Hazards posed by the war in Ukraine: A study of population information risk and mitigation efforts

line 1: Petko Dimov
line 2: *Department of Distance Learning, Language Training and Qualifications*
line 3: *Rakovski National Defence College*
line 4: Sofia, Bulgaria
line 5: p.dimov@rndc.bg

line 1: Georgi Marinov
line 2: *Department of Logistics*
line 3: *Rakovski National Defence College*
line 4: Sofia, Bulgaria
line 5: g.marinov@rndc.bg

***Abstract*. The Russian-Ukrainian conflict is the most significant security crisis since World War II. Intense fighting has irreparable effects on water, air, soil, and the ecosystem. They are leading to a massive loss of life and unfolding social and humanitarian disaster in the Black Sea region.**

Even more significant, however, is the information disaster in cyberspace, which has gone far beyond these borders and even affected the whole world.

This study reviews available normative documents to examine the maximum amount of documents related to managing Russia's and Ukraine's combat operations in information warfare.

Access to the state electronic databases of Russia and Ukraine, which provide access to many normative documents, was used to fulfill the set objective. These are the "Official web portal of the Parliament of Ukraine" (Verkhovna Rada of Ukraine) and "The Federal Assembly" of the Russian Federation (The State Duma).

The aggregate number of sources examined is 83564. Based on the criteria for inclusion, the total number of articles analyzed was reduced to 216, as they specifically pertain to security in information and cyberspace.

The research findings on information risk between the two countries indicate that their primary focus was ensuring cyber security following the outbreak of war. However, one of the initial priorities was to address the safeguarding of e-government and the information security of citizens. Subsequently, steps were implemented to combat false information and coordinate their media, which was crucial to the operation's success.

The analysis indicates that Russia is presently experiencing defeat in the information war between the Western world and Ukraine. However, it is achieving resounding success within its borders and is garnering support from Chinese citizens as well as other isolated nations like Iran and North Korea. Partial achievements have been observed in Asia and Africa. However, the situation could rapidly shift due to the superior influence of Western powers on popular social platforms, including Facebook, Twitter, Instagram, YouTube, and Google.

This conflict has transcended into more than a mere battle between two nations and their military forces. It embodies the form of an impending conflict— the war behind the war.

Keywords: cyber operations, cyberwar, information operations, warfare

I. Introduction

The war between Russia and Ukraine is the most significant security crisis since World War II. Intense combat is causing irreversible damage to water, air, soil, and the biosphere, resulting in substantial casualties and a developing crisis in the Black Sea region. This poses specific political, economic, and energy dangers for Europe. The information catastrophe in cyberspace has extended beyond boundaries and impacted the entire planet.

The article analyzes normative activity and legal actions in the information sphere and cyberspace. It examines 83564 normative documents issued by the Russian Federation and Ukrainian governments during the war, as published in state electronic databases.

II. Methodology

This study reviews available normative documents to examine the maximum amount of documents related to managing Russia's and Ukraine's combat operations in information warfare.

Access to the state electronic databases of Russia and Ukraine, which provide access to many normative documents, was used to fulfill the set objective. These are the "Official web portal of the Parliament of Ukraine" (Verkhovna Rada of Ukraine) and "The Federal Assembly" of the Russian Federation (The State Duma).

Print ISSN 1691-5402
Online ISSN 2256-070X
https://doi.org/10.17770/etr2024vol4.8229

The search principle for articles used the following keywords: 'Information operations' AND 'cyber operations'; 'cyberwar' AND 'information warfare*'; 'Ukraine' AND 'Russia'; 'cybersecurity' AND 'information security'.

As the topic is relatively new, a limit of documents was set for the period 14 May 2021 until 3 January 2024.

Inclusion criteria

1.) Official documents are published in English or Russian.

2.) Normative documents related to changes in information and cyber security

3.) Official normative documents issued by Ukraine and the Russian Federation governments.

4.) Influence on own, opposite, and allied citizens.

5.) Unclassified documents issued by Ukraine and the Russian Federation were used.

III. Results and discussion

Ukraine's Actions in the Information Domain.

The normative activity of Ukraine after the start of operations was studied, and 45151 legal decisions and decrees were reviewed from the web portal of the State Rada (zakon.rada.gov.ua), 142 of which affect the population in the domain of information.

Strategic Communications Strategy, Information Security Protection Strategy, and Cybersecurity Strategy [1] were adopted before the start of the war and updated promptly just before the war by Decree No. 447 of 14 May 2021.

The "Basic Principles of Cyber Security Act" also governs changes by wartime laws, for example. It defines the objects of critical information infrastructure and the requirements for the various actors.

In other words, it can be said that Ukraine has a relatively modern legal framework in the field of cybersecurity. In the field of information security, changes are required with the entry into force of the "Presidential Decree on Martial Law", such as, for example, the early graduation of cadets from the Institute of Special Communication and Information Protection of the Polytechnic University of Kyiv [2].

To counter the massive cyberattacks at the start of the 08 March war, Decree 42 ordered banks and government organizations to store their users' data in cloud storage only in the EU, the United Kingdom, the United States, or Canada [3]. In this connection, a law was passed on 13 March to ensure the functioning of information and communication systems and public electronic registers, stipulating that backup copies be created for storage outside the occupied territories. On 15 March, the Criminal Procedure Code was updated to counter cyberattacks. The Law on Electronic Communications was adopted, changing the "Procedure for maintaining a register of providers of electronic communications networks and services" and the means for their certification.

One of the first things that the Ministry of Digital Transformation of Ukraine is doing is to create an electronic identity document during the martial law period (eDocument), which provides information about the person using the mobile application Diia, and this is done automatically, without the presence of the user through the "Unified state web portal for electronic services".

On 19 March, Decree 151 was issued to neutralize threats to the country's information security, with digital terrestrial radio and television facilities operating around the clock from a particular wartime location. Taking into account the direct military aggression of the Russian Federation, the active dissemination of disinformation by the aggressor state, the distortion of information, as well as the justification or denial of the armed aggression of the Russian Federation, Decree No. 152/2022 of 19 March 2022 of the President of Ukraine on the implementation of a unified information policy under the law of war is issued. A unified information policy is a priority issue of national security, which is implemented by combining all national TV channels, whose program content consists mainly of information and analytical programs on a unified information platform for strategic communication "United News #UArazom".

All activities about the collection, processing, and dissemination of official information products shall be assigned to the Ukrainian National News Agency "Ukrinform", and the production and broadcasting of television and radio programs to the State Enterprise "Multimedia Platform for International Broadcasting of Ukraine", the latter being allocated additional funds for the creation of a Russian-language television project "Svoboda". Two programs are also established: the "Development and Modernization of the State Special Communication and Information Protection System" and the "National Information Program" to ensure the protection and uninterrupted operation of the National Telecommunications Network and critical information infrastructure facilities - national electronic information resources and state information and communication systems.

A law banning the propaganda of the Russian neo-Nazi totalitarian regime, and the symbols used by the armed and other military formations of the Russian Federation in the war against Ukraine, has been adopted.

Already in the early days of the conflict, Ukraine broadcast many products that evoked strong emotions to boost the patriotism and morale of its audience. Messages are broadcast on all channels, focusing on the internet and social media. All announcements are initially approved and published in official channels or online conferences and subsequently distributed in social groups, Facebook, Twitter, YouTube, etc [4]. Telegram was not left out, so several groups and applications were created.

Ukraine's online propaganda primarily focuses on its heroes and martyrs who tell the story of Ukrainian courage. This is a classic example of modern propaganda that is critical to the narrative that Ukrainians are fighting for a just cause and will win this war. These messages must influence the hearts and minds of their citizens. This is especially important in this conflict as the Ukrainians try to maintain high morale among their fighters.

Modern means include cyberattacks, viral messaging, and drowning the opposing narrative in a sea of adversary content. This is why new wars are developing at breakneck speed on social media and official websites, and more

content is needed to spread the messages of our narrative and drown out that of the enemy. Social media has become a significant channel for pushing information, and tech companies can play a role in the information war, whether they are vetted or not.

Ukraine's strategy for influencing an allied audience relies on creating emotions that evoke patriotism and support. Constantly broadcast clips of the President of Ukraine created a patriotic, courageous image of Volodymyr Zelenskyy, who presented himself as a hero seeking support.

This is why the Ukrainian government turned to Western social media, showing an excellent understanding of information technology and modern marketing techniques. For example, the "Hero Stickers" initiative was created on Twitter to bring together various hacking organizations to carry out cyberattacks against Russia with remarkable results. The world's largest hacking organization, Anonymous, attacked Russian government websites, including access to personal data stored on the Ministry of Defense of the Russian Federation website. According to Chinese sources, 27% of DDoS attacks on Russian sites were launched in the US, which is unlikely to have been carried out by individual hackers but rather the work of an organized government force [5].

In the fight for the enemy audience, the Armed Forces of Ukraine started to search for contacts on social networks of relatives of captured and killed Russian soldiers and tried to communicate with them in an attempt to create mass discontent against the government. One striking example in this area is the website "The Project", which identifies the names of Russian commanders of troops and units taking part in a particular operation. "Project" publishes a database with information about the Russian army units involved in the war, which area of the country they came from, and the names of their commanders. A particular unit of hackers investigates the biographies of these officers and the state of the military units they command, tracks down their relatives, and attempts to influence them on social networks.

Investigations that fuel stereotypes about Russians have also been published. According to the state website, "the average income of division commanders in 2019 was 160 thousand rubles (2348 euros at the current exchange rate). They also own a small apartment, with 1/3 of the officers having mortgage loans, and ¼ having traffic tickets, some for drinking". But we must remember that they should be looking for bad examples, scandals, corruption, and other misdeeds to publicize.

After the rapid update of the legislation at the beginning of the war, Ukraine already had modern legislation in the field, but it did not stop there. It continued to adapt to enemy actions and to propose new initiatives in the information domain. The Ministry of Defence has launched a new digital service app that reduces the administrative burden on soldiers in combat. On April 24, 2023, the Restart in Cyberspace project began training citizens ages 25 to 60 to help in the field. At the end of 2023, the adopted Action Plan for 2023-2024 for implementing the Cybersecurity Strategy of Ukraine was published. It states that for the first quarter of 2024, the Ministry of Defense should establish a cyber military in the MoD system and a military incident response center. It was establishing a national cyber-attack detection system, countering acts of cyber-terrorism, and establishing a cyber-intelligence system [6]. Improve regulatory, organizational, and personnel support for the national system, and improve training of employees, etc.

Actions of the Russian Federation in the Information Domain.

In the government website publication.pravo.gov.ru, a search for regulatory documents signed in the period 24 February 2022 to 3 January 2024 found 38413 results of the Russian Duma, the Government, and decrees of the President of the Russian Federation, of which almost 74 concerned security in information and cyberspace.

The documents show that in an attempt to protect its audience, Russia is also stepping up efforts to block, restrict, and control the various foreign social platforms and providers operating on its territory. The Presidential Decree prohibits using foreign security at critical information infrastructure sites [7].

As soon as the war began, Deputy Prime Minister Dmitry Chernyshenko instructed the Russian Ministry of Digital Development, Communications, and Mass Media to prepare priority measures to protect the country's information infrastructure. As a result, measures taken include allocating funds to support the IT industry, increasing salaries for employees in the IT sector, granting support for promising local IT solutions, and providing preferential loans to IT companies for ongoing operations and implementation of new projects.

Yandex, Rostelecom, and VK immediately announced that they would provide their public "clouds" to maximize the speed of state sites. According to a leaked government telegram published on Nexta, the Deputy Prime Minister has ordered all government websites and web services to switch to Russia's ".ru" domain name system by March 11 and to switch to using DNS servers located on Russian territory, as well as to "complicate the password policy" [8].

In addition to stopping foreign hosting, a decree is issued with additional measures that stop traffic counters, analytics tools, and banner ads provided by foreign companies, such as Google Analytics [9].

Already on the ninth day of the war, the State Duma passed a law on punishment for spreading fake news related to the actions of the Russian armed forces, which imposes a fine of 700,000 to 1.5 million rubles or up to 3 years in prison. If this has led to severe consequences - from 10 to 15 years in prison [10], i.e., anyone can not spread whatever information they want about the events in Ukraine. Still, only such information originates from official Russian institutions. That is why most websites and blogs are silent on this issue, lest they make a mistake somewhere and get fined or imprisoned [11].

At the beginning of the third week of the war, the Prosecutor General's Office of the Russian Federation asked the court to recognize the technology company Meta as an extremist organization and ban their activities in Russia based on Article 280 and Article 205.1 of the

Criminal Code of the Russian Federation for "public calls" to carry out extremist activities and promote terrorist activities on Facebook and Instagram, and for having discriminated against state media since 2020. With this decision, the government blocked Facebook and Instagram and then suggested that government agencies create accounts on domestic social networks such as RuTube (for video), VK (a Facebook clone), Fiesta (like Instagram), and Telegram. Gazprom Media, too, created a kind of TikTok called Yappy.

Google and YouTube stopped selling online ads in Russia, and TikTok stopped live streaming and publishing new content in the country [12]. Twitter has announced that some users in Russia cannot access the social network. Microsoft banned sales to Russian citizens following a similar move by Apple. BBC, Voice of America, Deutsche Welle, and Radio Free Europe were blocked. The independent Echo of Moscow radio was taken off air for continuing to call what was happening in Ukraine a "war". The same was the fate of the opposition television "Dozhd".

These actions will likely make it difficult for most Russian citizens to see an adversary's point of view. Still, a recent Levada Center survey shows that nearly a quarter of Russian citizens surveyed use VPNs to access blocked websites, citing connection points outside Russia [13].

The restriction on access to foreign technologies and communication platforms forces users to rely on alternative and available services from Russian companies, and the Russian authorities strictly control these services.

Since the start of the war in Ukraine, Russian users have had significant problems accessing government websites and online banking clients.

Several dozen organizations in the world have digital master certificates, but 75% of them are issued by just five of the largest companies that are based in the US [14].

For this reason, the Ministry of Digital Development, Communications and Mass Media of the Russian Federation offers its master certificate from which subsidiary public service certificates are issued. The problem is that browsers like Chrome, Safari, Microsoft Edge, and Mozilla don't recognize this certificate. Therefore, Russian users must manually add the Russian certificate to the trusted list or switch to Yandex and Atom's Russian browsers. Since the certificate is state property, installing it is trusting the authorities.

Regarding the enemy audience, the Russians' strategy combines physical influence, cyberattacks, information, and psychological operations conducted by previously prepared powerful formations.

Among the first targets in the military operation were critical elements of Ukraine's media and communications infrastructure. Proof of this is the first object destroyed by sabotage – the main television repeater in Eastern Ukraine. Subsequently, mobile operators' base stations have been impacted by sabotage and fire strikes, hacking attacks for data theft, DDoS of important portals and official websites with botnets of the "Maray" type, and signal jamming by radio electronic warfare units [15]. Because of this, there are almost no Ukrainian mobile operators in Crimea and Eastern Ukraine and no Ukrainian radio and television stations.

In cyberspace, information is initially gathered through phishing, the purchase of compromised data from hacker forums, and attacks to access address books of mail servers. Typical social engineering techniques or direct penetration through software vulnerabilities in management systems are used for penetration. Next is the internal distribution of the malicious "NotPetya" type code and the theft of data and its transmission via encrypted communication software such as the Telegram Group API or the theft of files using Robocopy, which copies them to an additional cloud drive.

In the adversary's information space, the Kremlin, through direct or indirect funding, creates disinformation content, maintains "factories" of trolls, and distributes this content in a coordinated manner on social networks. These "trolls" are most often people working from home who create and maintain fake (and, more recently, real) profiles, which they use on command to share "news" in groups and pages, as well as writing comments under news articles [16]. This, in turn, leads to algorithmic amplification of these posts (because lots of people are interested), with Facebook (and other social networks) showing it to more and more people.

Regarding the strategy of influencing the allied audience, what often fails to be understood is that Russian propaganda, despite popular belief, is not mainly focused on the Western world. Russia is aware that, for the most part, the people here are hostile to Russia, and nothing will change that. However, gaining popularity in Africa and Asia is an achievable goal and is undoubtedly the focus of Russian information and psychological operations. For example, we might see a news story about a difference in behavior toward Ukrainian and black refugees that does not impact us but has a significant impact in India or Africa [17]. While this news has no repercussions in Europe, countries like Nigeria may have a different view [18].

Russian propaganda pays special attention to China, even though all the fighting events are accompanied by live reports from Chinese journalists, stating that the Chinese do not support NATO enlargement [19]. The Carter Center China Focus provided the first poll of Chinese public opinion on Russia's invasion of Ukraine in April. The results show that 75% of respondents agree that supporting Russia in Ukraine is China's national interest [20]. However, more than 60% of respondents support a neutral policy through moral support without supplying arms to Russia. Notably, only 16% of respondents support providing arms to Russia, only 3% more than those who believe China should change its current course and condemn the Russian invasion. Moreover, the Chinese Foreign Ministry spokesman also repeatedly blames NATO for getting too close to Russia's borders.

Television crews with pre-prepared reports or cameras positioned to film the enemy for provocation are widely used in information warfare. For this purpose, formations are deployed and fire from kindergartens, schools and residential or public buildings. Within 1 - 2 hours after the event, reports are broadcast in which actors play. Russian television and news agencies (NTV, Channel One, Life News, Channel 24, Zvezda, RIA Novosti, Russia Today,

Rossiya Segodnya, ITAR-TASS, and Komsomolskaya Pravda), as well as Internet publications and agencies (Anna News and Life News) allegedly belonging to the GRU and FSB, are massively involved in this process in Ukraine.

One of the main goals of the Kremlin's disinformation is to shift blame for alleged war crimes committed in Ukraine. For example, when a missile strike by Russian forces hit the train station in Kramatorsk on April 8, killing dozens of innocent people fleeing the horrors of war, Russia blamed Ukraine for the attack.

Some basic principles in misinformation are denial, blame, blame-shifting, and distraction (denial - distraction - blame-shifting). An example of this is the atrocities in Bucha. First, they denied it, then started saying it was provocative. They shift blame and blame Ukraine, and finally, for the distraction, they release similar sadistic videos showing Ukrainian torturers of captured Russian soldiers.

They often use coordinated email trolling operations on Telegram Cyber Front Z, allegedly linked to the "troll farm" that floods the information space with false accusations of war crimes allegedly committed by Ukrainian "neo-Nazis" to drown pro-Ukrainian voices in a sea of lies.

The main narrative of Russian propaganda is that they are not fighting the Ukrainian people but trying to liberate them from a group of neo-Nazis. Naturally, Russia also has its form of mythmaking. Still, it is far less effective since Russian state media, by law, must call the conflict a "special military operation" rather than a war.

The Russians, in 2023, passed several bills and amendments to streamline various state information registries, and the trend is for them to become increasingly closed, with no information from Western citizens available in them.

IV. Conclusions

At the strategic level, the struggle for public opinion in the information space and the protection of critical infrastructure are of utmost importance and have the potential to achieve victory or loss.

This information war proves beyond doubt to people around the world that social media platforms can be successfully used as very effective weapons of mass destruction to create unprecedented disaster in cyberspace. Critical infrastructure, government websites, and social platforms should be strategic assets like diplomacy.

The chronology of the adoption of regulations in the two countries after the start of the war shows that they aimed at securing cyber security at the beginning. Still, one of the first things to be addressed was the protection of e-government and the info security of citizens. Next, measures were taken to counter disinformation and synchronize their media, which is critical to the operation's success.

5G technologies will play a crucial role in future wars, mainly if operating against a more potent adversary with air superiority.

The war shows that the scope of information operations has gone far beyond Russia and Ukraine. It has affected the whole world. The US, NATO, China, several corporations, significant banks, NGOs, international institutions, and various professional and industry organizations, among others, are involved.

In the end, this analysis shows that Russia is currently losing the information war in the Western world and Ukraine but is having complete success in Russia itself and gaining the understanding of Chinese citizens and other isolated countries such as Iran and North Korea. There have been some partial successes in Asia and Africa, but that could quickly change because the Western powers have much better reach on social platforms like Facebook, Twitter, Instagram, YouTube, and Google.

In the end, it can be said that Ukraine has built modern and very effective cyber units, while Russia is increasingly closing itself off in the Internet space.

REFERENCES

[1] "Про Стратегію кібербезпеки України," Офіційний вебпортал парламенту України, https://zakon.rada.gov.ua/laws/show/n0003525-16#Text [accessed Feb. 28, 2024].

[2 "Про проведення в 2022 році дострокового випуску курсантів випускного курсу Інституту спеціального зв'язку та захисту інформації національного технічного університету України 'київський політехнічний інститут імені Ігоря Сікорського,'" Офіційний вебпортал парламенту України, https://zakon.rada.gov.ua/laws/show/207-2022-%D1%80#Text [accessed Feb. 28, 2024].

[3] "Про використання банками хмарних послуг в умовах воєнного стану в Україні," Офіційний вебпортал парламенту України, https://zakon.rada.gov.ua/laws/show/v0042500-22#Text [accessed Feb. 28, 2024].

[4] A. Shevtsov, C. Tzagkarakis, D. Antonakaki, P. Pratikakis, and S. Ioannidis, "Twitter dataset on the Russo-Ukrainian War," arXiv.org, https://arxiv.org/abs/2204.08530 [accessed Feb. 28, 2024].

[5] "中睿天下对俄乌网络冲突战略战术的研究分析," 知乎专栏, https://zhuanlan.zhihu.com/p/486137021 [accessed Feb. 28, 2024].

[6] [1] "Про затвердження плану заходів на 2023-2024 роки з реалізації Стратегії кібербезпеки України," Офіційний вебпортал парламенту України, https://zakon.rada.gov.ua/laws/show/1163-2023-%D1%80#Text (accessed Mar. 7, 2024).

[7] Указ Президента Российской Федерации от 01.05.2022 № 250 · Официальное опубликование правовых актов, http://publication.pravo.gov.ru/Document/View/0001202205010023?index=3&rangeSize=1 [accessed Feb. 28, 2024].

[8] "#Russia began active preparations for disconnection from the global Internet No later than March 11, all servers and domains must be transferred to the #russian zone. In addition, detailed data on the network infrastructure of the sites is being collected. pic.twitter.com/wocdrqojej," Twitter, https://twitter.com/nexta_tv/status/1500553480548892679 [accessed Feb. 28, 2024].

[9] Указ Президента Российской Федерации от 01.05.2022 № 250 · Официальное опубликование правовых актов, http://publication.pravo.gov.ru/Document/View/0001202205010023?index=3&rangeSize=1 [accessed Feb. 28, 2024].

[10] Criminal Code of the Russian Federation from 25.03.2022 http://pravo.gov.ru/proxy/ips/?docbody&nd=102041891&ysclid=l6s7e4gnxa970611260 [accessed Feb. 28, 2024].

[11] "Хронология военной спецоперации: главные события за первый месяц," Реальное время, https://realnoevremya.ru/articles/245500-hronologiya-voennoy-specoperacii-30-glavnyh-sobytiy-za-mesyac [accessed Feb. 28, 2024].

[12] "Русия започна активна подготовка за изключване от глобалния Интернет," boulevardbulgaria.bg, https://boulevardbulgaria.bg/articles/rusiya-zapochna-aktivna-

podgotovka-za-izklyuchvane-ot-globalniya-internet [accessed Feb. 28, 2024].

[13] Internet, social networks and VPN, https://www.levada.ru/en/2022/04/22/internet-social-networks-and-vpn/ [accessed Feb. 28, 2024].

[14] A. Bougias, A. Episcopos, and G. N. Leledakis, "Valuation of European firms during the Russia–Ukraine war," Economics Letters, vol. 218, p. 110750, Sep. 2022. doi:10.1016/j.econlet.2022.110750 [accessed Feb. 28, 2024].

[15] Поуки от хибридните бойни действия ..., https://postvai.com/analizi/hibridni-deistwia.html [accessed Feb. 28, 2024].

[16] Bozho, "Какво прави държавата срещу дезинформацията?," БЛОГодаря, https://blog.bozho.net/blog/3907 [accessed Feb. 28, 2024].

[17] Africans in Ukraine face racism from authorities as they escape, https://www.axios.com/africans-in-ukraine-racism-81bf8ebd-2d03-4373-bdeb-b5de9db7ec91.html [accessed Feb. 28, 2024].

[18] F. O. Talabi et al., "The use of social media storytelling for help-seeking and help-receiving among Nigerian refugees of the Ukraine–Russia war," Telematics and Informatics, vol. 71, p. 101836, Jul. 2022. doi:10.1016/j.tele.2022.101836 [accessed Feb. 28, 2024].

[19] O. B. Okooboh, "Oriana Skylar Mastro on US-china engagement and War in Ukraine," U.S.-China Perception Monitor, https://uscnpm.org/2022/04/28/oriana-skylar-mastro-russia-ukraine-china-interview/ [accessed Feb. 28, 2024].

[20] "Chinese public opinion on the war in Ukraine," U.S.-China Perception Monitor, https://uscnpm.org/2022/04/19/chinese-public-opinion-war-in-ukraine/#:~:text=To%20our%20knowledge%2C%20this%20is%20the%20first%20representative,support%20China%20mediating%20an%20end%20to%20the%20conflict. [accessed Feb. 28, 2024].