concluded that the development of ICT does not only have a positive impact on society, but it can also have a negative impact. Regardless of the high or low ranking of the ICT Development Index, it does not necessarily prove that a country cannot abuse ICT. The conflict between Ukraine and Russia shows that there has been abuse of ICT development. ICT has become a hegemony tool in the information society of Ukraine and Russia. Everyone can maximize the use of ICT to convey personal, group and national agendas because the content of the media used can be arranged according to their wishes and interests. Distortion of information can not only threaten the security and integrity of a country but also has the potential to lead to a prolonged modern conflict as happened between Ukraine and Russia.

The conflict between the two Eastern European countries shows that advances in information and communication technology have not only changed the pattern of human life, but also the conventional methods of war. The conflict between Ukraine and Russia is a concrete example of the information war that has occurred in the 21st century. The use of ICT by Russia in the midst of the conflict with Ukraine shows how well an integrated and well-organized information warfare strategy is. Therefore, Ukraine tends to be unprepared to respond to Russia's strategy. Thus, it can be concluded that Russia is more dominant in the conflict with Ukraine.

REFERENCES

- Agenda Setting” (<http://zimmer.csufresno.edu/~johnca/spch100/7-4-agenda.htm>)
- Altheide, David. L. (1984). “Media Hegemony: A Failure of Perspective”, *The Public Opinion Quarterly*, Vol.48, No.2 (Summer, 1984), Oxford University Press on behalf of the American Association for Public Opinion Research
- Buzan, Barry. (1983). *People, States, and Fear: The National Security Problem in International Relations*. Brighton: Wheatsheaf Books Ltd.
- Countries and Territories. <https://freedomhouse.org/countries/freedom-world/scores>

- Digital 2021: Ukraine. <https://datareportal.com/reports/digital-2021-ukraine>
- Ethics in the Information Society: The Nine 'P's: A Discussion Paper for the WSIS+10 Process 2013 – 2015. Geneva: Globethics.net
- Giles, K., 2016. The Next Phase of Russian Information Warfare. Riga: NATO Strategic Communications Centre of Excellence
- Giles, Keir. (2015). Handbook of Russian Information Warfare.
- Hancock, B., Ockleford, E., & Windridge, K. (2007). An Introduction to Qualitative Research. The NIHR RDS EM
- Huhtinen, Aki-Mauri. (2007). Different Types of Information Warfare. National Defence College, Finland
- ICT Development Index 2017. <https://www.itu.int/net4/ITU-D/idi/2017/index.html> <https://www.statista.com/statistics/1187715/share-of-russians-with-ict-skills-by-area/>
- Information and Communication Technologies (ICT)* (2021). <http://aims.fao.org/information-and-communication-technologies-ict>
- Information and communication technologies (ICT)* (2021). <http://uis.unesco.org/en/glossary-term/information-and-communication-technologies-ict>
- International Telecommunication Union. 2015. Measuring the Information Society Report 2015 Executive Summary: Geneva Switzerland
- Internet Penetration in Central and Eastern Europe as of 2020, by country. <https://www.statista.com/statistics/1167158/internet-penetration-in-cee-region/>
- Moore, Nick. Chapter 20: The Information Study. Policy Studies Institute, United Kingdom
- Number of social network users in selected countries in 2020 and 2025. <https://www.statista.com/statistics/278341/number-of-social-network-users-in-selected-countries/>
- Putin Recognizes Crimea as Sovereign State, <http://ukraine.csis.org/crimea.htm#30>
- Renz, B., & Smith, H. (2016). Russia and Hybrid warfare - going beyond the label. (Aleksanteri Papers; No. 1/2016). Kikumora Publications. http://www.helsinki.fi/aleksanteri/english/publications/presentations/papers/ap_1_2016.pdf
- Share of population with information and communication technology (ICT) skills in Russia from 2017 to 2020, by type of area. <https://www.statista.com/statistics/1187715/share-of-russians-with-ict-skills-by-area/>
- The Ukraine Crisis Timeline: *Crimean Parliament Votes to Secede from Ukraine, Join Russia*, <http://ukraine.csis.org/crimea.htm#6>

The Ukraine Crisis Timeline: *Final Referendum Results:97% Favor Russia*, <http://ukraine.csis.org/crimea.htm#29>

Ukraine Suspend Preparations for EU Trade Deal, <http://ukraine.csis.org/kyiv.htm#1>

Weiss, Andrew S. (2021). *New Tools, Old Tricks: Emerging Technologies and Russia's Global Tool Kit*. Carnegie Endowment for International Peace