Fake News in International Conflicts: A Humanitarian Crisis in the Post-Truth Era

Fu Kwong-or Ricky†

Introduction

"World War III is coming," is it 'fake news'? On February 24, 2022, Russia launched a large-scale invasion of Ukraine, or "special military operation," three days after Russia officially recognized the Donetsk People's Republic and the Luhansk People's Republic. Shortly after the whole world witnessed the largest military conflict in Europe since World War II, a wave of misinformation soon spread widely across platforms such as Facebook, Twitter, and YouTube. From footage of military action by troops to photos of airstrikes raining down on Ukraine, observers and peace-hopers worldwide were left with deep doubts. Despite the fact that academic research has identified and conceptualized the relationship between disinformation and its erosive effect on democracy, their corresponding effects and countermeasures in international armed conflicts on such a prominent scale are unclear. Notwithstanding the thick political nature of the potential disinformation campaign taking place,[1] the following analysis seeks to examine the role that international law and media platforms play in the process of misinformation generation and dissemination. This Article focuses on the defensive mechanism against misinformation, for there is no concrete evidence of any State acknowledging and adopting any integral disinformation operation in the current armed conflict, falling short of Article 11 of the Responsibility of States for Internationally Wrongful Acts (ARSIWA).[2] Rhetorically illustrated as a football match, this Article seeks to explicate the loss in the battlefield of misinformation amid the Russia-Ukraine armed conflicts. It is argued that the *Goalkeeper*, *Midfielder*, and *Defender* all failed to perform their duties in defending the match: (1) *Goalkeeper*, the unreliable fact-checkers failed to clear the ball (misinformation); (2) *Midfielder*, the countermeasures provided under international laws failed to put a shot on combating misinformation in the current military conflict and; (3) *Defender*, the cyberspace governance strategies failed to defend the widespread misinformation in the current

† Fu Kwong-or Ricky received his Juris Doctor from the University of Hong Kong in 2022. While in law school, he worked as an academic research assistant and was a legal writer for Lexis Nexis.

1. *See generally* Irina Khaldarova and Mervi Pantti, *Fake News: The narrative battle over the Ukrainian conflict*, 10 JOURNALISM PRACTICE, 891 (2016). The author showed that there is a new media ecology which "strategic narratives are created, projected and interpreted" in the Russia-Ukraine conflicts.

2. Int'l Law Comm'n, Rep. on Responsibility of States for Internationally Wrongful Acts, U.N. Doc.A/RES/56/83 (2001) [hereinafter State Responsibility Articles].

military conflict. These three key players, namely the fact-checkers, countermeasures under international law, and State cyber governance, knit a correlated security net to safeguard the outbreak of misinformation in international armed conflicts. Such a security net provides the necessary tools for the outsiders to verify the information, take down any alleged devices disseminating misinformation, and monitor the flows of information in cyberspace:

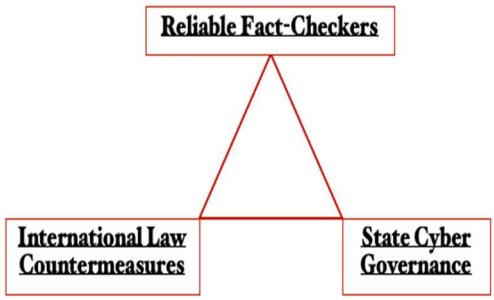

Figure: The 'security net' against misinformation

Such a net was poorly knitted in the current armed conflict. The loss in the battlefield of misinformation signified the triumph of decentralized content creation in the digital age, strengthening misbelief, and failing to defend the precious value of news reporting in our age. Moreover, the polarized political culture in the post-truth era made it difficult for the legal regime to intervene in the phenomenon of misinformation, further marginalizing the less privileged social members to evaluate the credibility of information they receive—especially those who suffered various degrees of harm under gunfire. Ultimately, any form of misinformation in international armed conflicts could potentially impose humanitarian concerns on both the nationals and refugees of the participating State. The international community should act immediately to preserve accurate news reporting in war zones, instead of amplifying speculations, by such measures as proposed in this Article.

A. Goalkeeper: The Unreliable Fact-Checkers

In the rise of misinformation, nationwide fact-checkers have adopted a mechanism to verify information suspected to be false or inaccurate by collecting online information "diffused within their national (online) public spheres to disprove false information."[3] Fact-checkers also play a central role in the battlefield of anti-misinformation campaigns worldwide; studies found

3. Edda Humprecht, *Where 'fake news' flourishes: a comparison across four Western democracies*, 22 INFO., COMMC'N & SOC'Y 1973, 1988 (2019).

that their participation increased 400% in 60 countries since 2014.[4]

In general, fact-checkers are developed by news organizations, private groups, and social media platforms such as Facebook.[5] Technically, there are various ways of detecting misinformation such as "[m]achine learning, Natural Language Processing, [c]rowd-sourced techniques, [e]xpert fact-checker, as well as Hybrid Expert-Machine[s]."[6] Apart from the private sector, scholars suggest that jurisdictions follow countries, such as Singapore, which legitimized the State as the 'ultimate fact-checker' by passing its anti-fake news law, the Protection Against Online Falsehoods and Manipulation ACT (POFMA). International organizations, such as the World Health Organization (WHO), International Center for Journalists (ICFJ), and the International Telecommunication Union (ITU) also stand at the forefront of combating misinformation by transmitting "authoritative information based on science . . . ." To this connection, larger organizations with more resources are perceived as better channels of verification. In particular, they are of the capacity to create and operate automated fact-checkers that integrate AI in the process of fact-checking, enabling quicker responses.

However, the difficulties to verify information in regional war zone arise when the channels of verification are blocked or prohibited by the parties. In this regard, apart from the centralized power, decentralized sources of verification contributing to the process may form new norms of fact-checking. Platforms such as UkraineFacts, gathering more than 400 entries from over 45 countries, enable readers to verify false information. In spite of that, such platforms mainly deal with information that contains out-of-context images and photos from previous protests or conflicts. In other words, raw information from nowhere seemingly relevant to the current conflicts is still very difficult to verify by and on these platforms.

In fact, the news authorities of the war-participating parties are also not reliable sources of news verification, making it more difficult for the fact-checkers to operate amid waves of propaganda. Observers even found that there are fake fact-checkers operated by pro-Russian groups to have framed a picture of uncertainties among the communities. On the other hand, taking the reports of the Snake Island as an example, even Ukraine officials are not sure whether the thirteen border guards were alive or dead stationing the island at the early stage of the Russian-Ukraine conflicts. At the same time, the dramatic help from Elon Musk with his company's Starlink satellite internet access station further exposed the difficulties for fact-checkers in regional war zones when internet connection or facilities are severely damaged. Whilst the information released by the authorities is doubtful,

---

4. Nguyen Vo & Kyumin Lee, *Where are the facts? Searching for Fact-checked Information to Alleviate the Spread of Fake News*, *in* 2020 CONFERENCE ON EMPIRICAL METHODS IN NATURAL LANGUAGE PROCESSING 7717, 7717(2020).

5. Edson C. Tandoc Jr., *The Facts of fake news: A Research Review*, 13 *Sociology Compass* 1, 1–2 (2019).

6. Botambu Collins et al., *Fake News Types and Detection Models on Social Media A State-of-the-Art Survey*, ASIAN CONF. ON INTELLIGENT INFO. & DATABASE SYS. 562, 573 (2020).

internet blockage and inconsistency further bring difficulties to fact-checkers and news media.

All in all, the limitations of fact-checkers are a serious problem when verifying what information outsiders see and receive. On the one hand, potential misinformation campaigns that purport to mislead audiences makes information from the local authorities doubtful; on the other, weak regulatory forces and the lack of internationally enforceable legal frameworks to combat misinformation has provided the blooming soil for widespread misinformation. This Article, therefore, argues that fact-checkers, as a goalkeeper, failed to clear the ball (misinformation), resulting in the first loss of the current match against misinformation.

B. Midfielder: International Countermeasures and their Limitations

Taking a step back from the above, there can be international countermeasures taken by States, or Ukraine in the current case, if the goalkeepers failed to clear the ball. International countermeasures, as a *midfielder*, can be taken to fight back the match through strategic plans. For instance, according to the Convention on Cybercrime (Budapest Convention), under Article 23, a State can launch investigations or proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic forms of a criminal offense. Further, under Article 22 of the State Responsibility Articles, the wrongfulness of a State's action violating international obligations would be precluded if it constitutes a countermeasure taken against another State.[7] The conditions of which are provided under Articles 51 and 52 of the State Responsibility Articles, requiring that countermeasures be proportional (*commensurate with the injury suffered*), and that notifications be sent to the responsible State, etc.[8] Further, the claimed Russian cyberattack campaign on Ukraine's civilian digital targets may raise concerns under the Geneva Convention.

The above international countermeasures, however, may be difficult to adopt in the current armed conflict. On the one hand, Ukrainian officials may not be able to find any device of a station deployed by the Russian authorities conducting the proclaimed misinformation campaign. Even worse, the information may be released directly from Russia's soil, resulting in a potential infringement of sovereignty if Ukraine has taken any actions to take down the devices. On the other hand, it is questionable whether Russian authorities would cooperate with Ukraine to take down such devices as provided under the corresponding provisions of the Budapest Convention. In such a hypothetical situation, such international countermeasures to be adopted in the present armed conflict for the only purpose of combating the dissemination of misinformation may not be proportional, and thus would be very difficult to assist the parties in resolving the problem. Yet, it must be stated that the increasingly emerging Russian disinformation narrative may

7. State Responsibility Articles, *supra* note 2.
8. *Id*.

yet be the evidence for the information war in the current conflict if it could stretch beyond mere ideological bargaining and conflicts. If that is the case, further investigation may be the most reliable defense for Ukraine in seeking international countermeasures to defend itself in the information war.

C. Defender: Cyberspace Governance and its Limitations

Stepping back from the above, even if external countermeasures are not applicable in the present armed conflict, there may as well be other measures taken internally by the State to form a robust line of defense. As the *defender*, the State's cyberspace governance can be a powerful mechanism to cope with the incidents of misinformation if they are widely spread across national media and online platforms. For instance, Singapore passed its own Protection Against Online Falsehoods and Manipulation Act (POFMA), empowering local authorities to take measures against misinformation "towards a political end." In another instance, U.S. lawmakers have been increasingly aware of the antitrust enforcement against the U.S. technology giants in recent years.

The concept of cyberspace, as adopted in this Article, connects closely with the concept of "cyber sovereignty." Such a concept provides that the State regulates its own cyberspace to protect against external interference and damage without exception. Different States may have different concerns when implementing their cyberspace defense policies. For instance, liberal democracies adopted the "multi-stake model," and authoritarian regimes based their models on stabilities concerns. In some studies, it is suggested that cyberspace does not only cover the internet, but also the societal infrastructure, such as electrical grids, water supply systems, and transportation systems. Cyberspace governance offers the State actor a place to interfere with the rising powers of technology giants and cyber-terrorism.[9] Whilst there are concerns of power abuse by the State actor, academia has increasingly conceptualized the regulatory framework applicable to prevent so, such as the concept of "data federalism." Observers further suggest that the current armed conflict signified a "focal point for contest," which advocates for global connectivity, market economies, and a global commons. From such a perspective, it is true that the robustness of cyberspace governance signifies the resilience of cyberspace in responding to outer attacks and the control of misinformation by a State.

In the present armed conflict, robust cyberspace governance can assist Ukraine in gaining back control of the information battlefield, or even any sort of cyberspace attack causing security threats. Out of surprise, observers opined that Ukraine's cyberspace governance is relatively strong, having survived a wave of destructive malware and critical infrastructure attacks. Yet, it must be stated that the opponent of Ukraine in the current conflict is Russia, a State that has been involved in countless cyber-attacks in the past

9. *See generally* Li Yan, *Global Cyberspace Governance: State Actors and the China-US Cyber Relationship*, 29 CHINA INST. CONTEMP. INT'L REL. 105 (2019).

decades, lauding itself as a cyber superpower. Empirically, Microsoft's Threat Intelligence Center detected a wave of cyberattacks directly against Ukraine's digital infrastructure as soon as the early stage of the Russian military operation on February 24, 2022. Further, from a report conducted by the Geneva Centre for Security Sector Governance in 2020, one of the threats to Ukraine's national cybersecurity is the insufficient level of protection of the country's critical infrastructure, public electronic information resources, and information. Because Ukrainian cyberspace infrastructures have been severely damaged during the armed conflict, the damages imposed a serious burden on the nation to formulate its own line of defense against military cyberattacks and the dissemination of misinformation. The *defender* failed to offer a robust defense in line with the severe attacks that the country faced.

Conclusion: What is the 'Truth' and Who is Believing It?

All in all, this Article seeks to conceptualize three lines of defenses against misinformation amid regional armed conflicts, particularly amid the largest armed conflict on European soil since the World War. It rhetorically identifies three actors and factors, labeling them as the *goalkeeper* (fact-checkers), *midfielder* (international countermeasures), and *defender* (State cyber governance). It then demonstrates how the failure of these three crucial actors resulted in the wide dissemination of misinformation in the current armed conflict. I argue that their cooperation would form a robust safety net, which not only would curb the dissemination of the misinformation, but also mitigate the resultant adverse humanitarian effects. After all, in the post-truth era, research finds that individuals would base their own judgment on pre-existing ideological beliefs when they are analyzing the truthfulness of the information before them. In the education sector, researchers are also faced with the threat that people's abilities are limited amid the spread of misinformation and denial of well-established scientific claims.[10] What is at stake in the current armed conflict is that not only that those outside of Ukraine would be misled amid the waves of misinformation, but also that those suffering from the conflict in the regional war zone cannot verify information concerning the war victims' lives and safety. The imbalanced resources of information verification further sows the seeds of fear and uncertainty, eventually causing humanitarian concerns for those trying to save the lives of victims in the armed conflicts, including the refugees. In order to win or fight back in the battlefield of misinformation in Ukraine, it takes the tide cooperation of the three actors/factors identified in this Article, namely, (1) fact-checkers, (2) international countermeasures and; (3) State cyber governance.

10. Sarit Barzilai and Clark A. Chinn, *A review of educational responses to the "post-truth" condition: Four lenses on "post-truth" problems*, 55 EDUC. PSYCH. 107, 119 (2020).