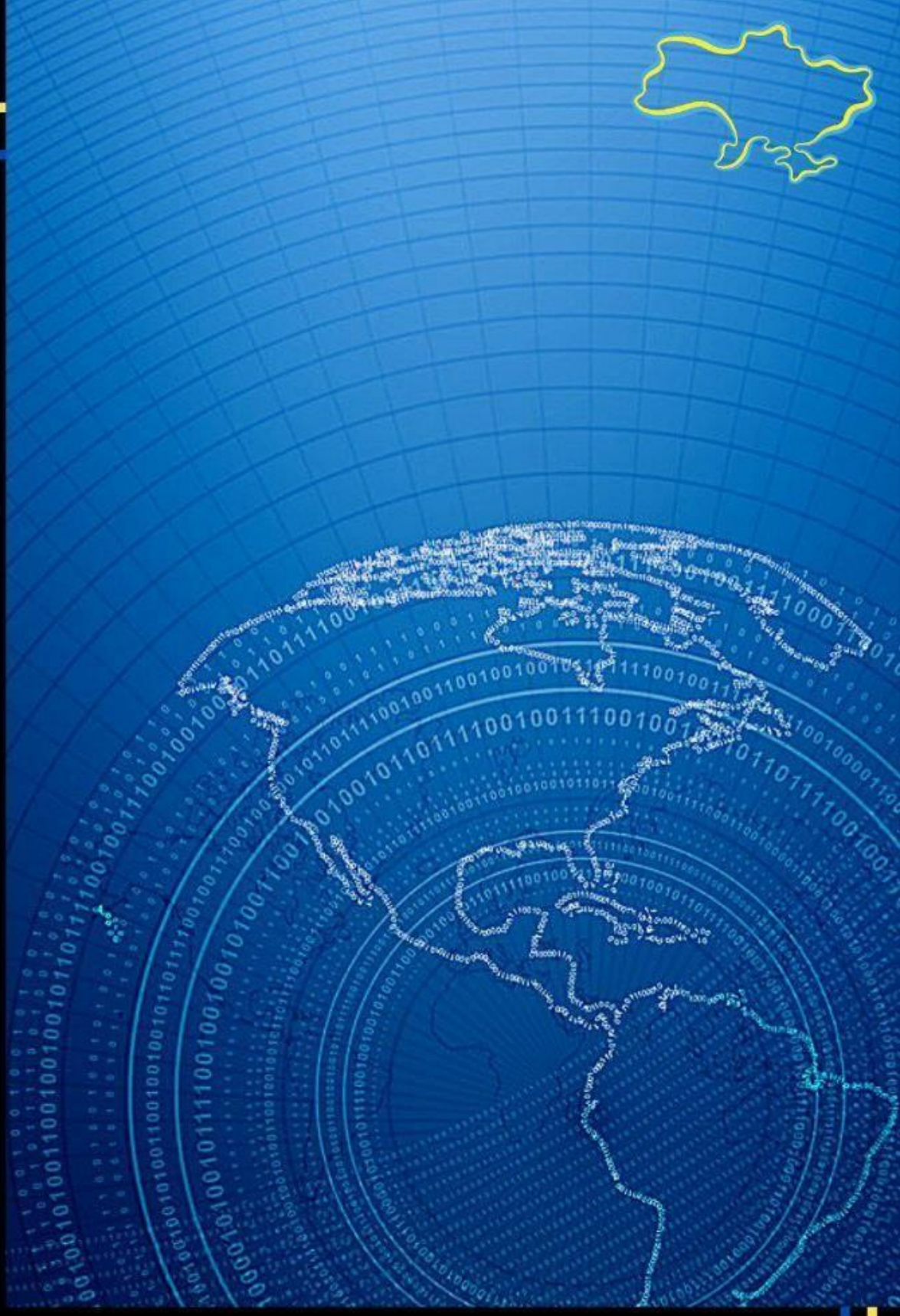
ТРАКТАТ СОВИ



ІНФОРМАЦІЙНІ ВІЙНИ: ПРИЧИНИ, ПРОБЛЕМИ, НАСЛІДКИ

Студентський науково-практичний журнал

12 ЛИПНЯ 2022 РОКУ

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

ТРАКТАТ СОВИ:

ІНФОРМАЦІЙНА ВІЙНА:ПРОБЛЕМИ ТА НАСЛІДКИ

ІІ Студентський науково-практичний журнал

12 липня 2022 року

Київ 2022

УДК; 330.341;338.24

Трактат сови: Інформаційна війна: проблеми та наслідки. Матеріали II студентського науково практичного журналу (м. Київ, 12 липня 2022 р.)/ За заг.ред. Харченко О.А. (та ін.). Київ. ДТЕУ. 2022.

У збірнику містяться матеріали, що були подані у II Студентський науково-практичний журнал «Трактат сови: Інформаційна війна: проблеми та наслідки» (м. Київ, 12 липня 2022 р.). Для студентів що займаються дослідженням питань соціально-економічного, інформаційного розвитку.

УДК 330.341; 338.24

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

Факультет інформаційних технологій

ЧЛЕНИ ОРГАНІЗАЦІЙНОГО КОМІТЕТУ

Харченко Олександр Анатолійович, кандидат технічних наук, доцент, декан факультету інформаційних технологій

Хорольська Карина Вікторівна, заступник декана факультету інформаційних технологій, асистент кафедри інженерії програмного забезпечення та кібербезпеки

Криворучко Олена Володимирівна, доктор технічних наук, професор, завідувач кафедри інженерії програмного забезпечення та кібербезпеки

Кулаженко Володимир Валерійович, кандидат економічних наук, доцент

Іванова Олена Миколаївна, кандидат економічних наук, доцент

Мельник Анастасія Юріївна, студентка факультету інформаційних технологій 4 курсу 1 групи

Васильєва Владлена Юріївна, студентка факультету інформаційних технологій 2 курсу 9 групи

Шаяхметова Олександра Русланівна, студентка факультету інформаційних технологій 4 курсу 1 групи

Кушка Антон Сергійович, студент факультету інформаційних технологій 3 курсу 7 групи

Астаф’єва Вікторія Сергіївна, студентка факультету інформаційних технологій 2 курсу 6 групи

ЗМІСТ

Astafieva V.S.,

bachelor's degree specialty «Computer Science»

faculty of Information Technology 2 courses 6 groups

State University of Trade and Economics

Kyiv, Ukraine

Scientific adviser: H. Starosta

Senior Lecturer at the Department of Modern European Languages

UKRAINIANS IN THE INFORMATION WAR AGAINST RUSSIA

Abstract: the information war of Ukraine against Russia, at the moment of its beginning, the current impact, the changes and consequences have been studied.

Key words: information war, sites, army, DDOS attack.

Russia has long been considered perhaps the strongest player in information wars. Over the past decade, Russian propaganda has managed to conduct several successful operations to destabilize the situation in the West - among the most successful ones is clearly the interference in the US presidential election in 2016.

So, it is necessary to understand what the information war between Ukraine and Russia is:

Russian-Ukrainian information war is a set of measures constantly carried out by governmental and non-governmental organizations of Russia and Ukraine in the information space of Ukraine, Russia, other countries and international organizations aimed at gaining strategic and political advantages by demoralizing or misleading the enemy and countering the other side in the global confrontation between Russia and Ukraine, as well as the confrontation between Russia and the "Western world". It has begun in times of the collapse of the USSR and is still going on to this day as an essential ideological component of the modern Russian-Ukrainian war. [1]

The main principles of the information war, which began an active phase on February 24, 2022 are:

• While Ukrainian cyber troops are working, Russian sites are resting.

• Troops are not just an IT army of programmers or marketers.

• This is the "Creative Forces of Ukraine" in the Telegram, which work with fakes.

• And the Instagram detachment of girls who posted cats on social networks a few days ago and are now blocking the pages of Russian propagandists.

Anyone can join the ranks of the IT army, no one there demands certificates and measure professional suitability. To do this, just join the Telegram channel “IT ARMY of Ukraine”, there are daily tasks of varying complexity, for people of different specialties.

For example, for psychologist Valery Androsov. He has past experience in IT and does not know from textbooks what a DDOS attack is.

“All IT fellow soldiers are engaged in such DDOS attacks, that is to attack enemy sites with a huge amount of data”, Valery Androsov says. “ In fact, it is very similar to gypsies who flock to you, overwhelm you with noise and information, and you just hang out, stand in a stupor and give money (sorry, all respectable and patriotic Roma, for such an example)”.

According to the psychologist, here is the same principle, that is, from a huge number of places comes a huge amount of data, the server does not have time to process them and just goes to bed. Everything to the primitive is simple and clear.

“To take part in the DDOS attack, you need to enter a certain program, depending on what you are working on”, Valery says. “Because there are tools for programmers, they are a bit more complicated, but the tasks and the result are greater. There are tools for ordinary people who just need to go to the site, press a few buttons, and thus help put some hostile information resource. But due to the fact

that many people come there to join the cyber war, such "light" sites go down by themselves, that is, it is not the most reliable thing".

I also have experience in DDOS attacks, and in order to create a community of people who can help the country in this, I organized a group of students from the Kyiv National University of Trade and Economics and all those who want to help.

We directly blocked pages on various social networks: Youtube videos with military positions and propaganda (Fig. 1), Telegram channels, posts on Instagram, Facebook and organized DDOS attacks on sites of military and political significance (Fig. 2).

Fig. 1 Example of videos that have been blocked

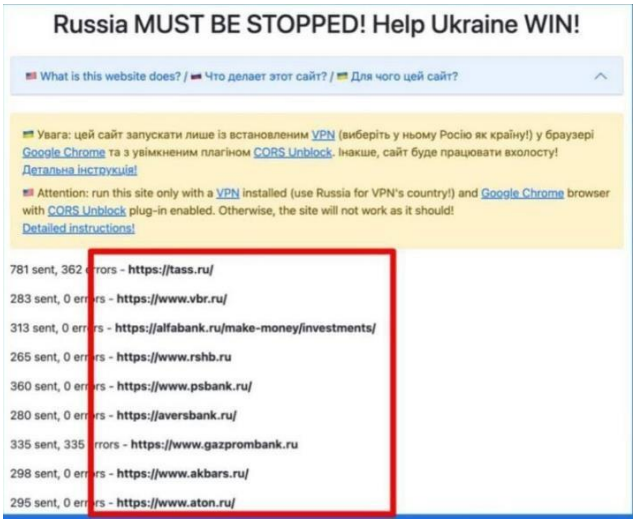


Fig.2 Links to sites and resources we used for attacks and block

What exactly is a DDOS attack?

A denial of service attack, DoS, is an attempt to cause harm by making the target system (such as a website or application) inaccessible to end users. To do this, attackers typically generate an insane number of packets or requests that the system cannot handle and becomes inaccessible to "normal" calls.

Hackers use multiple hacked and controlled sources (computers, smartphones, tablets) to carry out a distributed denial-of-service (DDoS) attack. This technique can be scattered around the world. It is virtually impossible to track the "main" computers from which attackers give orders to start or stop an attack. For example, in the case of Oschadbank, the system was torpedoed by about a million requests per second. In Privatbank the number of attacks is much bigger. [2]

The cyber army has its own front and the struggle against the strong advantage of Ukrainians continues on it. Creating chaos disorients the enemy and disrupts his logistics centers and networks.

I must say that the power of the centralized Russian military machine has in fact proved itself greatly exaggerated. The enemy has significant problems with information security, probably due to the usual negligence and corruption.

There are currently several areas on the cyber front.

These include:

• DDOS-attacks of Russian sites that slow down or disable the work of sites (government, banking institutions, media, information portals, etc.),

• sending letters,

• active presence in social networks.

In addition, there is a famous group of hackers Anonymous, who hack all sorts of databases to obtain important and valuable information, gain access to information sources, which allows us to transmit our information through them.

Anyone can join this fight, even without IT experience: there is a special chat in the telegram with instructions. It is impossible to find traces of Ukrainian cyber warriors, because all these attacks go through virtual networks.

As the Russian Federation denies the large number of dead and captured soldiers, and the sites that published information about it are being blocked en masse. The Ukrainians decided to convey this information to the occupiers by all means. Interview with a member of this front:

"I am just posting on Instagram and Facebook with the tags of those cities about which there is information that a military unit came from there. And now I'm still looking for forums where the mothers of Russian soldiers discuss the service. I also add comments on Google maps, to institutions. I am looking for the cities from which I am a prisoner. There are already calls on Instagram for those who are looking for their lost. To find or not to find - I do not know. "[3]

The information front during the war directly serves the fighting. That is, the country uses various tools to help itself in battle. Continuing the analogy between kinetic and information wars, imagine that territory can be compared to attention. That is, they are fighting and gaining attention in the information war. As a territory, it can be retained or reconquered. There are many ways to conquer territory in a kinetic war: to go on the offensive with artillery, to take the city in a ring or to land a landing party. Attentively similar.

So in this analogy, fakes are soldiers of the information army. They have a clear task. There are many of them in comparison with, say, technology. Russia's information and military tactics are very similar. They stamp fakes in packs, just as they send their soldiers to fight. In old and worn-out uniforms, without normal supplies. What is the story about a Russian lieutenant colonel who was taken prisoner in the pants [4] of the Ukrainian army. Inadequate fakes are sent by detachments to the Ukrainian infospace, and if they return - that is, do not receive enough attention - they are sent back into battle. There are fakes that are thrown over

the years over and over again. The Russians do not feel sorry for the infantry, as well as with the fakes. Always ready to send more. At the same level there are manipulations, speculations and other misfortunes.

Above the fakes are messages, clear and understandable messages. They are like rockets, they are released for a specific purpose. Messages can be true, manipulative or completely false. This is their danger, because if everything is quite clear with the fake, then with the message it is not. The message consists of fakes, that is, Russia uses fakes, half-truths and manipulations to fill the message, to shape it. They are much smaller than fakes, because resources are needed to form and promote a message. There can be several messages and sometimes they even contradict each other. For example, since the beginning of the full-scale invasion, Russian propaganda has been spreading the following messages: "Ukraine was preparing to attack Belarus", "Ukraine was preparing to attack Crimea", "Ukraine was preparing to attack Transnistria". At the same time, Russia is constantly repeating the message about the "weakness of the Ukrainian army". What does not prevent the Russians, when it is beneficial to them, to say that they are opposed by a strong and numerous "American-trained" opponent.

In healthy strategic communication, messages should not contradict each other, but in the world of Russian information influences, everything is different. Because Russia's task is often to confuse the audience, to confuse it so much that its coordinate system is completely lost. In other words, Russia does not necessarily want to force Ukrainians to believe in something; on the contrary, it often tries to undermine trust and say that no one can be trusted.

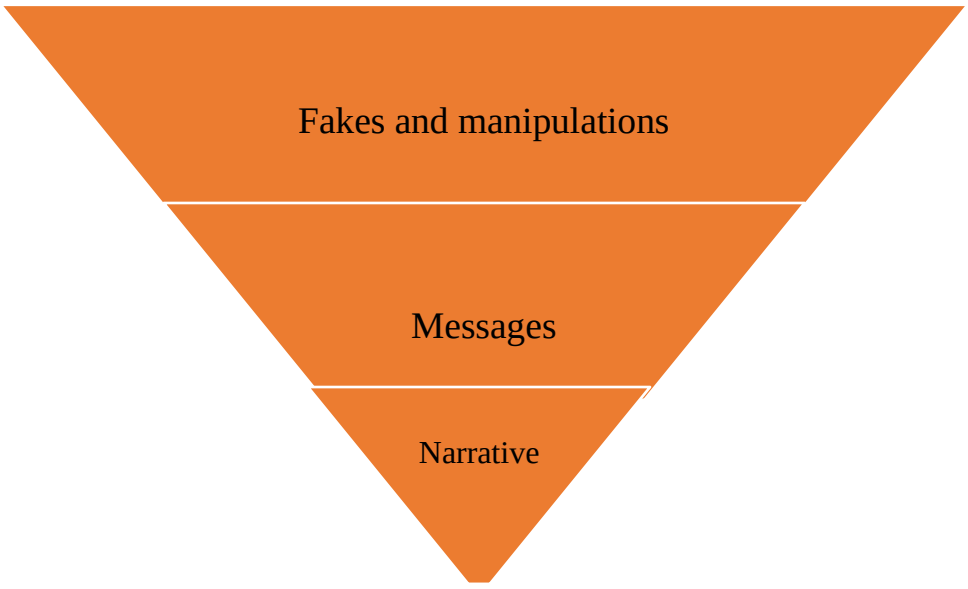
The collection of messages is combined into a narrative. Such a story, a story that explains the world around. The task of narratives is to form a certain worldview. The narrative is the most strategically important, because the messages can be modified, and the narrative is a constant story. Time and resources are needed to form a narrative qualitatively. Russia's most popular narrative about Ukraine is the assertion of an "insolvent state." The messages that fill this narrative are about

history, corruption, culture, economics, and so on. That is, anything that can be used to confirm the narrative.

Another central narrative is the assertion of "Ukrainian Nazis". Russia uses this worldview as one of the grounds for a full-scale invasion of Ukraine. Moreover, to feed this narrative, the Kremlin continues to talk about the denazification of Ukraine as one of the demands of peace agreements. This narrative is also filled with various messages concerning both Ukrainian history and the present. In particular, "Ukraine is ruled by Nazis", "Ukraine has forgotten about the victory over Nazism", "the UPA is Hitler's collaborators" or that the slogan "Glory to Ukraine!" Is a tracing of the Nazi slogan "Heil Hitler!". This list is endless.

So, there is a narrative that consists of messages that feed on fakes, manipulations and speculations.

This is the pyramid of information warfare:



You can easily identify Russian fakes, but at the same time succumb to certain messages of Russian misinformation or generally believe in the narrative. It is also important to remember that informational and psychological influence is always carried out in order to change behavior. That is, each fake, provocation or speculation in its entirety must push to action. For example, to vote for a particular

party in the election, to go or not to protest. There are many tools in the arsenal of the Russian propaganda machine: from "active events" on the ground to bots on social networks. That is, the tools may be different, but the meanings of informational influence are always built on the principle of "narrative - messages - fakes, manipulation, speculation."

- Groups that before the war were imprisoned for something completely different, are now actively fighting against fakes, mostly Instagram, - says Victoria. - For example, we have a small victory - Mykola Baskov's post is already officially called - "false information". He has already created a new profile where he writes that he was blocked by the Ukrainian authorities, but the comments under his post are laughable - there the girls write: "Kolya, don't worry, it's not the government, it's us." [5]

What helps Ukrainians to actively wage an information war?

First, it is the active actions of the Ukrainian authorities. Volodymyr Zelensky quickly became one of the symbols of the Ukrainian struggle, and his appeals are constantly aimed at supporting the fighting spirit of both the army and the entire Ukrainian people.

Minister of Digital Transformation Mikhail Fedorov is also actively working with thousands of international companies, providing them with truthful information and clearly explaining that any cooperation with Russia is toxic. The results of this work are enormous: hundreds of large companies have left the Russian market to allocate funds to support Ukrainian refugees. And the employees of these companies will learn the truth about the war in Ukraine.

The Ukrainian army is also promptly updating a huge amount of information - from the loss of the enemy to calls not to publish the exact addresses of enemy shells.

Secondly, it is the Ukrainian cyber army. Telegram has launched several channels that organize a digital resistance that opposes Russian propaganda and

coordinates cyberattacks against Russian media in an attempt to bring the truth to the international community.

Eliot Higgins, one of the founders of the Bellingcat project, says that for the first time in a long time, it is the disinformation fighters who win the information war, not the disseminators.

Third, these are Ukrainian programmers who have been attacking Russian media sites, banks and government agencies since the first days of the war, and creating various sites to help volunteers and refugees from Ukraine.

The IT army is destroying everything in its path:

• IT specialists put up the Russian website of the State Service for 1 minute

• The Moscow Stock Exchange fell in 5 minutes. Sberbank and BestChange managed to do the same

• Websites of the FSB, Roskomnadzor, the President of the Russian Federation, the Government of the Russian Federation, the State Duma, the Federation Council and a number of others fell

• The website of the National Bank of Belarus is adjacent, as dozens of other strategic websites are

• The sites of the largest Russian media have been hacked: TASS, "Kommersant" and "Fontanka"

• The site of the occupiers with a propaganda merch was blocked

• Finally, the truth about the war in Ukraine was seen and heard on digital television in Russia.

Conclusions: So, the key to winning the information war in the era of social media is to understand that the audience is not only its target, but also its participant. Unity and the desire to share the necessary messages with the whole world became

the most important weapon, which led to the fact that Ukraine completely defeated Russia on the information front.

It can be argued that during the information war the enemy can manipulate consciousness for large-scale expansion and threaten Ukraine's national security. Therefore, adequate information counteraction is needed. The main strategy is to show how we want to see the new Ukraine.

References:

1. РОСІЙСЬКО-УКРАЇНСЬКА ІНФОРМАЦІЙНА ВІЙНА [Електронний ресурс] – Режим доступу до ресурсу: http://surl.li/cejgz .

2. DDOS- ТА ІНФОРМАТАКИ: УРОКИ ДЛЯ УКРАЇНИ, УКРАЇНЦІВ ТА БАНКІВ [Електронний ресурс] / 2022 – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-economy/3406448-ddos-ta-informataki-uroki-dla-ukraini-ukrainciv-ta-bankiv.html

3. ІТ-армія не вбиває, але робить боляче. [Електронний ресурс] /2022 – Режим доступу до ресурсу: https://vn.20minut.ua/Podii/it-armiya-ne-vbivae-ale-robit-bolyache-11528834.html

4. УКРАЇНСЬКА ПРАВДА [Електронний ресурс] / – 2022. –Режим доступу до ресурсу: https://www.pravda.com.ua/news/2022/03/22/7333529/

5. DDOS-атаки, фото полонених: як українці атакують ворога на кіберфронті [Електронний ресурс] / – 2022. – Режим доступу до ресурсу: https://vchasnoua.com/donbass/71793-ddos-ataki-foto-polonenikh-yak-ukrajintsi-atakuyut-voroga-na-kiberfronti

Будьонний М. А.,

здобувач освітнього ступеня «бакалавр» спеціальності

«Комп'ютерні науки»

факультету інформаційних технологій 2 курсу 6 групи

Державний торговельно-економічний університет

м. Київ, Україна

ІНФОРМАЦІЙНІ ВІЙНИ: ПРОБЛЕМАТИКА ТА НАСЛІДКИ

Інформаційну війну як термін сформував американський дослідник М. Маклуен: «Істинно тотальна війна – це війна за допомогою інформації». Мається на увазі, що та ж боротьба за капітал, простори збуту та інші ресурси чи ідеї відходять на другий план, головним постає доступ до інформаційних ресурсів, знань. Це призводить до того, що сучасні війни все частіше ведуться на так званому «невидимому» фронті, в інформаційному просторі за допомогою інформаційних же видів озброєння.

Інформаційна війна, тобто війна за допомогою потоків інформації, описується ще в Біблії, де згадано персонажа на ім'я Гедеон, який під час воєн постійно вдавався до залякування ворога. Одного разу його «операція» призвела до того, що його супротивник злякався настільки, що завдав удару по своїм же військам.

Проте найбільшого значення інформаційні війни набули в XX ст., коли стали масовими газети, активно почали використовуватись телебачення, радіо та інші виду зв'язку, що зробило можливим поширення великих блоків інформації на великі відстані та між численними людьми. [1]

Вже в 20-х роках XX ст. країни почали використовувати нові засоби інформації аби просувати свої ідеї, ідеологію, політичні погляди тощо в маси (як на своїх співгромадян, так і на чужих).

Метою інформаційної війни вважають намагання однієї сторони погіршити моральні та матеріальні сили та можливості супротивника або опонента/конкурента та посилити власні. Цей вид війни передбачає широке використання пропагандистського впливу на свідомість людей в ідеологічних та емоційних галузях, частіше всього в різноманітних формах, аби збити цільового глядача з пантелику і не дати йому зрозуміти, що він дивиться банальну пропаганду, а не якийсь дискурс.

Інформаційна війна не призводить до безпосереднього кровопролиття чи руйнувань, не позбавляє людей даху над головою, що і є головною проблемою інформаційних війн. Все тому, що в наші час інформаційна війна є частиною більш страшною за своєю суттю війною – гібридної.

Вже гібридна війна має як ознаки інформаційної, так і реальної війни, інформаційна ж «готує» людей до того, що почнеться згодом, що і викликає в мислячих людей більше всього острахів та хвилювань.

В той же час, не можна недооцінювати ті руйнування, які інформаційні війни завдають суспільній психології та психології окремої людини. Іноді психологічні впливи є набагато серйознішими за ті, які людина може відчути під час безпосереднього військового конфлікту, хоча, знову ж-таки, не слід забувати про гібридну війну.[2]

Чим суспільство є розвиненішим та осучасненим, тим більше воно залежить від інформації та від ти джерел, за допомогою яких воно цю інформацію і отримує. Це можна назвати і благословенням і прокляттям водночас. Чим людина сучасніша, тим більше і тим якісніше вона мислить, проте в той же час і більш вразливішою виявляється перед впливом та навіть маніпулюванням ворожих систем. Інтернет – це всього лише вершина світової інформаційної конструкції, вершина айсберга, що водночас є і джерелом інформації, і джерелом проблем, про які Ви можете і не знайти, проте велика ймовірність, що вони знайдуть Вас самі.

Тобто, головна та першочергова мета інформаційної війни – поширити інформаційні потоки супротивника та замінити повністю або частково своїми, зробивши користувачів, що цю інформацію споживають, своїми «клієнтами», після чого продовжувати їх «оброблювати» доти, доки не буде досягнений необхідний результат.

Наслідками ж інформаційної війни можна назвати почуття постійної тривожності, як мінімум, і небезпеки як максимум, адже ти не знаєш напевне чи правдиву інформацію ти читаєш, чи дійсно твоя думка сформована тобою, чи її за тебе чемно та обережно сформулювали, після чого ти став її безпосереднім носієм.

Інформаційна війна нині є так званою неоголошуваною війною, війною, яка може точитись десятиліттями, руйнуючи той чи інший сегмент інформаційного простору не лише окремої держави, а й світового соціуму.

Інформаційна війна в наш час стала лише вісником війни справжньої, жорстокої та кровопролитної, якій передувала гібридна війна, де стали задіяними як методи «старої» так і «нової» школи. Людство зіткнулось з новим до цього не баченим явищем – війною, яку не видно неозброєним оком, і нам ще потрібно буде як слід вивчити всі можливі розв'язки, всі можливі арени бойових дій, на яких можна влаштувати і свою інформаційно виставу, адже наше століття – століття розвитку, століття інформації, століття змін…

Список використаних джерел:

1. Проноза І. І. ІНФОРМАЦІЙНА ВІЙНА: СУТНІСТЬ ТА ОСОБЛИВОСТІ ПРОЯВУ [Електронний ресурс]– Режим доступу до ресурсу: http://app.nuoua.od.ua/archive/61_2018/9.pdf.

2. Власюк В. В. ДЕЯКІ ОСНОВИ ПОНЯТТЯ "ГІБРИДНА ВІЙНА" В МІЖНАРОДНОМУ ПРАВІ [Електронний ресурс] – Режим доступу до ресурсу: http://lcslaw.knu.ua/index.php/item/207-deyaki-osnovy-ponyattya-hibrydna-viyna-v-mizhnarodnomu-pravi-vlasiuk-v-v-karman-ya-v.

Vasilieva V. Yu.,

Applicant for the degree of "bachelor"

Specialty "Cybersecurity", 2 course, 9 group

Faculty of Information Technologies

State University of Trade and Economics

Kyiv, Ukraine

INFORMATION WARS AS A MODERN PHENOMENON

Abstract: The article addresses the issues of information warfare, focusing on informational and psychological operations. What is the information war, when does it appear, and its causes?

Keywords: information war, information influence, counteraction

Problem statement: studying the question of what is information warfare, its development and its causes.

Purpose: there is an analysis of the manifestations of information warfare as a modern global phenomenon.

The term "Information War" means: "measures taken to gain an informational advantage over the enemy by taking means to influence his information, processes based on information processing and computer networks while protecting their information, processes based on information processing, information systems and computer networks ".

The experience of recent armed conflicts shows that one of the most important mechanisms of war is not only changes in military affairs, but also the information revolution, which is now undergoing a stage of formation.

The first operational information warfare experience, as one of the complex military confrontations, was initiated in the 1991 Gulf War. The success of the use

of information weapons not only encouraged the United States to understand the role of the information struggle, but also set an example to other nations of how to use and conduct it [1].

An example of its large-scale use is the information war waged by Russia against Ukraine.

Psychological influence on the opponent is an ancient mechanism of influence on the opponent.

Manipulation of people's consciousness as a form of influencing them to control them has been and remains an effective means of political and legal struggle. This kind of power potential has been used since ancient times.

The spread of information warfare in recent times intensified during the Cold War. It included two levels of "combat": visible and invisible. The obvious way to use tools that may not have been visible to the general public, but everyone knew about them. These include intelligence, international confrontation and, ultimately, ideological confrontation. Implicit - was the use of information and psychological technology to influence the mass consciousness, it performed the function of supporting the main, to some extent, official actions.

False information is the basis of such a war. Quite often, under the guise of a great goal - patriotism, protection of indigenous peoples, protection of human rights and freedoms, the fight against terrorism, etc., there is military aggression.

The annexation of Crimea and the military conflict in the East of our state are a consequence of the purposeful influence of the information war. According to official data, there have been 5,000 cases of Russian disinformation since 2015, of which about 2,000 concerned Ukraine.

Modern scholars point out that information warfare is a term that has two meanings: first, the impact on the civilian population and/or the military of another state by disseminating certain information.

From a military point of view, war is traditionally about destroying or weakening the enemy's physical resources. Instead, the aim of information warfare in military terms would be to attack the enemy's resources and infrastructure, a so-called «soft attack» that does not produce immediate results and is not always visible.

The information war has become one of the most dangerous weapons today. Using compromising material, pouring dirt, throwing false information and trying to mislead with the help of information have become the meaning of life for many.

Information has an impact on the masses. With the successful manipulation of the masses' consciousness, it is possible to achieve almost any goal: to destroy the opponent, remove competitors from the road or start a war[2].

Against the background of recent events in Ukraine, it is clear that the main struggle between political forces is through information.

The American researcher McLuhan said an interesting thesis: "A truly total war is a war with the help of information."

The purpose of information warfare is to weaken the moral and material forces of the enemy and to strengthen one's own. It provides for measures of propaganda influence on human consciousness in the ideological and emotional spheres.

Information warfare considers information as a separate object or as a potential weapon and a profitable target. Information warfare can be seen as a qualitatively new type of hostilities, active counteraction in the information space.

The main action of information weapons is the diversion or distortion of information flows and decision-making processes of the enemy.

Information wars are more often used at the international level. Ukraine and Russia have been waging such a war for more than a year. Russia constantly

provokes the Ukrainian government with loud statements and simply treats Ukrainians with contempt in its information materials[3].

The most important, in our opinion, are electronic and psychological wars. Electronic warfare is influenced by electronic means of communication - radio, television and computer networks.

Psychological warfare is carried out through propaganda, "brainwashing" and other methods of information processing of the population.

The topic of information weapons, information influence on society and the formation of ideological personalities in various spheres of his life is not new, because many researchers have revealed the basic mechanisms of information influences. However, they are constantly improving in various directions, and due to this, there are many new and unaccounted aspects, the study of which aims to identify them, further development, structuring and dissemination in society.

Information influence is the dissemination of certain ideas, views or ideologies as a means of a certain policy, its main tool is the media information (media) and various communications.

Information influence or propaganda is defined as purposeful, systematic attempts to form perceptions, to manipulate consciousness.

Although influence began its history with the beginning of the history of society, the first scientific school to specifically study the problem of informational influence was the American School of Media Studies. This school studied it primarily on the material of the First World War.

This school, in particular, identified three main types of information influences:

1. "White" influence. Its main characteristic is that the journalist openly calls himself and allows to connect the texts with the real source. A striking example of

such information is the statements of the president, the government, and the official news agency.

2. "Gray" influence. The journalist uses specially created sources to disseminate materials or promote certain materials in the independent media. An example of such "gray" information influence can be information disseminated through non-governmental media, non-governmental organizations, etc.

3. "Black" influence. The journalist distributes materials on behalf of a third party, such as an underground organization. The information war against Ukraine is aimed not only at shaking up the situation inside the country but also at creating a negative image of Ukraine in the world[3].

This process started in 2005 during the first gas war. At that time, Ukraine was successfully presented as a dishonest and at least dubious gas transit country, even though for decades Ukraine never allowed the disruption of natural gas supplies to Europe, which were (and continue to be)

- the gradual decline of Ukraine's international image to weaken its geopolitical significance;

- appropriate dosing and distortion of information to destabilize the situation in the country and implement its policy;

- formation of the stereotype of inferiority and

the secondary nature of Ukrainians, as well as the corresponding destruction of the feelings of the nation and the people;

- the dominance of the Russian language, culture and traditions to establish self-identification while displacing the Ukrainian language and culture.

The second part of the great information war came when the war broke out in 2014. And conditionally the third began on February 24, 2022, when Russia began to wipe out various cities of Ukraine. Each new video conference of the president of the enemy consists of 99 percent propaganda and brazen lies. Every day, the

inhabitants of the enemy amaze us even more with how sincerely they believe that there is no war, as they say, that Ukrainians deserve to die during rocket fire.

Thus, an incredibly powerful information war is being waged against Ukraine, but the Ukrainian authorities never carry out counter-offensive actions but are limited to defense. In addition, it is necessary to develop a strategy and tactics of struggle in the information field and to create a structure that will analyze and collect the necessary information for the struggle.

- formation of the stereotype of inferiority and the secondary nature of Ukrainians, as well as the corresponding destruction of the feelings of the nation and the people;
- the dominance of the Russian language, culture and traditions to establish self-identification while displacing the Ukrainian language and culture.

The second part of the great information war came when the war broke out in 2014. And conditionally the third began on February 24, 2022, when Russia began to wipe out various cities of Ukraine. Each new video conference of the president of the enemy consists of 99 percent propaganda and brazen lies. Every day, the inhabitants of the enemy amaze us even more with how sincerely they believe that there is no war, as they say that Ukrainians deserve to die during rocket fire.

Thus, an incredibly powerful information war is being waged against Ukraine, but the Ukrainian authorities never carry out counter-offensive actions but are limited to defense. In addition, it is necessary to develop a strategy and tactics of struggle in the information field and to create a structure that will analyze and collect the necessary information for the struggle [2].

Conclusion: Information wars are a special challenge for the modern value system. Manipulation of information through the psychological impact on the opponent has historically been a means of warfare.

Technological progress and globalization have affected not only the dynamics of international relations but also the information space. The latter, in the

end, becomes another factor that affects different levels of human and interstate relations. Thanks to the global media, billions of people around the world can receive accurate information, and the main barrier is, first of all, knowledge of a foreign language and time.

However, in such circumstances, new opportunities for manipulation and misinformation appear. Strong and rich states or transnational corporations, which have the appropriate tools and technological base, can implement their policies more effectively and influence weaker players. These processes are characterized by secrecy and covert activity, which, in the end, are planned and distributed over time. This complicates effective protection against such actions, which, in the end - purposefully, can be weakened through informational and psychological operations. Lack of public awareness of information warfare will also be one of its fundamental goals. Particularly high risk of feeling the impact of such measures is characteristic of the media, their employees and owners.

References:

1. Information war: essence, means of realization, results and possibilities of counteraction [Electronic resource] // URL: https://core.ac.uk/download/pdf/268616704.pdf. - 2022.
2. Information war: essence, means of realization, results and possibilities of counteraction [Electronic resource] // URL: https://core.ac.uk/download/pdf/268616704.pdf. - 2022.
3. Information war, information and psychological operations: concepts, methods and applications [Electronic resource] // URL: https://capd.pl/images/dokumenty/04UA_Lelonek.pdf.

Волосацький О. О.,
Здобувач освітнього ступеня «бакалавр» спеціальності
«Кібербезпека»
факультету інформаційних технологій 1 курсу 11 групи
Державний торговельно-економічний університет
м. Київ, Україна

ЯК БОРОТИСЯ З ДЕЗІНФОРМАЦІЄЮ В СОЦІАЛЬНИХ МЕРЕЖАХ?

Анотація: Досліджено методи захисту соціальних мереж від поширення дезінформації. Виявлено стратегії, які допоможуть захистити себе від неправдивої інформації та фейків. Доведено, що дотримуючись певних правил можна захистити соціальні мережі від дезінформації.

Ключові слова: дезінформація, боротьба з дезінформацією, фейк, соціальні мережі.

В умовах війни РФ проти нашої держави українці стикаються з дезінформацією, інформаційними атаками, зламом аккаунтів.

Зараз у соцмережах і медіа багато фейків та дезінформації. Усе це вороги роблять для того, щоб українці втратили віру в перемогу й опустили руки. Тож потрібно будь-яким чином захистити себе від дезінформації, особливо в соціальних мережах. Це можна зробити самостійно. Ось стратегії, які ви можете використати на найпопулярніших платформах, таких, як Facebook, Twitter, Youtube та Instagram.

1. Facebook

У Facebook вашим першим кроком може бути вибірковість того, за ким ви стежите. На новини, які заповнюють вашу стрічку Facebook, впливають користувачі, за якими ви стежите. Якщо ви стежите за користувачами чи

групами, які поширюють дезінформацію, шанси вищі, що публікації у вашій стрічці також будуть неточними та оманливими.

Варто стежити за авторитетними джерелами новин і тими, хто надає достовірну інформацію, яка може бути підкріплена перевіреною статистикою, інтерв'ю та дослідженнями. Якщо ви це зробите, ваша стрічка новин включатиме інші надійні джерела, засновані на фактах.

Ви також можете скасувати підписку або заблокувати користувачів, якщо вважаєте, що вони часто діляться фейковими новинами або дезінформацією. Якщо ви бажаєте зробити більш проміжний крок, ви можете приховати пости людей та організацій, які часто надсилають фейкову інформацію.

Ви можете розглянути можливість вивчення опції «Чому я бачу це» у Facebook. Натиснувши на це, ви отримаєте інформацію про те, чому в стрічці з'явився певний пост. Наприклад, ви можете бути в онлайн-групі, яка часто публікує інформацію, що вводить в оману. Ви можете виявити, що часто коментуєте певний обліковий запис. Якщо це робити, це збільшить ймовірність того, що у вашій стрічці з'являться публікації з цього облікового запису, навіть якщо ці дописи містять недостовірну інформацію.

2. Twitter

Twitter схожий на Facebook тим, що інформація, яку ви бачите у своїй хронології Twitter, багато в чому залежить від того, за ким стежите. Якщо стежити за джерелами, які регулярно публікують дезінформацію або неправдиві новини, ваша хронологія, швидше за все, буде заповнена такого роду спотвореною інформацією або фейками.

Ось чому розумно бути вибірковим, вибираючи, за ким стежити в Twitter. Ви потенційно можете підвищити свої шанси стежити за законними джерелами новин, використовуючи функцію Списків Twitter. Списки - це кураторські групи облікових записів Twitter, за якими ви можете стежити.

Список, наприклад, може включати лише відомі новинні сайти або надійні журналістські організації. Якщо ви будете дотримуватися таких Списків, ви, швидше за все, зменшите кількість дезінформації у вашій хронології.

Ви також можете звернутися до розділу "Теми" Twitter. Ця функція дозволяє слідувати певним темам. Наприклад, ви можете стежити за новинами війни в Україні чи конкретно в регіоні, в якому проживаєте.

3. YouTube

YouTube став ключовим джерелом новин для багатьох. Це робить YouTube мішенню для тих, хто сподівається поширювати фейкові новини. Ось чому YouTube зробив кілька кроків, щоб обмежити поширення дезінформації зі свого сайту.

YouTube повідомляє, що з початку 2019 року запустив понад 30 змін, покликаних зменшити дезінформацію.

Що це за зміни? YouTube тепер більш активно просуває авторитетний контент у своїй панелі "Дивитися далі", коли люди дивляться прикордонний контент. Це також звело рекомендації до такого роду прикордонного змісту.

Надія полягає в тому, що глядачі, які дивляться сумнівний контент, натиснуть на рекомендоване відео з законного джерела новин після перегляду сумнівного контенту, потенційно протидіючи деякій інформації, що вводить в оману, яку щойно переглянули ці глядачі. Також можна скаржитися на канали, які займаються поширенням дезінформації. Це один із найбільш дієвих методів блокування Instagram фейкових новин на цій платформі.

4. Instagram

Завдяки своїй популярності Instagram теж став мішенню для аферистів, «зомбі» та тих, хто свідомо вирішив поширювати дезінформацію. Facebook, якому належить Instagram, заявив, що найняв сторонніх фактчекерів для

перевірки на наявність неправдивої інформації. Facebook заявляє, що працює з 45 сторонніми фактчекерами по всьому світу. Ці шашки сертифіковані через Міжнародну мережу фактчекінгу, безпартійну групу.

Коли ці фактчекери знаходять підроблену або неповну інформацію, вони ускладнюють користувачам пошук, фільтруючи її з Explore і Хештегів. Instagram також зменшує видимість цієї інформації в стрічці та історіях Instagram.

Якщо Instagram позначає публікацію як неправдиву інформацію, є два варіанти: можна натиснути опцію «Побачити чому», щоб прочитати, чому фактчекери визначили публікацію як фейкові новини, або ви можете натиснути «Побачити публікацію», щоб переглянути інформацію в будь-якому випадку.

Є кілька порад, які допоможуть користувачам виявити неправдиву інформацію. Шахраї часто використовують у своїх заголовках великі літери і закінчують їх кількома знаками оклику. Як каже Instagram, якщо інформація в заголовку здається неймовірною, це, ймовірно, фейк.

Instagram також рекомендує, щоб ви завжди досліджували джерело публікації. Якщо ви впізнаєте джерело - можливо, аккаунти служб новин, офіційних людей, наприклад, президента України, або інший авторитетний постачальник новин – можна бути певним у достовірності поданої інформації.

Але якщо інформація надходить з джерела, якого ви ніколи раніше не бачили, потрібно подумати про те, щоб бути більш скептичними, читаючи таку інформацію.

Також стежте за орфографічними помилками, неправильною граматикою або незручними макетами. Це можуть бути ознаки недостовірної інформації.

Також будьте напоготові до сатири. Як пише Instagram, фейкові новини часто надходять з пародійних акаунтів, таких як The Onion. Ці історії є сатирою і не призначені для того, щоб їх сприймали як істинні. Якщо ви прочитали в Instagram щось абсолютно шокуюче, переконайтеся, що інформація надходить не з пародійних сайтів.

Висновки: Платформи соціальних мереж є все більш важливим способом для людей отримувати інформацію та спілкуватися з друзями та членами сім'ї. Але оскільки такі сайти, як Facebook, Twitter, YouTube та Instagram, настільки популярні, їх часто використовують ті, хто бажає поширювати дезінформацію, фейки чи залякування.

Незалежно від того, який сайт у соціальних мережах ви використовуєте, добре читати вміст з критичним розумом. Щось, що звучить неймовірно шокуюче, може бути прикладом дезінформації. Ви повинні перевірити інформацію, яку ви бачите, досліджуючи її джерело та перевіряючи її факти в Інтернеті.

Список використаних джерел:

1. Інформаційна війна – зброя масового знищення! [Електронний ресурс] - Режим доступу до джерела: https://www.pravda.com.ua/rus/articles/2006/04/20/4399050/

2. Інформаційні війни: тенденції та шляхи розвитку. [Електронний ресурс] – Режим доступу до джерела: https://ms.detector.media/manipulyatsii/post/6479/2012-08-12-informatsiini-viinitendentsii-ta-shlyakhi-rozvitku/

3. Російсько-українська інформаційна війна. [Електронний ресурс] - Режим доступу до джерела: https://www.radiosvoboda.org/a/informatsiyna-viyna-rosiyskyy-vplyv/31811302.html

Засадюк А.В.,
здобувач освітнього ступеня «бакалавр» спеціальності
«Цифрова економіка»
факультету інформаційних технологій 1 курсу 1 групи
Державний торговельно-економічний університет
м. Київ, Україна

ІНФОРМАЦІЙНА ГІГІЄНА

В нашій країні розпочалась війна і багато людей через це пішло на фронт. Деякі люди, що розуміються в комп'ютерах, а не в тому, як воювати в реальному житті, почали власну війну – інформаційну, яка є не менш важливою, ніж бої на відкритому просторі в реальному житті.

Інформаційна війна – вплив на населення іншої країни через розповсюдження певної інформації та захист громадян своєї країни від такого впливу. Головними об'єктами протистояння у ході такої війни є інформаційний простір, ресурси та тех. системи упр., навігації, комп'ютерні мережі, радіоелектронні засоби і пристрої та інше.

Усі великі збройні конфлікти кін. 20 – поч. 21 ст. (війни в Іраку 1991 і 2003, військ. операція НАТО проти Югославії 1999, грузино-російський конфлікт 2008, повалення повстанцями (за допомогою країн НАТО) режиму М. Каддафі в Лівії 2011 та ін.) супроводжувалися масованими інформаційними атаками. Чим сучасніша країна, тим більше вона покладається на інформацію і засоби її доставляння, а тому й уразливіше в інформаційних війнах. [1]

Так, новини, які дивляться всі, не завжди кажуть всю правду чи іноді можуть навіть збрехати, і за це не слід забувати, але таке - не зовсім інформаційна війна. Наразі, коли в нас війна з іншою країною, крім того, що використовується зброя, одночасно з тим українці попадають під вплив інформаційних війн. Інша країна намагається нас дезінформувати і сіяти

паніку , щоб зламати нас морально, але наші інформаційні воїни ламають їх плани.

В умовах сьогодення слід дотримуватись інформаційної гігієни. Під час війни надзвичайно важливо дотримуватись правил інформаційної гігієни, щоб не дати себе ошукати та вберегти психічне (а часом і фізичне) здоров'я. Де шукати правду, як відрізнити пропаганду та перевірити те, що транслюють ЗМІ й блогери.

В цей час в кожного вдома можна знайти якісь гаджети типу телефона, планшета чи ноутбука, так як на дворі 21 століття і це час інформаційних технологій. З одного боку, таким чином багато людей може постраждати від неправдивої інформації, але з іншого – всі ми можемо долучитися до інформаційної війни, спростовувати неправдиву інформацію і, можливо, навіть доносити правду країні, з якою йде війна, як і роблять навіть деякі наші студенти.

Щоб було менше шансів стати жертвою інформаційної війни, є деякі інтернет-ресурси, цінні в умовах нашого часу і положення:

- АБВ. Збройний конфлікт в термінах (Путівник для України)
- Порядок акредитації журналістів в зоні АТО
- Український державний центр радіочастот
- CERT-UA (Computer Emergency Response Team of Ukraine – команда реагування на комп'ютерні надзвичайні події України)
- Державна служба спеціального зв'язку та захисту інформації України.
- Dokaz
- Bellingcat Ukraine Conflict Vehicle Tracking Project
- Лікбез
- Стоптеррор
- Національний військово-історичний музей України

- Напрямки роботи проросійської пропаганди в Україні.
- Як працюють проросійські блогери
- Інформаційні акценти нової військової доктрини Кремля
- Кремлівська експансія у світовому інфопросторі [2]

Перш, ніж вірити будь-якій інформації слід її перевірити в достовірних ресурсах.

Три базові правила інформаційної гігієни:

- Перевіряйте інформацію.
- Не допомагайте ворогу.
- Дбайте про свою безпеку в соцмережах.

І як висновок, не робіть того, чого від кожного з нас чекає ворог.

Список використаних джерел:

1. Інформаційна війна. *Енциклопедія Сучасної України*. URL: https://esu.com.ua/search_articles.php?id=12460 (дата звернення: 24.03.2022).

2. Інформаційна війна. *Міністерство інформаційної політики України*. URL: https://mkip.gov.ua/content/informaciyna-viyna.html (дата звернення: 24.03.2022).

Івасенко К.І.,

здобувач освітнього ступеня «бакалавр» спеціальності

«Цифрова економіка»

факультету інформаційних технологій 1 курсу 1 групи

Державний торговельно - економічний університет

м. Київ, Україна

ІНФОРМАЦІЙНА ВІЙНА ЯК СУЧАСНА ГЛОБАЛЬНА ПРОБЛЕМА

Анотація: Питання інформаційної війни вийшло на новий рівень в XXI столітті завдяки інформаційним технологіям. З кожним роком її вплив охоплює більшу кількість населення. Маніпулювання свідомістю людей як форма впливу на них з метою їх контролю була і залишається ефективним засобом політико-правової боротьби.

Ключові слова: інформаційна війна, інформаційні технології, пропаганда, фейк, дезінформація, наратив, конфлікт.

Весь світ увійшов у цифровий простір, де розвиток технологій відбувається постійно. Інформаційні технології поступово увірвались у наше життя і ми вже навіть не уявляємо як жити без них. Сьогодні світ стоїть на так званому «історичному роздоріжжі», коли інформаційні технології несуть не лише користь, а й шкоду. У публічному просторі часто можна зустріти такі терміни, як: «інформаційна війна», «дезінформація» та «фейк». В епоху інформатизації суспільства все частіше постає відкрите питання інформаційних війн. Сучасні науковці вказують, що інформаційна війна – термін, що означає вплив на цивільне населення і / або військовослужбовців іншої держави шляхом поширення певної інформації. [1] Інформаційна війна являє собою сферу, яка швидко розвивається і викликає зростаючий інтерес для планувальників оборони та політиків. Війна залишається вічною проблемою людства, незалежно від поля бою,

зброї чи захисту. Зміна підходу до традиційних дій у збройних конфліктах полягає у введенні нових чи нетрадиційних заходах для спрямованого впливу на цільову аудиторію. Засоби інформаційної війни можуть використовуватися як в умовах прямого збройного конфлікту, так і за його відсутності, зокрема, завдяки тому, що заходи і методи інформаційної війни не потребують прямого контакту протиборчих сил.

Ведення війни в інформаційному просторі дуже відрізняється від самого поняття «війна», бо зазвичай інформаційні війни ніхто не оголошує, і взагалі ці війни можуть бути непомітними Придушення волі людей і програмування патернів їхньої поведінки пов'язують з поняттями «маніпуляція громадською думкою» / «маніпуляція масовою свідомістю», що дуже близькі за своєю суттю поняттю «інформаційна війна». Однією з таких інформаційних війн є непроголошена Україні війна від російської федерації. Остання має значний досвід у пропагуванні та ефективному маніпулюванні громадян народних республік. У 2022 році американська організація NewsGuard виявила та відстежила більше 20 інтернет-доменів (деякі з відверто державною формою власністю, такі як RT, Sputnik і ТАСС), які просувають фейковий контент на основні платформи соціальних мереж. [2] NewsGuard у своєму останньому аналізі повідомляє, що ця російська дезінформаційна система поширює 10 найпопулярніших російсько-українських «військових міфів»:

- «Російськомовні люди Донбасу в Україні зазнали геноциду».
- «Польськомовні диверсанти намагалися бомбити хлорний завод на Донбасі».
- «Українські війська обстріляли дитячий садок у Луганську на сході України 17 лютого 2022року».
- «росія не націлена на руйнування цивільної інфраструктури в Україні на початку вторгнення».

- «Нацизм поширюється в українській політиці та суспільстві, підтримується владою Києва».
- «Захід організував державний переворот для повалення проросійської української влади у 2014 році».
- «Сполучені Штати мають мережу лабораторій біологічної зброї у Східній Європі».
- «НАТО має військову базу в Одесі на півдні України».
- «Крим юридично приєднався до росії».
- «Сучасна Україна була цілком створена комуністичною росією». [3]

Є, звичайно, конкретні докази того, що всі ці фейкові новини чи антиукраїнські наративи є неправдивими: свідки, записи, дані та джерела українських та міжнародних ЗМІ. Попри такі підтвердження проросійські новини не перестають поширюватися по всьому світу та вводити людей в інформаційну оману.

Правдиве відображення російсько-української війни можна скласти, узагальнивши інформацію, надану урядом та адміністрацією України, а також ЗМІ. Інформація, яку надає американська розвідка CIA, іноді суттєво відрізняється від української, наприклад, щодо кількості загиблих російських солдатів. Оголошення їх кількості має на меті інформування населення України щодо втрат ворога і вплив на моральний дух українських військових. Також такі дії з боку українського уряду спрямовані на психологічну підтримку громадян, які виснажені війною, та надання населенню України морального зміцнення духу для того, щоб довго переслідувати мету і були сили витримати військову та інформаційну війну. Сконструйований наратив про безглуздість і безрезультатність російських військ (навіть якщо це підтверджується фактами) та інформація про великі успіхи українських військ мають впливати на психіку українців і підтримувати їх високий моральний дух, мотивацію та віру в успіх. Через

російсько-український конфлікт варто згадати інформаційну війну проти росії з боку Америки. Central Intelligence Agency неодноразово заздалегідь надавали розвідувальні відомості про переміщення російських військ на території України. Такі дії розвідки США мають на меті принизити наміри та елемент несподіванки з боку росіян, а також створити плутанину та примусово своїми діями змінити події в світі. Науковці, які вивчають еволюцію російських інформаційних операцій, зазвичай стверджують, що вони є спадщиною радянського стратегічного мислення та пропагандистської практики. На рис.1 представлено всі витрати, які використала росія у 2014 році.

Рис.1.Витрати на пропаганду росії у 2014 [4]

Віра про потенціал інформаційної технології до демократії, яка протиставляє авторитарну цензуру демократичній відкритості, не визнає, що всі держави, незалежно від типу режиму, прагнуть здійснювати інформаційний суверенітет, керуючи розповсюдженням інформації в межах своїх кордонів. Наприклад, Велика Британія та Сполучені Штати намагалися видалити з Інтернету контент, створений ІДІЛ. [5] Водночас порушення інформаційного суверенітету суперників у мирний та воєнний час є елементом міждержавної конкуренції.

Спроби захистити або порушити інформаційний суверенітет – бажання зберегти інформаційний суверенітет, що підтверджувало звинувачення Сполучених Штатів у тому, що росія намагалася маніпулювати дискусіями в соціальних мережах у США, пропагуючи фейкові новини та теорії змови. Тому, хоча просування цифрової демократії має схвальну мету, той факт, що вона ґрунтується на порушенні інформаційного суверенітету цільових держав, означає, що вона буде сприйматися як загроза.

Рис. 2. Система пропаганди росії [6]

Зусилля росії з дезінформації на Близькому Сході (рис.2) почались з арабомовною аудиторією у травні 2007 року, запустивши RT Arabic. По-перше, «арабська весна» та роль, яку відіграли соціальні медіа у потрясіннях, змусили росію зрозуміти, що близькосхідний інформаційний простір надає пропагандистській росії широкі можливості для просування своїх стратегічних наративів. По-друге, військове втручання росії в Сирію ознаменувало повернення росії в регіон і, таким чином, змусило створити місцеву пропагандистську групу. В результаті російські та сирійські ЗМІ розвинули міцні зв’язки, що сприяло співпраці шляхом обміну інформацією та досвідом. У 2016 році Sham FM і Sputnik, дві найпопулярніші радіостанції Сирії, об’єдналися , щоб запустити щоденне одногодинне радіо-шоу, яке розповідало про військові події в країні, а дії росії були відзначені для похвали. [7]

Оскільки роль соціальних медіа в регіоні зростав, кіберпростір Близького Сходу вабив Кремль розширити свій інформаційний вплив. Надмірна залежність від платформ соціальних мереж для отримання новин у країнах Близького Сходу дозволяє Москві охопити мільйони людей. RT і Sputnik Arabic створюють значно більше контенту в Twitter, ніж BBC Arabic або Al Jazeera. У той час як RT Arabic і Sputnik Arabic щодня публікують у середньому 180 і 87 твітів відповідно з моменту їх створення, Al Jazeera зберігає в середньому 55 твітів, а BBC Arabic – лише 32. Загалом RT і Sputnik підкреслюють, що США та їх європейські союзники відповідають за нестабільність на Близькому Сході, культивуючи імідж Москви як стабілізуючої сили. З огляду на обурення багатьох на Близькому Сході з приводу невдач Заходу в регіоні, ця розповідь, природно, резонує. [8] Дії росії відіграють значну роль у пропаганді фейків та розвитку інформаційних воєн. Незважаючи на опір населення, до якого застосовують різні методи інформаційної боротьби, пропаганда рф має активний агресивний вплив, що призводить до негативних наслідків.

Висновки: Незважаючи на те, що інформаційна війна стає все більш популярною серед лідерів багатьох країн, вона залишається неоднозначним і нечітким поняттям, яке використовується в різних контекстах. Велика частина дискусій навколо інформаційної війни зосереджена насамперед на засобах інформаційної війни (проблеми організації та ресурсів), у той час як сфера та значення інформаційної війни залишаються значною мірою невизначеними. Повсякденне спостереження за діяльністю російської держави та пов’язаних з нею злочинних суб’єктів демонструє, що вся російська держава бере участь у політичній війні та інформаційній війні. Наслідки глобальної війни дуже відчутні на психологічному рівні громадян країн, на яких направлена ця інформаційна війна.

Список використаних джерел:

1. Почепцов, Г.Г. Сучасні інформаційні війни/ Г.Г. Почепцов – К: Сінтег, 2015. – 180 с.
2. NewsGuard [Електронний ресурс] - Режим доступу до ресурсу: https://www.newsguardtech.com/misinformation-monitor/march-2022/
3. Russia-Ukraine Disinformation Tracking Center: 200+ Websites Spreading War Disinformation And The Top Myths They Publish [Електронний ресурс] - Режим доступу до ресурсу: https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/
4. Машина пропаганди Путіна. [Електронний ресурс] – Режим доступу: https://www.epravda.com.ua/publications/2014/04/1/433089/
5. Цензура онлайн-пропаганди ІДІЛ працює не дуже добре. [Електронний ресурс] - Режим доступу до ресурсу: https://www.washingtonpost.com/news/monkey cage/wp/2015/06/18/censoring-isiss-online-propaganda-isnt-working-out-very-well/
6. Машина пропаганди Путіна. [Електронний ресурс] – Режим доступу: https://www.epravda.com.ua/publications/2014/04/1/433089/
7. Цифровий Близький Схід: ще один фронт російської інформаційної війни. [Електронний ресурс] - Режим доступу: https://www.mei.edu/publications/digital-middle-east-another-front-russias-information-war
8. Росія на Близькому Сході: новий фронт інформаційної війни? [Електронний ресурс] – Режим доступу: https://jamestown.org/program/russia-middle-east-new-front-information/

Квятківська А. П.,

здобувач освітнього ступеня «бакалавр» спеціальності

«Цифрова економіка»

факультету інформаційних технологій 1 курсу 1 групи

Державний торговельно - економічний університет

м. Київ, Україна

НОВЕ ОБЛИЧЧЯ ВІЙНИ, ВИКЛИКИ ТА ПРОБЛЕМИ В УКРАЇНІ

Істинно тотальна війна
- це війна за допомогою
інформації
М.Маклюен

Анотація: Реалії сьогодення такі, що майже кожна війна на фронті супроводжується війною на інформаційному просторі. Інформаційні війни використовуються в прихованій ворожнечі, з метою послабити моральні і матеріальні сили супротивника та посилити власні. В Україні з 2014 року, рф веде інформаційну війну проти України, а з 24 лютого 2022 року інформаційна війна набула нових рис. Інформаційна війна на сьогодні є масштабною; агресор використовує засоби маскультури в окупованих територіях, значно збільшує аудіовізуальні засоби.

Ключові слова: інформаційна війна, кіберфронт, інформаційні технології, хакерські атаки.

З розвитком глобалізації, інформатизації та діджиталізації інформаційні війни стали потужною силою у боротьбі з ворогом.

Є різні праці та теорії щодо часу виникнення та розвитку інформаційних воєн. Одні науковці вважають, що інформаційні війни супроводжують всю історію людства. Спочатку вони були релігійними та

ідеологічніми, причому для боротьби з носіями чужих поглядів застосовувалися всі види репресій. [1]

Інші ж науковці вважають, що інформаційні війни виникли тоді, коли країни стали пов'язані не лише товарами, а й послугами, що забезпечили розвиток інформаційних технологій і здатність мати зв'язок з будь-якою країною світу [2]. Першою інформаційною війною вважають війну в Перській затоці 1991 р. (сторони США та Ірак). [3] У цій війні були використані такі засоби інформаційного впливу: 1) розповсюджувалися листівки з виправданнями дій США; листівки-дозволи для солдатів-дезертирів; листівки з попередженнями про бомбардування для залякування військ противника; 2) з'явилася ідеологема «США захищають демократію в усьому світі» (трансформація лозунгу Першої світової «США захищають свободу для всіх людей»); 3) використовувалися лжесвідки, які розповідали про "жорстокість" іракських солдатів; 4) робота журналістів була організована так, що американський глядач не бачив жорстоких сцен із театру воєнних дій.[4]

Інформаційна війна – це операція, яка проводиться з метою отримання інформаційної переваги над супротивником. Полягає в контролі власного інформаційного простору, захисту доступу до власної інформації, при отриманні та використанні інформації опонента, руйнуванні їх інформаційних систем та порушення інформаційного потоку. На відміну від тактичного ведення війни, інформаційні війни часто не розкривають мету, а діють на послаблення іншої сторони. [5]

Дж.Аркілла є чи не найпершим на сьогодні американським вченим із питань інформаційної війни, який сформулював такі три правила цієї боротьби:

- ієрархіям важко боротися з мережами,
- потрібні мережі, щоб воювати з мережами,

- той, хто освоїть першим мережеві форми, буде мати суттєві переваги . [6]

Як бачимо, розвиток технологій є важливою передумовою ведення інформаційної війни, а особливо, в сучасному світі, в період розвитку нанотехнологій, штучного інтелекту. Тому можна стверджувати, що перемога у інформаційній війні за більш розвиненою країною, де технології є пріоритетними від старих методів ієрархічної влади.

Провідний експерт з питань інформаційної війни Мартін Лібіцкі сформував концепцію інформаційної війни, що складається з наступних семи підобластей:

- Електронна війна (EW),
- війна на основі розвідки (IBW),
- Хакерська війна (HW),
- Командно-контрольна війна (C2W),
- Психологічна війна,
- Економічна,
- Інформаційна війна та кібервійна (Libicki). [2]

Не всі інформаційні війни включають в себе всі ці під-області, адже часто інформаційні війни є неоголошеними, ведуться приховано. Проте, якщо ми говоримо про повномасштабну відкриту війну, то часто сторони використовують всі під-області.

Світ швидко змінюється, і інформаційна війна відіграє велику роль, усвідомлюємо ми це чи ні, але ми стали її учасниками. Хакерські атаки на Україну здійснювалися з 2014 року, телеканали пропаганди працювали аж до санкцій. А з часу повномасштабного вторгнення російської федерації від 24 лютого 2022 на Україну було здійснено 240 атак – за даними Microsoft. [7]

Один із журналістів на брюсельській прес-конференції за підсумками косовської операції зауважив: «На війні, тим більше на інформаційній,

першою помирає правда». Це і формує ряд проблем та труднощів у веденні інформаційної війни. [8]

Оскільки в ході інформаційної війни здійснюється вплив на психологічну сферу людини, мас чи певних соціальних груп, — методи її ведення базуються на соціально-психологічних чинниках. Тому однією з проблем є захист населення, високий рівень розвитку психологічної допомоги. А особливо, це стосується тих територій, що перебували чи перебувають під окупацією. О. Зеленська ініціювала створення Національної програми психічного здоров'я та психосоціальної підтримки. Її мета – допомогти громадянам подолати надзвичайний стрес та наслідки травм, отриманих внаслідок війни, попередити розвиток психічних розладів. [9]

Ще однією значною проблемою наразі є формування єдиного фронту на чолі українських ЗМІ, єдина мета яких поширювати правду на весь світ про події на противагу пропаганді. Сьогодні журналісти виконують значну роботу, проте як зазначив Президент Володимир Зеленський у інтерв'ю українськими ЗМІ з нагоди Дня журналіста про те, що у нас недостатньо сформовані ті інструменти, що поширюють інформацію про війну далеко за кордонами нашими країнами, а особливо в тих країнах чи територіях, де звикли чути російське телебачення. Та й пам'ятаємо, що пропагандистська машина росії працює не перший рік, її коріння за межами їх кордонів. Лише після вторгнення 30 країн Європи повністю або частково вимкнули зі свого ефіру російські пропагандистські канали.[10] Тому боротьба за правду, висвітлення тих подій має поширюватися далеко за межі України. Вихід українських новин, програм, що ведуть хроніки війни допоможе сконсолідувати світ у боротьбі проти аргесора.

Ще варто зауважити про те, що ведення інформаційної війни також потребує фінансування, підтримання програмного забезпечення. Для того щоб продовжувати завдавати взломів інфраструктурних об'єктів та баз даних.

Четверта проблема, яка, можливо, виявиться пізніше: з початку війни ми спостерігаємо значний відтік робочої сили за кордон, студенти переводяться до іноземних ЗВО. Це може спричинити значний брак пропозиції робочої сили і у сфері ІТ в Україні, а значить і послаблення на кіберфронті. Понад 6 млн українців з початку війни виїхало за кордон, а за даними журналістів серед ІТ-фахівців виїзду за кордон, то туди переїхали 14% опитаних. Більшість із них – у Польщі (35% із тих, хто виїхав за кордон). Наступна за популярністю – Німеччина (10%)

Втім, ми маємо значну перевагу, на нашому фронті діють і інші країни. Велику частку у інформаційній війні проти росії займає США. Введення санкцій обмежують ряд послуг для громадян рф щодо доступу Міжнародного контенту та послуг. [11]

Оскільки, інформаційна війна стала масштабнішою, усі вищеперераховані сім областей широко використовуються ворогом, ми ніяк не можемо її уникнути, а тому ми маємо сприяти перемозі України на всіх фронтах. Україна в сучасних умовах задля ефективнішої боротьби з ворогом, повинна продовжувати покращувати ефективність інформаційної зброї (сукупність спеціалізованих (фізичних, інформаційних, програмних, радіоелектронних) методів і засобів тимчасового або безповоротного виводу з ладу функцій або служб інформаційної інфраструктури в цілому або окремих її елементів). Так ми формуємо сильний кіберфронт у протистоянні з ворогом, будуємо механізм розповсюдження правди про злочини окупантів, що допомагає нам здобути перемогу.

Висновки: Отож, інформаційна війна поряд з повномасштабним вторгненням є новим викликом для українців та всього світу. Ворог діє на багатьох областях, в тому числі і підобластях інформаційної війни. Ми маємо протистояти значним тискам, зокрема, хакерським атакам, психологічному тиску, пропаганді і іншим засобам інформаційної війни. Деякі проблеми ще потребують законодавчого рівня, інші потребують ресурсів, а в окупованих

територіях – доступу. Основними проблемами, окресленими в ці статті: захист і психологічна допомога жителям в окупованих територіях, формування єдиного фронту уряд-ЗМІ, брак фінансів, відтік ІТ-фахівців.

Список використаних джерел:

1. Інформаційна політика [Електронний ресурс] – Режим до ресурсу: http://enpuir.npu.edu.ua/bitstream/handle/123456789/25591/Zhadko%2064-95.pdf?sequence=1
2. Інформаційне протиборство у зовнішній політиці США [Електронний ресурс] – Режим до ресурсу: http://journals.iir.kiev.ua/index.php/apmv/article/viewFile/223/199
3. Information war is at its peak in the Ukraine conflict [Електронний ресурс] – Режим доступу до ресурсу: https://www.sundayguardianlive.com/news/information-war-peak-ukraine-conflict
4. Strategic Information Warfare [Електронний ресурс] – Режим доступу до ресурсу: https://www.rand.org/pubs/monograph_reports/MR661.htm
5. Психологічна допомога має бути першим кроком до відновлення постраждалих від війни [Електронний ресурс] – Режим доступу до ресурсу: https://www.rv.gov.ua/news/psihologichna-dopomoga-maye-buti-pershim-krokom-do-vidnovlennya-mentalnogo-dobrobutu-postrazhdalih-vid-vijni.
6. Закриття пропагандистських товарів [Електронний ресурс] – Режим доступу до ресурсу: https://www.ukrinform.ua/rubric-world/3442308-vze-30-krain-evropi-povnistu-abo-castkovo-vimknuli-rosijski-propagandistski-kanali.html
7. New UK centre will help fight information war [Електронний ресурс] – Режим доступу до ресурсу: https://www.bbc.com/news/technology-61718097

Корчага Т.А.,
здобувач освітнього ступеня «бакалавр»
спеціальності "Комп'ютерні науки"
Факультету інформаційних технологій
Науковий керівник: ***Величко О.Д.,***
кафедра цифрової економіки та системного аналізу
Державний торговельно-економічний університет
м. Київ, Україна

ІНФОРМАЦІЙНІ ВІЙНИ ЯК ЗАСІБ ВПЛИВУ НА ЛЮДСТВО

Анотація: Досліджено особливості, мотиви та прийоми ведення інформаційних війн на сучасному етапі. Розкрито можливі контрзаходи протидії ворогам, а також розглянуті стратегії, шляхи ведення інформаційного протиборства. Доведено, що інформаційна війна не менш руйнівна, бо торкається свідомості та психології людини, і як наслідок, може формувати хибне сприйняття реальності.

Ключові слова: Збір інформації, інформаційна війна, інформаційна атака, соціальні мережі, фейкова інформація, криптографія, мережа, захист даних.

Постановка проблеми. В сучасному суспільстві інформаційні війни виступають засобом для досягнення стратегічних цілей, в першу чергу через стрімкий розвиток інформаційних технологій, що впливає на масштаб аудиторії розповсюдження та швидкість поширення. Засоби інформаційного впливу стають доступними все більшому колу людей через мережу Інтернет, провідні ЗМІ, радіо, телебачення та інше. Інформаційна війна не менш руйнівна, бо торкається свідомості та психології людини, і як наслідок, формує хибне сприйняття реальності. Проблематика, пов'язана з інформаційними війнами - це дослідити, у тому числі на основі наукових публікацій, сучасні

методи та засоби ведення інформаційних війн, що є необхідним разом з розумінням мотивів та цілей ведення таких війн та розглянути засоби захисту та протидії.

Аналіз останніх досліджень та публікацій. В [1] автор перш за все досліджує представлені різними дослідниками значення сутності поняття "інформаційна війна" та висловлює думку щодо складності терміну: "На сьогодні поняття "інформаційна війна" визначається по-різному. Це пов’язано з багатозначністю терміну "information warfare", що породило безліч різночитань при його перекладах. Зазначене поняття може трактуватися як "інформаційна війна", "інформаційне протиборство", "інформаційно - психологічна війна" ".

Висновок, що випливає з аналізу різноманітних визначень терміну - це складність предмету дослідження й акцептування уваги на певних аспектах, зокрема: "на соціально-комунікативному аспекті інформаційних воєн", згідно якого "інформаційна війна представляє собою комунікативну технологію, котра має на меті досягнення інформаційної переваги в інтересах національної стратегії". В роботі [2] автор висловлюється щодо реагування на пост - правду: "ми повинні визнати цей так званий інформаційний розлад як невідкладну суспільну кризу і провести ретельне міждисциплінарне наукове дослідження для боротьби з цією проблемою."

Результати дослідження. Враховуючи дослідження, що проведені автором [1], найбільш вдале визначення поняття "інформаційна війна" з точки зору суспільного значення, описане в [3]: "Інформаційна війна(ІВ) – вплив на населення іншої країни у мирний або військовий час через розповсюдження певної інформації та захист громадян власної країни від такого впливу".

Таким чином, основні завдання ІВ з точки зору впливу на свідомість: необхідний вплив на ворога та захист власних громадян.

Інший аспект ІВ позначений в роботі [4]:

"Інформаційна війна розглядає інформацію як окремий об’єкт або як потенційну зброю та вигідну ціль. Інформаційну війну можна розглядати як якісно новий вид бойових дій, активна протидія в інформаційному просторі. Інформаційна війна – це атака інформаційної функції, незалежно від засобів, які застосовуються".

Важливам на сучасному етапі є використання ІТ технологій, що значно впливають на канали розповсюдження, зберігання, обробки та донесення інформації до населення. Канадська авторка, що спеціалізується на вивченні війн сказала, " що засоби інформаційного впливу змінюються разом із технологічним прогресом, а також про соціальні мережі як нову зброю в інформаційній війні."[5]

Інформацію стосовно ІВ слід розглядати й в контексті ІТ як інформаційну перевагу, що особливо важливо для військових дій як "здатність збирати, обробляти та поширювати інформацію ефективніше або ефективніше, ніж супротивник."[6]

Існує багато прийомів ведення інформаційних війн.

- Збір інформації – один з них, оскільки "той, хто володіє інформацією - володіє світом";

Ідея полягає в тому, що чим більше інформації, тим вище обізнаність щодо ситуації, що веде до кращих результатів у використанні інформації з певною ціллю, у тому числі проти пропаганди та маніпулювання для захисту та протилежне зі сторони ворога (соціально-комунікативний аспект).

Технології точного визначення місцезнаходження, такі як навігація на основі глобальної системи позиціонування (GPS), значною мірою полегшили проблеми знання позиції противника та стали певною мірою можливі завдяки застосуванню технологій розвідки та спостереження(військовий аспект використання новітніх технологій).

Такі технології, що могли надати достовірні факти перебування ворога, точний час нападу - є технологіями захисту від дезінформації про перебування.

- Інформаційний транспорт.

Збір великої кількості вичерпної інформації, безумовно, є хорошою практикою, але він не має великої цінності, якщо інформація зберігається в сховищі й не використовується. Таким чином, здатність своєчасно передавати інформацію в руки тих, хто її потребує, є ще одним важливим аспектом інформаційної війни. Інструменти, які використовуються в цій області, - це не зовсім зброя, а скоріше технології, які використовуються у військових ситуаціях. Найважливішим із цих інструментів є комунікаційна інфраструктура, що складається з мереж комп'ютерів, маршрутизаторів, телефонних ліній, оптоволоконного кабелю, телефонів, телевізорів, радіоприймачів та інших технологій і протоколів транспортування даних. Без цих технологій можливість транспортування інформації в режимі реального часу, що вимагається за сучасними стандартами, була б неможливою.

- Захист інформації.

Одним із найбільш широко узгоджених аспектів інформаційної війни є необхідність мінімізувати обсяг інформації, до якої має доступ ваш опонент. Головним завданням цього є захист інформації, яку ви маєте, від захоплення іншою стороною. Зброя, яка використовується для захисту нашої інформації, поділяється на два класи. По-перше, це технології, які фізично захищають наші життєво важливі засоби зберігання даних, комп’ютери та транспортні механізми, включаючи бомбо- та куленепробивні кожухи та механізми запобігання вторгненню, такі як замки та сканування відбитків пальців. По-друге, технології, які запобігають видимості та перехопленню фрагментів ворогом. Це, безумовно, включає основні технології комп’ютерної безпеки, такі як паролі, а також більш складні технології- шифрування.

- Пропаганда та маніпулювання інформацією.

Інформаційні маніпуляції в контексті інформаційної війни – це зміна інформації з метою спотворити картину реальності опонента. Це можна зробити за допомогою ряду технологій, зокрема комп'ютерного програмного забезпечення для редагування тексту, графіки, відео, аудіо та інших форм передачі інформації. Розробка маніпульованих даних зазвичай виконується вручну, щоб ті, хто командує, мали контроль над тим, яке зображення представляється ворогу, але вищезгадані технології зазвичай використовуються для пришвидшення процесу фізичного маніпулювання після визначення вмісту.

Пропаганду та маніпулювання можна вважати "атакою" на власних громадян, при відсутності захисту, спотворює та деморалізує населення, що неможливо відділити правду від неправди, й формується світ пост - правди, який використовується ворогом, є особливим методом впливу на психіку та знижує можливості аналітичного розпізнавання у населення.

Канали маніпуляції - це загальнодоступні інформаційні канали, що населення в більшості їм довіряє: телебачення, радіо, газети та новітні канали через мобільний зв'язок: особливо під час війни задіяні Мессенджери, що використовуються великими спільнотами: Telegram, Viber, WhatsApp, самі мобільні телефони та соціальні мережі. Підступність використання таких каналів, що об'єднують світ та спільноти, у швидкості розповсюдження дезінформації, а також "якщо ми не згодні щодо того, що є правдою, то авторитарні мережі можуть ефективніше просувати свою версію реальності. "[2]

У роботі [2] автор попереджає не бути легковажними стосовно мемів, маніпулятивних відео чи до тих, хто видає себе за іншу особу й використовує довіру до іншої людини: "Легко припустити, що меми – це нешкідлива розвага, а не потужна наративна зброя в битві між демократією та авторитаризмом. Але

вони є одними з інструментів нових глобальних інформаційних воєн, і вони будуть розвиватися лише в міру прогресу машинного навчання. "

Інформаційна війна – це операція, яка проводиться з метою отримання інформаційної переваги над супротивником. Вона полягає в контролі власного інформаційного простору, захисту доступу до власної інформації, при отриманні та використанні інформації опонента, руйнуванні їх інформаційних систем та порушення інформаційного потоку. Інформаційна війна не є новим явищем, але вона містить інноваційні елементи. Інформаційні війни можуть проходити кількома шляхами. Кіберпростір і пов'язана з ним область нових технологій створюють важливе поле для інформаційної війни. Діяльність кібервійни може складатися з кібератак, руйнування інформаційних систем супротивника, але вони також можуть включати так звані соціальні кібератаки, створюючи у свідомості людей специфічний образ світу, що відповідає цілям інформаційної війни, яку веде дана країна.

Захищатися від атак збору інформації означає не дати нашим ворогам зібрати інформацію про нас і про конфліктну ситуацію. Це передбачає захист нашої власної інформації від перехоплення та запобігання потраплянню інформації до об’єктів збору ворога. Основною технологічною зброєю для захисту власної інформації є шифрування. На жаль, нещодавнє зростання складності криптографії дуже ускладнило контрзаходи. "Декодування повідомлень, створених комп'ютером, швидко стає неможливим. Комбінація таких технологій, як стандарт потрійного цифрового шифрування (DES) для передачі повідомлень за допомогою закритих ключів, і шифрування з відкритим ключем (PKE) для передачі приватних ключів за допомогою відкритих ключів".

Хоча криптографія є найефективнішою, вона не є єдиним інструментом захисту інформації. Насправді паролі є набагато більш поширеною технікою для захисту інформаційних систем від несанкціонованого доступу. Однак, на

жаль, системи паролів залежать від людей, які відстежують і вводять коди, що створює для них значну вразливість.

Як тільки ворог має інформацію, мало хто може зробити, щоб запобігти маніпулюванню нею. З огляду на це, насправді існує лише два контрзаходи для захисту від такого роду атак. По-перше, можна працювати, щоб не допустити перехоплення інформації ворогом. Найефективнішими тут є методи захисту інформації, оскільки вони не дозволяють ворогу отримати доступ до інформації або зрозуміти її у початковій формі. Другий, і, можливо, більш важливий ключ у захисті від маніпуляцій з даними — запобігти повторному введенню змінених даних у потік реальної інформації. На щастя, для цього існує кілька методів, найпоширенішою з яких є резервування. Збираючи ту саму інформацію з кількох зайвих джерел, ви збільшуєте ймовірність того, що правильна інформація пройде. Навіть якщо ворогу вдасться зіпсувати ці дані на одній лінії зв’язку, ви легко виявите погані дані, оскільки вони відрізняються від картини, намальованої рештою ваших джерел.

Ми бачимо, що інформаційна війна не менш складна, ніж традиційна війна. Вона включає багато різних стратегій, технік, зброї та захисту. Багато хто стверджує, що підгрупа тем, представлених тут як інформаційна війна, не враховує важливих загроз національній безпеці. Але цього достатньо, щоб наші військові були зайняті дуже довго. Оскільки ті, хто займає лідируючі позиції в інформаційній війні, дізнаються більше про нові загрози, пов’язані з інформацією, ми зможемо додати їх до переліку методів "інформаційної війни" та почати визначати зброю та контрзаходи для них. До того часу ми повинні використати інформацію, яку маємо, щоб підготуватися до того, щоб бути комбатантами в інформаційній війні, яка вже вирує.

Інформація є інтеркомунікативною, тому її не можна класифікувати за секторами чи галузями. Дуже помилково вважати, що інформація лише у військовій сфері заслуговує на збереження таємниці, а інформація для цивільних цілей не відноситься до категорії секретності. Фактично, якщо не

вжити заходів безпеки для захисту комп'ютерів і мереж, інформація може бути втрачена. Подібним чином, якщо ми думаємо, що отримувати інформацію ворога – це справа відділів розвідки та безпеки, і що вона не має нічого спільного ні з ким іншим, ми втратимо гарну нагоду виграти інформаційну війну.

Інформаційна війна повністю відрізняється від загальноприйнятої концепції націлювання на ціль і знищення її кулями, або командирів, які спираються на зображення та зображення, отримані за допомогою візуального виявлення та за допомогою обладнання дистанційного зондування, для проведення операцій з карти або піщаного столу. Вона коштує недорого, оскільки ворожа країна може отримати паралізуючий удар через Інтернет, а сторона, яка отримує, не зможе зрозуміти, дитяча це витівка чи напад її ворога. Ця характеристика інформаційної війни визначає, що кожен учасник війни має вищу незалежність і більшу ініціативу. Крім того, Інтернет може генерувати велику кількість непотрібної інформації, яка займає обмежені канали та простір і блокує дію власної сторони. Тому лише ввімкнувши відповідні системи та поєднавши людський інтелект із штучним інтелектом за ефективної організації та координації, ми можемо втопити наших ворогів у океані інформаційного наступу.

Народна війна в умовах інформаційної війни ведеться сотнями мільйонів людей за допомогою сучасних інформаційних систем відкритого типу. Оскільки традиційний спосіб промислового виробництва змінився від централізації до дисперсії, а комерційна діяльність поширилася з міських районів на сільську місцевість, робочий метод і спосіб взаємодії у первісному розумінні все більше базуються на інформації. Політична мобілізація на війну повинна покладатися на інформаційні технології, щоб стати ефективною, наприклад, шляхом створення та розповсюдження програмного забезпечення політичної мобілізації через Інтернет, розсилання патріотичних повідомлень електронною поштою та створення баз даних для традиційної освіти. Таким

чином, сучасні технічні засоби масової інформації можуть бути повністю використані, а ефект відкритості та поширення Інтернету може бути розширений, щоб допомогти політичній мобілізації здійснювати свій тонкий вплив. Коротше кажучи, значення та наслідки народної війни глибоко змінилися в інформаційну епоху, і шанси того, що люди виявлять ініціативу та випадково беруть участь у війні, зросли.

Особлива технологія ведення інформаційної війни через мережу Інтернет. Всесвітня мережа все більш розширює можливості збору даних, захисту інформації та зриву інформації, а також полегшує доступ як до громадян певної країни, так і до міжнародної спільноти. Враховуючи швидкість комунікації, широке охоплення та низьку вартість інформації соціальні мережі відіграють вирішальну роль. Сайти соціальних мереж також є цінним джерелом інформації про цільові групи, на які має бути спрямована інформаційна діяльність.

"Нам потрібно розуміти передачу знань в Інтернеті; походження, мотивація та тактика дезінформаційних мереж, як закордонних, так і вітчизняних; і як саме навіть найосвіченіші шукачі доказів можуть мимоволі стати частиною операції впливу. Мало що відомо, наприклад, про наслідки тривалого впливу."[2]

Інтернет використовує, серед іншого:

- Фабрики тролів – організації, на яких працюють люди, які публікують коментарі в Інтернеті відповідно до завдань замовника, використовуючи фейкові профілі в соціальних мережах.
- Боти – програми, які автоматично надсилають повідомлення.
- Фальшиві новини – повідомлення, спрямовані на введення в оману користувачів ЗМІ.

ЗМІ не тільки повідомляють про воєнні конфлікти, а й стають об’єктами атак, зокрема, дезінформацією шляхом поширення фейкових новин.

Журналісти мають бути надзвичайно обережними у перевірці інформації, пов’язаної з міжнародними відносинами, оскільки повідомлення, які вони отримують, можуть бути частиною дезінформаційної діяльності. Інша проблема часто пов’язана зі зломом веб-сайтів, профіль яких протилежний діяльності держави, що веде інформаційну війну. Користувачі ЗМІ також часто стають жертвами інформаційної війни, яка ведеться як за допомогою так званих традиційних ЗМІ та Інтернет. Ознаки пропаганди та дезінформації присутні в численних повідомленнях ЗМІ, включаючи традиційні медіа, а також соціальні медіа. Користувачі ЗМІ все більше усвідомлюють це, вони є об'єктами (дез)інформаційної діяльності, спрямованої на вплив на їхнє сприйняття дійсності.

"Всяка війна заснована на обмані", — заявив стародавній китайський військовий стратег Сунь Цзи в "Мистецтві війни" (написано в 5 столітті до нашої ери). Оскільки все більше наше життя переміщується в Інтернет, багато хто вважає, що використання дезінформації як інструменту переконання та зброї впливу досягло нових висот. Ми маємо більше доступу до новин, ніж будь-коли раніше — від основних каналів новин до соціальних мереж до радіо та подкастів. І легше, ніж будь-коли, зв’язатися з нами — у будь-який час дня чи ночі — на будь-якому з наших численних пристроїв, підключених до мережі.

Зростання впливу Інтернету та соціальних мереж посилило проблему фейкових новин. Традиційна модель новин, коли невелика кількість ЗМІ, укомплектована підготовленими журналістами, які беруть інтерв’ю у надійних джерел, а потім перевіряють інформацію перед публікацією, була порушена поточним медіа-середовищем. Сьогодні теорії змови та чутки досить легко поширюються через різноманітні канали, повідомлення, які є безперервними, і середовище, яке часто не помічає суперечливу інформацію.

Реальність – це питання сприйняття, а інформація формує реальність. Зміщення реальності за допомогою неправдивої інформації дестабілізує — і

може мати серйозні наслідки для психічного здоров’я — призведе до значного занепокоєння тощо. Ми живемо у світі де усе дуже взаємопов’язано, не потрібно багато, щоб перекинутися в нестабільність чи навіть хаос. Хороша новина — і це не фейк — полягає в тому, що ви можете зробити кілька кроків, щоб захистити себе від негативного впливу фейкових новин.

"Мало що відомо, наприклад, про наслідки тривалого впливу дезінформації або про те, як вона впливає на наш мозок або поведінку при голосуванні. Щоб вивчити ці зв’язки, такі технологічні гіганти, як Facebook, Twitter і Google, повинні надати більше своїх даних незалежним дослідникам (захищаючи при цьому конфіденційність користувачів)."[2]

Отже, що ми можемо зробити, щоб боротися з фейковими новинами?

- Не вірте всьому, що читаєте!

Перевіряйте факти. Прості речі можуть допомогти: перевірте дату статті та джерело інформації. Подивіться на інформацію в URL-адресі. Академічні установи (позначаються .edu) та уряд (.gov) можуть бути одними з найнадійніших місць для досліджень, статистичних даних та фактичної інформації.

- Підтвердьте інформацію

Так, ми знаємо, що ви зайняті, і для розвінчування фейкових новин потрібен час. Тож звертайтеся до організацій, які присвячують себе такій слідчій роботі. Їхня місія: коли дезінформація приховує правду, вони прикривають завісу за допомогою перевірки фактів, оригінальних репортажів про розслідування та надання аналізу на основі доказів із задокументованими джерелами.

- Перевірте свої упередження

Так, ми розуміємо, що це непросто. Ми маємо тенденцію сприймати інформацію, в котру ми вже віримо, і відкидати ту, яку вважаємо

недостовірною. Цю концепцію важливо знати, оскільки вона допомагає нам зрозуміти, як соціальні медіа можуть вплинути на відлуння думок. Тому наступного разу, коли ви будете вражені публікацією в соціальних мережах про політика, якому ви опонуєте, зупиніться і поставте під сумнів те, що ви прочитали.

- Зберігайте почуття гумору

Однією з найпотужніших і найпозитивніших захисних стратегій, які ми маємо, є гумор. Нічна комедія та політична сатира не змінять новини, але можуть допомогти зменшити стрес і тривогу, викликані ними. Сміх — безкоштовні ліки, тому багато смійтеся.

- Канал сильних почуттів

Перетворення ваших почуттів стресу в дію може допомогти. Виходьте на акцію протесту, почніть петицію та надішліть її законодавцям штату та федеральному законодавству, зверніться до інформації, якій ви вірите. Ця нова ера фейкових новин не зникне, але ми маємо силу адаптуватися. Соцмережі напружують вас? Вимкніть розетку. Чи надто постійні та заплутані новини? Вимкни. І хто знає, можливо, на допомогу прийде саме технологія, яка сприяла виникненню проблеми.

Висновки: Новітні технології дають багато корисного для боротьби у інформаційних війнах, однак і створюють складні умови через складність систем та технологій, використовуючи ІТ, особливо соціальні мережі, для створення віртуальної спотвореної реальності.

"Якщо дослідники зможуть з’ясувати, що змусить людей зробити паузу для роздумів, це може бути одним із найефективніших способів захистити публічний дискурс і повернути свободу думки."[2]

Список використаних джерел:

1. Проноза І. І., ІНФОРМАЦІЙНА ВІЙНА: СУТНІСТЬ ТА ОСОБЛИВОСТІ ПРОЯВУ, ДЗ «Південноукраїнський національний педагогічний університет імені К. Д. Ушинського» [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: URL:http://app.nuoua.od.ua/archive/61_2018/9.pdf.

2. Aad Goudappel, Everyone Is an Agent in the New Information Warfare, [Електронний ресурс]. – 2019. – Режим доступу до ресурсу: URL:https://www.scientificamerican.com/article/everyone-is-an-agent-in-the-new-information-warfare/.

3. Енциклопедія сучасної України, [Електронний ресурс]. – 2011. – Режим доступу до ресурсу: URL:https://esu.com.ua/search_articles.php?id=12460.

4. Володимир Дудко, Інформаційна війна проти України та методи її ведення, [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: URL:http://www.polukr.net/uk/blog/2021/04/informacijna-vijna-proti-ukraini/.

5. АрміяINFORM, Інформаційну війну Україна вже виграла, [Електронний ресурс]. – 2021. – Режим доступу до ресурсу: URL:https://armyinform.com.ua/2022/03/17/informaczijnu-vijnu-ukrayina-vzhe-vygrala/.

6. Randall Whitaker, Information Warfare, [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: URL:https://www.sciencedirect.com/topics/social-sciences/information-warfare.

Мельник А.Ю,.

здобувач освітнього ступеня «бакалавр» спеціальності

«Економічна кібернетика»

факультету інформаційних технологій 4 курсу 1 групи

Державний національний торговельно-економічний університет

м. Київ, Україна

ГІБРИДНІ ВІЙНИ У ПОЛІТИЧНИХ КОНФЛІКТАХ

Анотація: У науковій статті розглянуто роль інформаційної війни у сучасній політичній практиці та її можливостей впливу на перебіг політичного конфлікту. Вивчено підходи до поняття інформаційної війни в рамках наукової дискусії про рівень самостійності цього явища як окремого виду війни. Досліджено компоненти інформаційної війни, у тому числі сучасні технології впливу на кіберпростір, атаки на комп'ютерні системи, пропаганда.

Ключові слова: інформаційна війна, інформаційно-психологічний вплив, кібернетична війна, політичний конфлікт, електронна війна, інформаційні технології.

Інформаційні технології на сучасному рівні розвитку створюють широкі можливості управління політичними конфліктами як у масштабах однієї держави, так і на регіональному рівні. Дані технології, що активно застосовуються в інформаційних війнах, мають низку переваг перед традиційними засобами боротьби завдяки своєму масованому впливу на моральний – психологічний стан населення країни-противника або окремих партій, рухів та політичний об'єднань. Особлива перевага інформаційної боротьби полягає в тому, що спецслужби неспроможні своєчасно виявити подібний вид впливу та вжити захисних заходів для забезпечення інформаційної безпеки. Інформаційна пропаганда як невід'ємна і значуща частина інформаційної війни створює атмосферу аморальності та бездуховності, дезорієнтує населення, контроль над яким стає неможливо встановити мирними засобами. Найнебезпечнішим наслідком такого впливу стає падіння авторитету та легітимності державної влади, проти яких

найчастіше і спрямовані інформаційні атаки. Інформаційні технології дедалі частіше застосовуються з метою дестабілізації політичних відносин між окремими суб'єктами сучасної політики, провокування політичного конфлікту. Інформаційна війна в політичному конфлікті орієнтована насамперед на внесення розколу в громадянське суспільство. Наслідком таких інформаційних заходів стає громадянська війна, яка в умовах складної зовнішньополітичної обстановки ускладнює прийняття рішень політичною елітою через безладні масові протести, акції та заворушення. Штучно ініційовані зіткнення на релігійній, етнічній та національній основі стають фундаментом для можливого знищення існуючого політичного устрою в даній державі. Тривала пропаганда не тільки веде до руйнування держави зсередини, але й знижує міжнародний авторитет країни-противника, що згодом позначається на його відносинах із регіональними партнерами. Інформаційна війна дедалі більше доводить свою ефективність у досягненні політичних цілей у регіоні та здатна завдати непоправної шкоди тому, проти кого вона ведеться.

Концептуальною основою теорії інформаційної війни, на думку автора наукової статті, є теорія "м'якої сили" С. Мана. Термін «м'яка сила» широко увійшов у лексикон політиків та вчених. «М'яка сила» стає комплексним інструментарієм для досягнення політичних цілей, яку можна використовувати перманентно як в умовах відкритого збройного конфлікту, так і у мирні періоди співпраці. «М'яка сила» включає насамперед ті технології, які найменш затратні, мають слабку розпізнаваність і високу ефективність у трансформації поведінки політичного супротивника не силовими методами. Але, водночас, слід зазначити, що в умовах посилення глобальної конкуренції, використання «м'якої сили» з метою політичного тиску на суверенні держави набуває деструктивного та протиправного характеру. Подібну політику з використанням інформаційних технологій як методу «м'якої сили» можна інтерпретувати як протиправне «М'яка сила» розглядається теоретиком як здатність впливати на інші держави з метою

реалізації власних цілей через співпрацю у певних сферах, спрямовану на переконання та формування позитивного сприйняття . Таким чином, інформаційні війни з їхніми можливостями маніпулювання суспільною свідомістю, політичною обстановкою та емоційним кліматом в інших державах дають змогу руйнувати його політичні та соціальні цінності без застосування фізичного насильства [1].

Необхідно виділити три основні групи визначення поняття «інформаційної війни», представлені сучасними дослідниками.

Автори першої групи пов'язують «інформаційну війну» з окремими інформаційними операціями. Слід зазначити, що В.С. Пірумов визначає інформаційну війну не лише як політичне протистояння з використанням інформаційно-комунікативних методів, а й як сукупність заходів щодо захисту інформаційного простору власної країни. Таким чином, інформаційна війна стає новим видом боротьби, в якому не менш важливим стає захист свого інформаційного ресурсу. Важливо також наголосити, що в даному випадку інформаційний захист, на відміну від технологій інформаційної агресії, має більш високу значущість, оскільки не залежно від бажання політичного суб'єкта інформаційний вплив може бути здійснений навіть у періоди благополучної та перспективної міжнародної політики. На відміну від традиційної війни, інформаційна війна завжди залишається неоголошеною і носить непередбачуваний характер. Важливо звернути увагу на той факт, що періоди міжнародного співробітництва потенційно небезпечніші за явні конфлікти, оскільки інформаційне втручання у «відкриту» для міжнародного контакту систему більш можливе порівняно з періодом гострих суперечностей, коли держави максимально активізують усі захисні механізми фізичних та інформаційних ресурсів. Виходячи з того, що інформаційна війна має перманентний характер, проблема інформаційної безпеки стає ключовою [2]. Так, В.І. Цимбал додає, що інформаційна війна є новим способом політичного протистояння. Отже, з цього погляду інформаційна війна стає інструментом політичної боротьби у всіх її формах [2].

Авторів другої групи представляють спеціалісти з інформаційних технологій військових відомств. На думку представників військової науки, інформаційна війна є процесом, який супроводжує збройне протиборство та не проводиться у мирні періоди. Інформаційні операції є додатковим засобом боротьби при активному застосуванні військової зброї, що дозволяє в короткий термін деморалізувати супротивника. Під час бойових дій важливим є охороняти інформаційну перевагу над противником, яка досягається своєчасним прийняттям інформаційних контрзаходів, виробленням технологій інформаційної підтримки та захисту. Досліджуючи роль інформаційних операцій у ході бойових дій, науковці звертають увагу, що вони підвищують ефективність військових дій, а процес досягнення політичних цілей стає більш прискореним [3].

Автори третьої групи визначень «інформаційної війни» вважають її явищем мирного періоду, метою якої є вирішення політичних завдань не силовим методом, а інформаційним, та запобігання можливому політичному конфлікту. Таким чином, думки про поняття «інформаційної війни» розділилися за принципом: чи це явище є самостійним процесом або складовою більш широкого поняття [4].

Узагальнивши вищевикладені погляди, слід зазначити, що інформаційна війна одночасно може супроводжувати військові дії та здійснюватися, замінюючи їх.

Враховуючи особисту думку то, інформаційна війна є самостійним поняттям. Незважаючи на те, що вона є одним із можливих шляхів ураження противника, і з цього погляду є засобом, вона має свої механізми впливу, прийоми, засоби та техніки і, більш того, її можливості виходять далеко за межі протистояння у політичних конфліктах.

Ми бачимо, що єдина думка у науковому світі щодо формування точної характеристики такого явища як «інформаційна війна» на цьому етапі не завершена. Подібні дискусії розвиваються у рамках пошуку єдиного термінологічного підходу. Так, деякі науковці звертають увагу на те, що сам

термін «інформаційна війна» не зовсім адекватний, і було б правильніше називати цей вид військових дій інформаційною боротьбою. Схиляючись до думки другої групи, цей термін вони пояснюють тим, що інформаційна війна є складовою частиною військового протиборства, а не самостійним процесом. Військово-політичне керівництво США на офіційному рівні замінили термін «інформаційна війна», таким терміном як «інформаційні операції». Інформаційна зброя була віднесена до зброї масової поразки для вирішення принципово нових конфліктів. США припинили використовувати термін «інформаційна війна», а на місце його стали використовувати термін «інформаційні операції». У країнах Західної Європи термін «інформаційна війна» замінений на термін «кібервійна», але наділяється він тим самим змістом і змістом, які приписують «інформаційним війнам» [4].

Також необхідно зазначити, що нині є безліч класифікацій інформаційної війни та сфер її застосування, що створює складнощі в тому, щоб дати їй точне визначення, але, незважаючи на це, ефективність інформаційних технологій залишається безперечною.

Так, враховуючи високу роль інформаційних технологій у політичних конфліктах, до сфер ведення бойових дій, крім землі, моря, повітря та космосу, тепер включається інформаційна сфера. Основними об'єктами поразки у сфері є інформаційна інфраструктура і психіка людини. Проте, незважаючи на різноманітність підходів, найбільш вичерпне визначення «інформаційної війни», яке має високий рівень визнання в наукових колах, запропонував американський теоретик М. Лібіки, виділивши сім її різновидів: протиборство розвідок та контррозвідок, протиборство в електронній сфері, психологічні операції, організовані стихійні атаки хакерів на інформаційні системи, інформаційно-економічні війни за контроль над торгівлею, військове протистояння, кібернетичні війни у віртуальному просторі. Іншими словами, можна сказати, що інформаційна війна включає інтегроване використання можливостей, серед яких виділяються психологічні та комп'ютерні мережеві операції як електронна зброя. В умовах військового політичного конфлікту

інформаційні технології здатні забезпечувати операції з військовою дезінформацією та дезорганізацією [5].

Основна перевага інформаційної війни полягає безпосередньо «у роботі з глибинними сенсами та уявленнями людини». Такий вид впливу, який можна було б назвати війною цінностей, змінюючи уявлення людини здатний програмувати його на певний вид поведінки у конкретній політичній ситуації. Результатом таких процесів стає те, що «маса, переконана в нав'язаних ззовні політичних ідеалах, стає практично некерованою для державної влади». Виходячи з цього, можна стверджувати, що цей вид впливу призводить до найнебезпечніших соціальних явищ в умовах політичного конфлікту – виходу народних дій з-під контролю та початку масових протестів. Іншими словами, інформаційний вплив та маніпуляція політичними настановами населення створює ситуацію нестабільності та різко скорочує шанси політичного супротивника на вигідне для нього вирішення політичного конфлікту. Але основною метою смислового інформаційного впливу на політичному конфлікті є зміна розміщення політичних сил у суспільстві.

Інформаційно-психологічна війна з необмеженими можливостями впливу на людину служить «засобом досягнення політичних цілей у масштабах однієї держави або навіть цілого регіону». В основі інформаційно-психологічної війни, згідно з аналізованою концепцією, лежить «конфлікт інтересів суб'єктів геополітичної конкуренції, метою якого є вирішення протиріч щодо здійснення політичного керівництва в інформаційному просторі та з приводу перерозподілу їх ролі та функцій у політичній системі інформаційно - го товариства». Таким чином, ми можемо зробити висновок, що всі відкриті та приховані інформаційні впливи спрямовані на досягнення інформаційної переваги над супротивником, що знаходить своє вираження у завданні йому ідеологічної та моральної шкоди [5].

Інформаційну війну не можна розглядати лише як можливість технічного втручання в інформаційні системи супротивника, оскільки вона здатна діяти на більш складних рівнях та вносити зміни до когнітивних,

поведінкових та розумових процесів людини. Об'єктом інформаційної агресії є поведінковий стереотип, доступ до якого відкривається через когнітивну сферу. Виходячи з цього, необхідно визнати, що зміна поведінкової структури можуть реалізувати як короткострокові плани, які можуть бути пов'язані з формуванням громадської думки стосовно державних діячів або політичних подій, так і вирішувати складніші завдання, які можна здійснити за допомогою інформаційно-комунікативних технологій.

Якщо поведінкова структура формується на когнітивному рівні, включаючи навички та прийоми мислення, то внесення будь-яких змін до когнітивної структури суспільної свідомості на рівні цілої країни може призвести до непередбачуваних наслідків у поведінковому стереотипі населеня.

Будь-яка соціальна система піддається руйнації, якщо через когнітивний механізм змінюється поведінкова структура, оскільки ці зміни здатні паралізувати системне управління. Геополітична модель інформаційної війни не може бути розглянута поза базовими підходами політичної психології та конфліктології, оскільки інформаційна війна має людський фактор, оскільки ведеться людьми та спрямована на людей.

Розглянутий психологічний аспект інформаційної війни стає також складовою іншого різновиду інформаційної війни, виділеної Лібіки – кібернетичної війни. Знову звертаючись до ідей даного теоретика, необхідно звернути увагу на одну з його фундаментальних робіт. У монографії «Кіберстримування і кібервійна» У М. Лібікі висуває основну свою ідею: кіберпростір є особливим типом простору, оскільки в ньому атака здійснюється «не за рахунок народження сили, а за рахунок використання вразливості супротивника» [4].

Так, кіберконфлікт умовно можна охарактеризувати як сукупність кількох сфер: соціальні медіа, стратегічна війна, промисловий шпигун з заподіянням шкоди інформаційній інфраструктурі та ідеологічна боротьба.

Так, кіберпростір стає новим полем боротьби задля досягнення військово-політичного переваги. Наслідком є тенденція, що спостерігається в багатьох країнах інвестувати фінансові ресурси в контроль над інтернет-простором, особливо в державах з авторитарним режимом, де передумови для народних повстань вже проявилися. Інтернет у таких випадках стає форумом для організації великомасштабних акцій [6].

Висновки: Підсумовуючи, необхідно сказати, що інформаційна війна, включає досить широкий арсенал засобів інформаційного придушення політичного супротивника. Нові розробки в галузі інформаційних технологій дозволили вести боротьбу на абсолютно нових рівнях геополітичного простору: кібернетичному та електронному. Вплив інформаційної зброї стає дедалі складнішим контролювати, що ставить перед міжнародною спільнотою проблему інформаційної безпеки та захисту інформаційних ресурсів в окремих країнах. У політичний конфлікт, який спочатку може вестись двома сторонами, через широкі можливості інформаційних технологій, може включатися дедалі більша кількість учасників, що значно відсуває межі конфліктного регіону. Даний вид війни особливо небезпечний своїм деструктивним впливом на всі сфери суспільства, включаючи більш тонкі матерії, такі як психіка людини, її цінності, почуття патріотизму та національної самосвідомості, які, у свою чергу, є важливою складовою політичного вибору та поведінки. Маніпуляція свідомістю населення політичного супротивника та світової спільноти в рамках регіонального конфлікту стає однією з найважливіших технологій інформаційної війни, оскільки дозволяє не лише спровокувати протилежний бік конфлікту на певні політичні кроки, а й створити вигідні зовнішні умови, за яких держави, опосередковане ставлення, що мають до конфлікту, сприйматимуть його так, як це необхідно «провокатору» для підвищення легітимності та визнання власних дій. Розглянутий вид боротьби дозволяє країнам, що мають інформаційну перевагу, досягати своїх політичних цілей як у військові, так і відносно мирні періоди.

Список використаних джерел:

1. Концепція «м'якої сили» в контексті зовнішньополітичної стратегії України [Електронний ресурс] – Режим доступу до ресурсу: http://repository.hneu.edu.ua/bitstream/123456789/21658/1/1.%20%D0%9A%D0%BE%D1%80%D0%BE%D1%82%D0%BA%D0%BE%D0%B2%20%D0%94.%20%D0%A1.%20%D0%93%D1%80%D0%B0%D0%BD%D1%96%2C%202018.pdf**.**

2. ІНФОРМАЦІЙНІ ВІЙНИ Й КІБЕРТЕРОРИЗМ: ПОНЯТТЯ, ОСОБЛИВОСТІ [Електронний ресурс] – Режим доступу до ресурсу: http://molodyvcheny.in.ua/files/journal/2017/10/160.pdf.

3. ІНФОРМАЦІЙНА ВІЙНА: ЧИННИКИ ЕСКАЛАЦІЇ І ЗАСОБИ ПРОТИДІЇ [Електронний ресурс] – Режим доступу до ресурсу: http://eprints.cdu.edu.ua/4387/1/kalinaich.pdf

4. КОНЦЕПТУАЛЬНІ ПІДХОДИ ДО РОЗУМІННЯ ІНФОРМАЦІЙНОЇ ВІЙНИ В СУЧАСНОМУ СВІТІ [Електронний ресурс] – Режим доступу: https://www.juris.vernadskyjournals.in.ua/journals/2019/3_2019/8.pdf.

5. ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНА АГРЕСІЯ [Електронний ресурс] – Режим доступу до ресурсу: http://enpuir.npu.edu.ua/bitstream/handle/123456789/22262/Kharytonenko_Kharchuk_HVIZh_2018_S.%2028-64.pdf?sequence=1.

6. Інформаційна війна проти України та методи її ведення [Електронний ресурс] – Режим доступу до ресурсу: http://www.polukr.net/uk/blog/2021/04/informacijna-vijna-proti-ukraini/.

Pina T.M.,

здобувач освітнього ступеня «бакалавр» спеціальності

«Економічна кібернетика»

факультет інформаційних технологій 4 курсу 1 групи

Державного торговельно-економічного університету

м. Київ, Україна

КОМУНІКАТИВНА ТЕХНОЛОГІЯ ВПЛИВУ НА МАСОВУ СВІДОМІСТЬ ТА ГРОМАДСЬКУ ДУМКУ

Анотація: Досліджено технології вливу масових комунікацій, їх функції, механізми, характер вливу та наслідки. Виявлено, що масові комунікації передбачають процес поширення інформації для впливу на свідомість людини. Доведено, що зі збільшенням поточного рівня науки та техніки та в умовах глобалізації, збільшується вплив масових комунікацій.

Ключові слова: інформаційна війна, суспільство, масова комунікація, вплив на свідомість, ЗМІ, маніпулювання.

Одним із видів технологій впливу є масова комунікація. За рахунок масових комунікацій з’являються інформаційні війни, вони виникли вже досить давно, зокрема вчені вважають, що вже татаро-монголи розповсюджували чутки, якщо інші країни їх не визнають і не здадуть свої території, то на них чекає розплата. Чутки – один з видів вливу на свідомість людини [1].

У світі засоби масової інформації (ЗМІ) стали потужним інструментом впливу на свідомість та психіку людей. В свою чергу найдоступнішим та найпопулярнішим засобом отримання інформації сьогодні є телебачення та інтернет. Люди повністю піддаються впливу тому, що нічого не знають про способи та технології маніпулювання масовими комунікаціями. Саме тому сучасні комунікативні технології управління свідомістю вимагає наукового осмислення. Масова комунікація передбачає процес поширення інформації, яка впливатиме на свідомості людей і досягає свою оповідальну чи

спонукальну мету за допомогою спеціалізованих засобів: друку, радіо- та телебачення, кіно, а також через соціальні мережі.

Масові комунікації настільки міцно увійшли до повсякденного життя людей, що вони самі не помічають того факту як щодня перебувають під їх впливом. Вплив масових комунікацій часто відбувається у нематеріальному сенсі. Воно характеризується впливом на духовний світ людини: стиль його мислення, систему цінностей, думка на певну тему, але в у багатьох випадках цей вплив має тісний зв'язок із матеріальною сферою, які по суті, сформовані під впливом масових комунікацій бажання, думки, інтересів; цілі людей знаходять своє вираження у їхніх діях та вчинках, які можуть бути спрямовані на будь-який речовий об'єкт [2].

У сучасному світі саме соціальні мережі стають найбільш значним засобом та регулятором управління свідомістю, саме тому, що в сучасному суспільстві лідируючі позиції ЗМІ (Засоби масової інформації) займають на Інтернет-просторі. Основними функціями масової комунікації є збереження, обробка та передача знань про події, явища, поняття з покоління в покоління, а також допомогу в соціалізації та освіті. Існує кілька механізмів впливу на масові комунікації [3]:

- переконання;
- зараження;
- навіювання;
- наслідування.

Зараження – несвідома форма включення особистості певні комунікатори. За допомогою цього механізму робиться великий наголос безпосередньо на емоційний бік особистості, викликається співчуття і співпереживання автору повідомлення, змушуючи читача відчувати ті ж самі почуття та емоції, що й автор. Наочними прикладами зараження є: закадровий сміх при перегляді телепередач або зворушлива музика, яка передає сигнали про сумний момент, спрямовуючи настрій особи на негативні мотиви.

Навіювання – це цілеспрямоване і, найчастіше, неаргументований вплив на одну особу або групу осіб, що використовується для запуску «ланцюгової реакції». Цей механізм працює у взаємодії із зараженням для посилення ефекту. Масові комунікації використовують механізм навіювання для впровадження паніки, страху чи будь-яких інших негативних емоцій у суспільство. Навіювання найчастіше використовується у застосуванні пропаганди певних установок. Передбачається, що людина не здатна об'єктивно оцінити подану інформацію і саме тому він її засвоює. До основних моментів навіювання відносяться:

- авторитетність джерела;
- наявність довіри до цього джерела;
- відсутність опору читача до сприйняття інформації.

Наслідування є імітаційним актом, повторення за зразком. Основна суть наслідування полягає у зміні психічного стану людини. Існують основні форми наслідування:

- наслідування іншого людині;
- наслідування стилю;
- наслідування мови манері.

Наслідування є свого роду пропагандою, оскільки засоби масової комунікації диктують суспільству, що добре, а що погано; що стильно, а що – ні. Засоби масової комунікації малюють образи правильної культури, якій має дотримуватися суспільства. Так, «трендсеттери» - це люди, які є відомими у різних соціальних мережах, які диктують суспільству норми поведінки, спілкування, як треба виглядати, що дивитися і що слухати, а соціум, який стежить за цими людьми, є наслідувачами та намагаються поводитися так само, як і трендсеттери в соціальних мережах. Мабуть, це найяскравіший приклад наслідування.

Всі ці механізми надають прямий вплив на глибину, повноту та ефективність комунікативної поведінки та найчастіше ці механізми працюють

цілісно, взаємодіючи один з одним. В результаті переконання отримана інформація перетворюється на відкладену у свідомості систему установок та принципів особистості. При застосуванні механізму переконання інформація будується на принципі логічних доказів, які змусять особистість повірити в інформацію, що надається. Головною умовою переконливої комунікації є вплив на раціональну та емоційну сфери особистості. У засобах масової комунікації саме ствердні довгі пропозиції та постановка теми є прикладами переконання, у таких прикладах вирішальну роль грають перші, що «кричать», як їх називають у світі журналістики та мас-медіа, заголовки.

Дані механізми є регуляторами суспільної поведінки та свідомості, і вони здатні змінювати свідомість соціуму залежно від своїх цілей як у позитивний бік, так і в негативний.

В даний час інформованість про події, що відбуваються у світі, є досить високою. У людей розширився спектр можливостей щодо різних дій із інформацією. Це пов'язано з виникненням у минулому столітті масових комунікацій.

В умовах глобалізації та поточного рівня розвитку науки та техніки масові комунікації носять електронний, цифровізованим, віртуальний характер. У зв'язку з цим у людей розширюються можливості отримання, використання та розповсюдження інформації. Разом з цим значно зростає рівень впливу масових комунікацій. Особлива роль у цьому плані відводиться інтернету та телебаченню, оскільки саме вони відкривають найповніший доступ до масивів інформації: дані можна отримувати, сприймаючи їх як на слух, так і зорово, причому спостерігаючи динамічну картину. Водночас вони доступні практично всьому населенню Землі. Вони містять різну інформацію, яку в одну мить можна замінити (веб-сайти в Інтернеті, телевізійні канали). ЗМІ надають сучасній людині багато свободи отримання відомостей різного формату. Розширюються можливості щодо створення та розповсюдження даних. Однак не завжди інформація, що передається носить достовірний характер і є корисною для ментальної чи практичної діяльності. Частина

людей поступово усвідомлює, що не всі дані, одержувані із зовні, мають сто відсоткову достовірність [4].

В даний момент більшість українців спостерігають наслідки вливу недостовірної та пропагандистської інформації на росіян. Наслідком є війна між Україною та росією, російські ЗМІ доносять недостовірну інформацію до свого народу, а, в свою чергу, вони не можуть відрізнити фейкову інформацію від реальної. Вплив на людину відбувається поступово і пропорційно, тобто інформація надається частково і в обмеженій кількості, з роками кількість неправдивої інформації збільшується.

Висновки: Отже, масова комунікація - це не просто спосіб навіювання, але і один із видів влади над свідомістю мас та індивідів. Сьогодні найбільш популярним та простим інструментом у впливі на аудиторію є телебачення, яке відображає реальність, та створює новий світ. Основна завдання ТБ – відвернути суспільство від справді значущих проблем та порушити його культурні підвалини, створюючи готові моделі поведінки.

Список використаних джерел:

1. Стадник А. Г. Інформаційна війна як комунікативна технологія впливу на масову свідомість та громадську думку / А. Г. Стадник // Грані. - 2016. - № 1. - С. 111-115. - Режим доступу: http://nbuv.gov.ua/UJRN/Grani_2016_1_22.

2. Пілат М. Є. Інформаційні впливи та інформаційні війни: сутність понять та їхній взаємозв'язок в інформаційну епоху / М. Є. Пілат // Вісник Львів. ун-ту. Серія: «Міжнародні відносини». – 2013. Вип. 32. – С. 185–190.

3. Ожеван М. А. Основні напрями зовнішніх інформаційно-маніпулятивних впливів на суспільні трансформації в Україні: засоби протидії / М. А. Ожеван // Стратегічні пріоритети. – 2011. – № 3. – С. 118–126.

4. Мотузенко Б. І. Соціокультурні аспекти маніпулятивного впливу / Мотузенко Б. І. – Дисертація на здобуття наукового ступеня кандидата соціологічних наук, Київський національний університет імені Тараса Шевченка, 2002.

Samchuk R.O

bachelor's degree specialty «Datar Science»

Faculty of Information Technologies, 3 course 11 group

State University of Trade and Economics

Kyiv, Ukraine

INFORMATION WAR IN 2022

Summary: Many people underestimate the impact of information warfare, but given the current development of technology, one should take into account the new opportunities and threats that arise with the evolution of technology. It is worth noting that in 2022, much more problems arise due to cyber warfare, as all major systems and "functions" of states are based on technology.

Today, information plays perhaps the most important role in people's lives, it has become an integral part of our lives. In the 21st century, information has become a regulator of all social, political, economic and social relations. The process of informatization at this stage is developing so rapidly that it leads to the creation of a single information space. This, of course, is positive for humanity, because of the rapid exchange of economic, political, technical and others. The information allows humanity to develop rapidly. However, the creation of an information society can lead to many information catastrophes, the destruction of the spirituality of society and lead large-scale technical disasters. It is the negative manifestations of the information society that give rise to such a concept as "information warfare", which today has become a real threat to human security. Observing the course and consequences of the wars and conflicts of the XX and XXI centuries, we see that the role of information support is growing rapidly, and indicates a new level of information conflict. Information warfare includes many aspects, the main of which is the impact on

human consciousness by various neurolinguistic means, which are to undermine the goals and worldview of people.

Thus, information warfare today is a comprehensive, holistic strategy that shows the importance of having information in the management, command and implementation of national policy. The information war is becoming a war for knowledge, for those who will know the answers to the most important questions that allow the masses to rule. Of course, in such a war, the number of victims is minimized, but it involves all people directly, which can lead to the destruction of society as such. The normal functioning of the social organism is completely determined by the level of development, quality and security of the information environment, any leakage of information, dissemination of some secret information seriously threatens not only information but also national security. Therefore, in our work, we want to talk about these wars, in which we can and may already be participants. Knowing about information wars, about the methods of their action, is an important step towards solving this problem, because in any case wars bring casualties, and as a result of information warfare there are many more victims than as a result of armed war. The consequences of information wars are catastrophic because such a war is very deep, it destroys the enemy, "from the inside", from the change of consciousness of the population and ends with numerous physical losses.

The topic of information wars is relevant today because information has become one of the most expensive and important goods through which a person can influence other people, social phenomena, and public administration. Each of us can become a participant in such a war, regardless of age, gender or other factors, so in our work, we would like to introduce you to the problems of information wars. Our tasks, in writing this work, were: generalization of methods and methods of information warfare, making several proposals to ensure information security and increasing the efficiency of information technology in Ukraine in this area.

Many people think that information wars came to us only in the twentieth century, with the advent of the technological era, but this is not the case. Information warfare is a historical concept, as evidenced by the informational and psychological impact on man mentioned in the biblical legend of Gideon, who once with three hundred warriors, sneaked into the enemy and carried out a wild night attack at the sound of drivers and shouting "sword of Yahweh and Gideon! ». Enemy soldiers kill each other in confusion and run chaotically, so Gideon frightened thousands of enemy troops. Even then, the great commander Sun Tzu said: "War is a way of deception", which means that to deceive the enemy is necessary not only in their maneuvers but in general by any method, including military disinformation of the enemy. The same informational and psychological influence on people was used in other operations, but their information sources were not perfect, so this war was not very effective. But in the seventeenth century, the first printed publications appeared, which took the information and psychological warfare to a new level, because it was propaganda through newspapers that helped lead whole masses of people to such generals as Frederick II, Peter I, and Napoleon. It was Napoleon who attached great importance to the press in the war with European countries, as everyone knows the saying of this great strategist: "Four newspapers can bring more evil to the enemy than an army of hundreds of thousands", and this was an important factor in Napoleon's success. to conquer the whole of Europe and stay in power for so long.

But the most active development of information technology was in the twentieth century: during the First and Second World Wars.

During the First World War, which showed the extraordinary effectiveness of the press in terms of influencing the psychology of people, and the formation of their desires and goals, there was a policy of strict military censorship, especially in the West. Europe, as well as in Russia, which included Ukrainian lands. This censorship was carried out to completely misinform the population, and thus to misinform the enemy, in many countries, laws, orders,

and prohibitions were issued, which in one way or another related to the information sphere.

After this war, a clear example of information policy is the policy of the Bolsheviks, who through various publications, the distribution of leaflets and various posters promoted and instilled their ideology among the population, and this allowed the formation of public opinion to govern society.

But the most effective information war was during the Second World War, it was during this period that the concept of "information war", "psychological war" and "information technology" finally crystallized. In Germany during this period, the Ministry of Propaganda was even organized, which demonstrates that Hitler's Germany actively used information weapons in the Second World War, in particular, Germany used the media, especially radio, and it worked. A striking example was the story when Goebbels attacked France and broadcast on the radio that the deciphered plan for the attack on the Bourbon Palace was picked up by the entire French press, and thus panic gripped France, helping Germany capture Paris. After the two wars, the issue of information security was considered by many countries and several international documents were issued to ensure the information security of the world, including UN resolutions "Achievements in information and telecommunications in the context of international security", "Declaration on youth respect and mutual understanding between peoples "the declaration emphasizes the important role of the media in this matter. But the time of the most active development of information warfare falls in the XXI century, the century in which we live with you. on information warfare.

So, based on all this, we can agree that information warfare is a historical concept that has been formed for many years, and today information warfare is a war waged with a variety of information weapons (computer, psychological, etc.), in all spheres of public life, the main task of which is to conquer the consciousness, ideology, spirituality of the enemy to gain its resources.

In the course of information confrontation, the objects of influence in the information sphere that need information security are, first of all, people, armaments and military equipment, elements of information and telecommunication systems, etc. Most developed countries have a strong information potential, which under certain conditions will ensure that any of them achieve their political goals, especially since today there are no specific international legal acts governing such a struggle. And that is why "information" crime is active today.

Information crime, as a subject of criminological research, should be understood as recognized as criminal manifestations of information warfare, and socio-negative manifestations that undermine information security, but not all crimes committed through informational influences can be classified as information crimes in criminal legal significance, although it cannot be said that information crimes include exclusively computer crimes, such as access to a computer or network without permission, interception of information carried out directly through external communication channels of the system, etc. Such crimes also include, for example, espionage, which is a criminal activity that consists of secretly gathering information or stealing materials that are a state secret, to transfer them to another state, and others.

This problem of information crime is a global problem, because the use of advanced information technology blurs the borders between countries, and allows the free commission of information crime, and such crime today is transnational, so one of the main problems in the world is information security.

Currently, special norms and principles have been developed, are in force and are being developed, which directly regulate the issues of international information exchange. the following special principles on which cooperation in the information sphere is organized can be distinguished in international legal documents:

• issues of foreign dissemination of information should be regulated by international documents;

• The media can legitimately be used to spread democratic ideas internationally;

• States should prevent the use of the media for the cross-border dissemination of ideas banned by the international community;

• States have international political responsibility for the compliance of the international activities of the national media with generally accepted norms of international law.

But unfortunately today there are very few, compared to the scale of information wars, regulations that would regulate the pure information sphere of public life. One such document is the Resolution on Advances in Information and Telecommunications in the Context of International Security, which called on Member States to address common information security issues, address specific information threat technologies, including unauthorized interference and misuse of information and telecommunications systems and information resources, develop international principles aimed at strengthening the security of global information and communication systems and the fight against information terrorism and crime. But many negotiations are underway on national security, ICT security and the functioning of public authorities, on agreements to protect information on medical data, and the intellectual property of scientific research against any unauthorized interference, including illegal banking and financial transactions.

Based on all the above, it can be seen that the problem of information crime and information security issues remain open. Today, as never before, the question arises of compiling a legal framework that would ensure the punishment of information criminals, and hence the information security of countries.

Highly developed industrialized countries have the most significant information influence in the world today, while other countries may fall victim to such influence and lose their sovereignty. Ukraine is under such a threat today. The possibility of information warfare and the use of information

weapons against Ukraine is especially growing now that there are unlimited opportunities to borrow foreign information technologies, various technological tools and software, non-traditional channels of information influence and unauthorized access to it, facilitate technical intelligence, expand operational opportunities to control the territory of Ukraine, the emergence of electronic terrorism. Of course, Ukraine's special services have the necessary tools and experience to prevent, intercept, distort and destroy information leaks in information and telecommunications networks and public systems, but the pace of improvement of information weapons today far exceeds the pace of defense technology in Ukraine. Today in our country there is a mismatch of the structure and content of the criminal law to the real needs of the information society, such miscalculations contribute to the improvement of methods and techniques of information warfare aimed at achieving socially dangerous consequences. Regarding the information war that Ukraine is facing today, the following should be noted:

• This war should be considered in the general context of the current situation in the country, in the context of a fierce struggle for power, the global economic crisis and in the protection of their state interests.

• In this information war it is necessary to note the participation of not two, but a larger number of participants, among which should be considered not only Russia but also Western European countries and international organizations.

• Ukraine should focus on two fronts: internal, where the government should stop all sorts of political battles, and external, where there are some difficulties in relations with some countries and various international organizations in general.

Therefore, taking into account one of the principles of our society "everything that is not prohibited by law is allowed", in modern conditions increases the need to reform the law to create an independent criminal law framework to ensure information security in Ukraine. Information security

professionals have been trying to bring this issue to the attention of senior management for a long time because it is one of the problems related to national security, they call for a comprehensive approach to this problem because information security is very acute today.

Conclusion: The experience of wars and conflicts in the history of the world has shown that any new sphere of human activity is becoming a sphere of armed struggle, such a weapon has become today's information, which preceded the formation of information wars in society. In general, the world does not stand still, technological progress equips modern man not only with new, improved means of production and communication, but also means of destroying themselves and others. Today, humanity has made such progress that it has become impossible to control some global natural phenomena, environmental weapons can artificially create hurricanes, storms and tsunamis. Many people die in such a war, and if each of us does not think about such a problem, then shortly a person may simply destroy himself.

Informatization of society has already led to many irreversible processes that negatively affect public life and destroy human spirituality, consciousness and understanding, this pace of modern development can lead to human degradation and their inability to think, feel and express emotions, ie turn people into machines. Science fiction has repeatedly described such processes and their consequences, and today we are on the verge that science fiction can become a reality. If we correctly understand the importance of information problems, then today we must move in the direction of overcoming them, because information weapons can destroy the most important thing that a person has - his consciousness. Researching information wars, we saw that their actions affect all spheres of society, and the consequences of such wars are extremely dangerous spiritual values society, which can lead to the destruction of society as such. And today the countries of the world must work on creating a legal framework that could regulate the processes of informatization of society.

References:

1. Інформаційна боротьба у воєнних конфліктах другої половини XX століття. Монографія. – К.:Альтерпрес, 2006. – 192 с.

2. Вилко В.М. Інформаційно-психологічне забезпечення Збройних сил США в локальних війнах і збройних конфліктах 1950-2000 рр. (Історичний аспект). – К.:НАОУ, 2005. – 216 с.

3. Резолюція „Досягнення у сфері інформатизації і телекомунікацій в контексті міжнародної безпеки” R 54149 (23.12.1999)

Шаяхметова О.Р.,
здобувач освітнього ступеня «бакалавр» спеціальності
«Економічна кібернетика»
факультету інформаційних технологій 4 курсу 1 групи
Державний торговельно-економічний університет
м. Київ, Україна

ІНФОРМАЦІЙНА ВІЙНА ПІД ЧАС ВТОРГНЕННЯ РОСІЇ В УКРАЇНУ

Анотація: У науковій статті розглянуто інформаційну війну між Україною та росією під час вторгнення останньої на територію незалежної України. Визначено різницю боротьби в інформаційному полі між Україною та росією. Проаналізовані одні з найбільш обговорюваних інформаційних вкидів зі сторони Російської Федерації.

Ключові слова: інформаційна війна, пропаганда, українські біолабораторії, неонацизм, пологовий будинок в Маріуполі, різанина в Бучі.

За довго до та під час вторгнення росії в Україну ЗМІ з обох сторін вели активну інформаційну війну. У зв’язку з військовою агресією Російської Федерації проти України, як один із напрямків інформаційної війни агресором використовується пропаганда війни засобами масової інформації. Метою російської сторони було створити причину для вторгнення та виправдати вторгнення. Напередодні вторгнення росія помилково заявляла, що відповідає на агресію України і звільняє її громадян від, так званих, фашистів і неонацистів, що не відповідає дійсності. А після початку вторгнення росія безпідставно заявляла, що українці бомбили їхні лікарні та вбивали мирних жителів. Отже, можна сказати, що російська тактика інформаційної війни – напад та обвинувачення української сторони.

Україна здійснює тактику захисту. З початку повномаштабного вторгнення найбільші мовники(«1+1», «Рада», «СТБ», «Україна 24», «UA:Перший» та «ICTV») об’єдналися у спільний телемарафон «Єдині новини», щоб озвучувати офіційну позицію держави, найважливішу

інформацію про гуманітарні коридори, зведення з фронту та випуски зі спростуванням ворожої дезінформації.

Одними з найпопулярніших російських пропагандистських легенд були наступні інформаційні вкиди:

Українські біолабораторії

6 березня російські ЗМІ стали стверджувати, що співробітники української біолабораторії передали Москві документи, що підтверджують зачистку слідів військово-біологічної програми, що реалізується в Україні, фінансованої міноборони США. Як доказ було наведено фотографію указу МОЗ України про знищення «особливо небезпечних патогенів збудників чуми, сибірки, туляремії, холери та інших смертельних хвороб». Наступного дня російські ЗМІ поширили утвердження колишнього офіцера армії США та експерта з боротьби з тероризмом Скотта Беннетт, який стверджував, що в американських лабораторіях в Україні розроблялася біологічна зброя, спрямована проти слов'ян.[1]

Ці твердження були спростовані українським МЗС, яке заявило наступне:

“Усі лабораторні можливості в Україні виконують єдину загальну функцію — індикацію та ідентифікацію збудників інфекційних хвороб, які мають значний епідемічний потенціал та/або міжнародне значення та підпадають під регуляцію відповідно до міжнародних правил.” [2]

Заступник держсекретаря США В. Нуланд також заявила, що в Україні є лише біологічні дослідницькі центри, а не лабораторії з виготовлення зброї.

Крім того, біологи заявили, що серед знищених штамів немає жодного особливо небезпечного, такі штами типові для мікробіологічних та епідеміологічних лабораторій; навіть знаходження штамів чуми, сибірки, туляремії або холери в лабораторії, що займається особливо небезпечними інфекціями, також не свідчило б про розробку Україною біологічної зброї.

Біолог Євген Кунін відкинув можливість, що документи про знищення потенційно небезпечних мікроорганізмів в українських лабораторіях

доводять, що Україна виготовляла біологічну зброю. Він заявив, що знищення мікроорганізмів у лабораторіях - це нормальна практика, а перелічені в документі бактерії погано підходять для розробки біологічної зброї та є практично в будь-якій епідеміологічній чи мікробіологічній лабораторії.[2]

Твердження про те, що в українських лабораторіях нібито намагалися створити етнічно-орієнтовану біозброю, ще сумнівніші, сама можливість створення такої зброї відкидається біологами. У 2017 році комісія експертів Російської академії наук склала висновок, науково обґрунтувавши неможливість створення генетичної зброї.[2]

Обстріл пологового будинку в Маріуполі

9 березня відбулося бомбардування будівлі пологового будинку № 3 у Маріуполі, внаслідок якої загинуло 4 особи та постраждало як мінімум 17 людей. За заявою української сторони, її було здійснено російською авіацією.

Російська сторона заперечувала всі звинувачення і заявляла, що дотримувалася оголошеного «режиму тиші», лікарня давно не працювала, а приміщення було опорним пунктом українського батальйону «Азов». Проте видавець та головний редактор проекту «Перевірено. Медіа» Ілля Бер у своєму розслідуванні зробив висновок, що у зроблених до обстрілу повідомленнях російської влади про розміщення націоналістичних батальйонів у пологових будинках, навіть якщо їм можна довіряти, або не називалися номери пологових будинків, або називався пологовий будинок № 1, а не розбомблене пологове відділення Лікарні № 3. Твердження про те, що одна і та ж вагітна Маріанна Підгурська видавала себе за двох жертв російського бомбардування, не відповідають дійсності, що підтверджується і даними від Factcheck.org.[3] Таким чином, Ілля Бер зробив висновок, що твердження про «постановочні» та «зрежисовані» кадри обстрілу не витримують жодної критики і точно не відповідають дійсності. Свій розбір він підсумував такими словами: «Поки що ми не знаємо точно, хто саме і звідки здійснив обстріл пологового відділення лікарні №3 Маріуполя».[3]

Різанина в Бучі

Російська сторона послідовно заперечувала свою причетність до масових вбивств цивільного населення в Бучі або називала свідчення вбивств підробленими, або звинувачувала в них українську сторону, незважаючи на численні докази того, що тіла вбитих цивільних з'явилися в Бучі під час присутності російського військового контингенту та свідчення скоєння вбивств мирних жителів російськими військовими. Bellingcat[4] та інші ЗМІ дійшли висновку, що дані ставлять під сумнів заяви Росії.

Так, хоча російська сторона стверджувала, що про трупи на вулицях Бучі не повідомляли протягом чотирьох днів (з відходу військ з Бучі 30 березня до перших фотографій трупів 3 квітня), насправді російські війська ще залишалися на околицях міста до 1 квітня, того ж дня в українських телеграм-каналах з'явилися перші світлини з місця подій. Начебто спостерігаються рухи трупів на відеодоказах різанини в Бучі насправді пояснювалися спотвореннями через краплю дощу, що стікає по лобовому склу, або спотворенням картинки в дзеркалі заднього виду. Заяви про те, що трупи нібито виглядають надто «свіжими», відкинули судмедексперти.

Нарешті, звинувачення українських військ у вбивствах мирних жителів спростовуються тим, що трупи з'явилися до виходу з міста російських військ.

Справжність часу супутникових знімків Maxar, оспорюваного проросійськими ЗМІ, було підтверджено BBC.[5]

Висновки: Підсумовуючи висловлене, можна стверджувати, що в п еріод інформаційної війни ворог може маніпулювати свідомістю для розсіювання паніки серед мирного населення та переконання світових лідерів у своїй правоті, що загрожує національній безпеці України. Тому необхідна адекватна інформаційна протидія.

Наразі Україна виграє передусім у тому, що їй вдалося підвищити рівень медіаграмотності населення та створити великої кількості українського контенту для закордонних авдиторій. Тому Україна веде максимально відкриту війну, щоб світ бачив правду.

Список використаних джерел:

1. Теорія змови про біолабораторії України [Електронний ресурс] – Режим доступу до ресурсу: https://uk.wikipedia.org/wiki/%D0%A2%D0%B5%D0%BE%D1%80%D1%96%D1%8F_%D0%B7%D0%BC%D0%BE%D0%B2%D0%B8_%D0%BF%D1%80%D0%BE_%D0%B1%D1%96%D0%BE%D0%BB%D0%B0%D0%B1%D0%BE%D1%80%D0%B0%D1%82%D0%BE%D1%80%D1%96%D1%97_%D0%A3%D0%BA%D1%80%D0%B0%D1%97%D0%BD%D0%B8
2. Заяви РФ про нібито розробку біологічної зброї в Україні [Електронний ресурс] – Режим доступу до ресурсу: ua.interfax.com.ua/news/general/809091.html
3. Social Media Posts Misrepresent Victims of Hospital Bombed in Mariupol [Електронний ресурс] – Режим доступу до ресурсу: https://www.factcheck.org/2022/03/social-media-posts-misrepresent-victims-of-hospital-bombed-in-mariupol/
4. Беллінгкет [Електронний ресурс] – Режим доступу до ресурсу: https://uk.bellingcat.com/
5. BBC News Русская служба [Електронний ресурс] – Режим доступу до ресурсу: https://www.bbc.com/russian

Наукове видання

Матеріали

ІІ Студенського науково-практичного журналу

ТРАКТАТ СОВИ:

ІНФОРМАЦІЙНА ВІЙНА:ПРОБЛЕМИ ТА НАСЛІДКИ

12 липня 2022 року

м. Київ

Редактор:

Мельник Анастасія Юріївна

Відповідальний секретар:

Васильєва Владлена Юріївна

Дизайн обкладинки:

Шаяхметова Олександра Русланівна

ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ,

Факультет інформаційних технологій,

02000, Україна, м. Київ, вул. Кіото 19,

тел. (+38044) 531-31-73,

e-mail: fitnauchit@gmail.com