GENEVA GRADUATE INSTITUTE

ALBERT HIRSCHMAN CENTRE ON DEMOCRACY

Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression

Response to the Call for submissions: Challenges to freedom of opinion and expression in times of conflicts and disturbances.

Dr. Jérôme Duberry, Albert Hirschman Centre on Democracy, Geneva Graduate Institute
Jerome.duberry@graduateinstitute.ch

Responses below are based on the following article (in attachment): Barela, S. J., & Duberry, J. (2021). Understanding Disinformation Operations in the 21st Century. *Defending Democracies: Combating Foreign Election Interference in a Digital Age (Duncan B. Hollis & Jens David Ohlin, eds., OUP)*.

1. a) Please describe specific situations where disinformation, misinformation or propaganda have been used or restrictions have been placed on the media or access to the Internet in order to instigate, aggravate or sustain hatred, violence or conflict. What means and methods are used to manipulate information in such situations?

- Confrontational and contradictory statements: In the context of Ukraine – Russia conflict, confrontational and contradictory statements by President Putin (1) conveyed the image of an unpredictable leadership; (2) raised the level of uncertainty about the real situation on the ground (i.e., thickening the fog of war[1]) and Russia's intentions; and (3) increased tensions within and among other States. These statements inflated war preparedness narrative while denying any troop movement close to Ukraine right before the conflict.[2] This approach enabled Russia to buy time in the initial stages of the conflict (e.g., prior to the annexation of Crimea). The publication of intelligence reports by the USA was an attempt to counter this strategy prior to the invasion of Ukraine in 2022. Former NATO's Supreme Allied Commander Europe, General Philip Breedlove, described Russian's information warfare in Ukraine as "the most amazing information warfare blitzkrieg we have ever seen in the history of information warfare."[3]
- Weaponization of information on social media platforms: Disinformation campaigns on social media platforms use three main instruments: (1) spreading false news through a large number of bots—handles or accounts that automate content distribution;[4] (2) paid, organized and supervised trolls—individuals who falsify their true identities to promote discord;[5] and (3) the use of cyborgs—accounts managed by individuals but sometimes taken over by bots or that present bot-like or malicious behavior.[6] This is well-illustrated by case of the former Russian's Internet Research Agency (IRA) with staff dedicated to specific regions and countries, and social media channels.[7] The role of these professionals was to produce memes, post about fifty comments on news articles daily, manage several fake accounts and six Facebook pages, tweet at least fifty times per day,[8] and also tasked to include five pre-defined keywords in all posts to encourage search engine pickup.[9] They would play opposing roles: (e.g., post an image or a meme to defend one view, and another adding a link to contradict and fuel political discord).[10] They could also change the narrative of a false account after some time, either to

[1] James J. Wirtz, *Cyber War and Strategic Culture: The Russian Integration of Cyber Power into Grand Strategy*, *in* Cyber War In Perspective: Russian Aggression Against Ukraine 29-38 (Kenneth Geers, ed., 2015).

[2] Mason Richey, *Contemporary Russian revisionism: understanding the Kremlin's hybrid warfare and the strategic and tactical deployment of disinformation*, 16 Asia Eur. J. 101-113 (2018).

[3] John Vandiver, *SACEUR: Allies Must Prepare for Russia 'Hybrid War'*, Stars and Stripes (2014).

[4] Zi Chu, Steven Gianvecchio, Haining Wang, and Sushil Jajodia, *Detecting automation of twitter accounts: Are you a human, bot, or cyborg?*, 9 IEEE Transc. Depen. Secure Comp. 811-824 (2012).

[5] Collins English Dictionary. *available at* <https://www.collinsdictionary.com/dictionary/english/troll>.

[6] Chu *et al, supra* note 104.

[7] *One Professional Russian Troll Tells All* (Radio Free Europe broadcast 25 Mar. 2015), *available at* <https://www.rferl.org/a/how-to-guide-russian-trolling-trolls/26919999.html>.

[8] *Russia Has a Troll Army That Is Trying to Mold Public Opinion on Internet News Sites*, Higher Learning (June 4, 2014), *available at* <http://thehigherlearning.com/2014/06/04/russia-has-a-troll-army-that-is-trying-to-mold-public-opinion-on-internet-news-sites>.

[9] *Russian Troll Tells All*, *supra* note 118.

[10] *Trolling for Putin: Russia's Information War Explained*, Yahoo, 5 April 2015, *available at* <https://www.yahoo.com/news/trolling-putin-russias-information-war-explained-063716887.html>.

create confusion or to identify new potential individuals for another disinformation campaign.[11] Moreover, the Russian government also supported bloggers and individuals (outside IRA) who spread pro-Russian stories on social media networks,[12] and simulate anti-Russian news sources to disseminate false information about the ongoing conflict.[13]

- Disinformation nudges: To be successful, disinformation operations require two elements[14] : on the one hand a "kernel of truth";[15] and on the other hand include local sources to lend credibility to the narrative.[16] Lt. Gen. Pacepa offered a useful imagery to illustrate the eroding power of disinformation: "a drop makes a hole in a stone not by force, but by constant dripping."[17] Digital technologies and more precisely social media platforms now provide an incessant delivery of drops that are individually crafted to leave a mark much more quickly.
- Reconnaissance for persuasion: Persuasion tactics enable the operator to send "specially prepared information to incline [a partner or opponent] to voluntarily make the predetermined decision desired by the initiator of the action."[18] To be effective, persuasion first requires a reconnaissance phase to collect data about the targets, whether they are individuals or organizations. Thanks to this first phase of information gathering, the disinformation operators can fully exploit the vulnerabilities of the targeted populations.

1. b) What role have States, armed groups or social media platforms played to instigate or mitigate such manipulation of information?

- Disinformation to win hybrid conflicts: (dis)information is a key component of defensive and offensive strategies in inter-State and intra-State hybrid conflicts.[19] Already in 2012, President Putin and Maj. Gen. Sergei Kuralenko—former Chief of Military Art at the Academy of the General Staff— perceived information technology as a new military tool.[20] They claimed that "the development of information technologies has caused significant changes in the ways wars are fought and led to a build-up of cyber-troops."[21] This corresponds to the Russian military's understanding of the rise of a"new generation of warfare" (*voina novogo pokoleniya*), and is well-illustrated by the (mis)use of (dis)information during the Russian military annexation of Crimea[22] and the Ukraine-Russia war.
- Reflexive control: The concept of "reflexive control" adopted by Russia consists of influencing the opponents' perceptions to make them adopt positions advantageous to Russian objectives.[23] It is not new and was applied against civilians and military targets. In fact, reflexive control is an information weapon that "been studied in the Soviet Union and Russia for over 40 years." to persuade the targeted individual or group of individuals to make choices and carry out actions in the interest of the initiator.[24]

[11] *Id.*

[12] Jill Dougherty, *Everyone Lies: The Ukraine Conflict and Russia's Media Transformation*, 88 HARV. CENTER ON MEDIA 1-29 (Discussion Paper Series, 2014).

[13] See https://euvsdisinfo.eu

[14] PACEPA AND RYCHLAK, *supra* note 2, at 96 ("To ensure credibility of the lies, two things were required. First the fabrications had to appear in Western sources; and second, there had to be what Sakharosky called "a kernel of truth" behind the allegations, so that at least some part of the story could be definitely verified—and to ensure that the calumny would never be put to rest").

[15] *Id.*at 38.

[16] *Id.* at 35-6.

[17] PACEPA AND RYCHLAK, *supra* note 2, at 350.

[18] Timothy Thomas, *Russia's Reflexive Control Theory and the Military*, 17 J. SLAVIC MILITARY STUDIES 237-256 (2004); *see also* Ido Kilovaty, *Doxfare: Politically Motivated Leaks and the Future of the Norm on Non-Intervention in the Era of Weaponized Information*, 9 HARV. NAT. SEC. J. 146-179 (2018).

[19] Dave Johnson, *Russia's Approach to Conflict: Implications for NATO's Deterrence and Defense*, 111 RESEARCH DIVISION NATO 1-12 (2015).

[20] OSCAR JONSSON, THE RUSSIAN UNDERSTANDING OF WAR: BLURRING THE LINES BETWEEN WAR AND PEACE (2019).

[21] Sergey V. Kuralenko, *Changing Trends in Armed Struggle in the Early 21st Century*, MILITARY THOUGHT 29, 29-35 (2012).

[22] Rod Thornton, *The changing nature of modern warfare: responding to Russian information warfare*, 160 RUSI J. 40-48 (2015). *See also* Nye, *supra* note 46.

[23] Maria Snegovaya, *Putin's information warfare in Ukraine: Soviet Origins of Russia's Hybrid's Warfare,* 1 RUSSIA REPORT 133-135 (2015).

[24] Thomas Timothy, *Russia's reflexive control theory and the military,* J. SLA. MIL. STU. 17, 237-256 (2004).

Thus reflexive control includes a large array of tools and strategies that are based on the understanding of how the targeted individuals make their decisions. What differs today is the great capacity to collect data about the opponent, which allows the initiator of the action to know their target extremely well, and consequently make their persuasion more effective.

2. b) Where do you see major legal and policy gaps or inconsistencies on these issues? Please share your thoughts on how they could be best addressed.

- Humanitarian law tools used for regulating armed conflict are ill-fitting: In many cases, disinformation occurs below the threshold of armed conflict. It does not draw a clear line between war and peace.[25] It can be used as a tactic to prepare for a conflict, increase the fog of war with contradictory and false news. It can be present across long periods of time. In this context, humanitarian law tools used for regulating armed conflict are ill-fitting. It is essential to look to other legal paradigms to understand the type of damage that can be wrought, as well as the most effective form of regulation.[26]
- The nature of disinformation makes it difficult to detect and combat: When an operation is successful, it means that individuals have accepted the "false" narrative, which may become the main narrative (at least in part of the population). In this context, facts checking and counter narrative are not often effective. Very few people will admit indeed that they have been duped, or influenced by someone without their knowledge. Moreover, they can be difficult to reach (i.e., locked in filter bubbles and echo chambers). Lastly, how do we talk about widely shared misunderstandings that have been pushed with tiny nudges from an outside force?[27]
- Vulnerability of individuals and the importance of digital literacy: Individuals tend to be vulnerable on online platforms when it comes to detecting and combatting against mis- and dis-information. They often do not have the skills or time to verify the source of dubious information. What is more, the design of online platforms and applications make this verification more difficult, by distributing a constant information of information to users, triggering what has been referred to as fantasy of abundance.[28] In this context, digital literacy is crucial, particularly among marginalized populations.
- Limited research space: It can reveal difficult to unveil and analyze information flows within a foreign society when the research space of online social media is restricted by online platforms.

[25] Ulrik Franke, War By Non-Military Means: Understanding Russian Information Warfare (2015).

[26] *See See Steven J. Barela, Cross-Border Cyber Ops to Erode Legitimacy: An Act of Coercion, Just Security (January 12, 2017); Steven J. Barela, Zero Shades of Grey: Russian-Ops Violate International Law, Just Security (March 29, 2018); Steven J. Barela and Samuli Haataja, Rethinking Cross-Border Interference in the Disinformation Age, in Hybrid Threats In The Grey Zone: Mapping The Terrain (Milton Regan and Aurel Sari, eds., 2020)*; Jens D Ohlin, *Did Russian Cyber Interference in the 2016 Election Violate International Law?* 95(7) Texas Law Review 1579 (2017); Sean Watts, "Low-Intensity Cyber Operations and the Principle of Non-Intervention" in Cyber War: Law and Ethics for Virtual Conflicts (Jens David Ohlin, Kevin Govern, and Claire Finkelstein, eds., 2015).

[27] Barela, S. J., & Duberry, J. (2021). Understanding Disinformation Operations in the 21st Century. *Defending Democracies: Combating Foreign Election Interference in a Digital Age* (Duncan B. Hollis & Jens David Ohlin, eds., OUP).

[28] Jodi Dean, Publicity's Secret: How Technoculture Capitalizes On Democracy (2002).