# **COMBATING NUCLEAR MISINFORMATION AND DISINFORMATION** *Tools, Approaches and the Role of NGOs and International Organizations*

M. FOWLER, E. BERGNER, K. NITISA Open Nuclear Network, a programme of One Earth Future Vienna, Austria Emails: mfowler@oneearthfuture.org, ebergner@oneearthfuture.org, knitisa@oneearthfuture.org

#### Abstract

The risk of unintentional misinformation or deliberate disinformation undermining or even compromising the analysis of open source information, including scientific literature that could relate to nuclear non-proliferation, requires both an advanced technical understanding of the risk and the development and deployment of tools and approaches to counter it. Given these challenges, this paper will seek to provide an assessment of the problem, and then indicate some potential mitigating steps, including some systematic approaches that governments and organizations have taken, and also tools and platforms that can be used by analysts and others to evaluate the credibility and veracity of open source data.

## 1. THE PROBLEM OF MISINFORMATION AND DISINFORMATION

With the rapid global expansion of open source information, the risk of unintentional misinformation or deliberate disinformation undermining or even compromising the analysis of and global response to issues of nuclear non-proliferation could also be increasing, without careful awareness and measures to counter this threat. Mis- and disinformation in scientific topics and even in scientific literature could lead organizations and the public worldwide to believe objectively inaccurate or even wholly false information related to nuclear non-proliferation, ultimately leading to support for wrong-headed or dangerous policies.

## 1.1. Open Source Information Challenges

For journalists, non-profit organizations, and other institutions, accessing publicly available information is an important component of their daily work; reliance upon open source information and open source analysis methods is becoming increasingly common in order to gather and process a wide range of information. That said, in the current, ever-shifting technological environment, compiling and analysing disparate and multimodal information has become a complicated process. [1] The ever-expanding and changing volume of highly diverse, publicly accessible content adds additional and constantly shifting challenges, and can make evaluation of open source information even more complicated and cumbersome.

In addition, much of the information available in open sources is largely unverified and can include disinformation furthering concealed agendas and interests. The mere existence of such disinformation in the public sphere increases the likelihood that false information will obfuscate facts and makes objectively true information more difficult to discover and information credibility more difficult to assess. [2] As a result, fact-checking has to be at the forefront when working with any publicly available data. To ensure trust in analyses that include the use of open source information, reliability and accuracy of the open source products must be ensured, standard and transparent methods must be used, and all open sources must be fully evaluated for accuracy, bias, and credibility. [3]

Most analysis and research addressing misinformation and disinformation has focused on social media, in large part because of their scale and breadth of reach — postings can be spread by anyone, anonymously, with little to no requirement for accuracy or transparency. However, scientific and technical research work, including that relevant for non-proliferation analysis, could also be vulnerable to disinformation, even to attempts to obfuscate or mislead. While leading peer-reviewed scientific journals maintain rigorous technical review and repeatability standards, the expansion of the internet has enabled the increase of non-peer-reviewed journals and informal publishing outlets, which allow researchers and others to publish data that appear to be scientific, but fail to meet the minimum standards for quality and transparency, and could include inflated or misleading language, implicit assumptions and bias, incomplete use of citations and, in some extreme cases, fully fabricated results. Analysts consulting such scientific and technical literature in their work may acquire a misunderstanding of technical reality. Interpreting such literature without properly understanding the risks and limitations could make developing a full and accurate understanding of scientific developments impossible. Specifically for nuclear non-proliferation analysis, this could lead to flawed understanding of nuclear fuel cycle activities and related industrial capabilities and, thus, to inappropriate verification measures, such as potentially missing necessary in-field verification activities or, conversely, undertaking unnecessary ones.

#### **1.2.** Disinformation Examples

Regarding non-proliferation, in several cases disinformation campaigns have originated in seemingly independently-run editorials, which are then picked up by State-affiliated media sources running multiple stories simultaneously, perhaps to maximize exposure. These stories then reach international outlets with either friendly agendas or inattentive editorial policies and are spread around the globe. [4] The end result is that the false information becomes deeply embedded in public discourse, reappearing in subsequent discussions, despite attempts by experts to correct the narrative. For example, in 2016, disinformation was spread about the demonstrably false redeployment of US tactical nuclear weapons from Turkey to Romania. [5] If such false information is accessed by an unaware open source analyst and then used as a basis for guiding decision making, the potential for miscalculation and subsequent escalation increases considerably.

Unintended spread of misinformation due to journalists' lack of adequate specific subject matter knowledge may also affect larger credible international news media organizations. This was the case in 2017 when several large international media platforms shared a story about the official deployment of the new Chinese nuclear-armed long-range ballistic missile DF-41, which featured a still from a video of what appeared to be a missile on a transporter erector launcher vehicle. [6] Subsequent open source investigation revealed that the video footage had been shot by a civilian and shared across social media, and the missile in the image had not been verified to be a DF-41 — the design appeared to contradict certain expert estimates at the time. The claim that the Chinese Government had proclaimed its official deployment could be traced to commentary in English-language Chinese news media which expressed a desire for a prompt official announcement, but clearly stated that no such statement had been made by credible government sources. Ultimately, this example illustrated how misinformation and a lack of a use of analytical tools and methods to check open source information could lead to major misunderstandings in ordinarily high-reliability sources.

A final example highlights how poor open source analysis methodology can affect State policy. In a 2015 book on Chinese military strategy, an advisor to then-President Trump reported Chinese nuclear forces as ten times the official US estimates. The advisor appears to have accessed the numbers from a study published around 2011 by a professor at a distinguished US-based university. It was later discovered that the professor had referred to Chinese-language blog posts which cited rumours from a 1995 Hong Kong tabloid, without properly verifying the origin of the numbers. An investigation launched while the professor was researching using this false information found that the original source of the inflated numbers was a 1986 article containing several technical errors written by a young US naval officer, which had been repeatedly discredited by experts. [7] By not verifying the original data source, the professor failed to investigate with due diligence, but then was able to use his credible platform to proliferate misinformation. Unfortunately, this misinformation ended up in the hands of a US presidential advisor, who also failed to verify the professor's article and data sources, and may have used this misinformation to inform policy decisions with far-reaching consequences.

## 2. ADDRESSING MISINFORMATION AND DISINFORMATION

Fortunately, as disinformation tactics have become more sophisticated, so has the general and technical understanding of the problem. States have begun developing systematic counter approaches, which could lead to coordinated responses to such events in the future. Additionally — although mostly developed for other areas, including general open source information and journalism — the development of tools and approaches to counter disinformation has made significant advances that can be applied to the analysis of scientific and technical information and non-proliferation.

## 2.1. Government Approaches

The spread of QAnon, anti-science, and social media disinformation campaigns confirms the saying that lies spread faster than truth. This complicates responding to widespread conspiracy theories and intentional, hard-to-detect disinformation. Tech companies, governments and policymakers have been looking at broad-spectrum approaches and interventions, including media literacy education, new regulations and artificial intelligence (AI). Governments have concluded that comprehensive, systematic approaches are necessary in combating disinformation. Some notable examples include the 2016 European Union creation of a unit dedicated to countering disinformation campaigns [8]; the 2017 *Information Security Strategy* of Ukraine [9]; the US Government creation of the Global Engagement Center, focusing on countering foreign influence and sharing threat information with the private sector; and the EU 2022 *Code of Practice on Disinformation* [10] and establishment of the European Media Literacy Week [11]. Further, in March 2022, the EU Commission proposed new policies to set up united cybersecurity and information security measures in all EU institutions, bodies, and agencies. The proposal implemented a collective framework for governance, risk management, and control for cybersecurity. [12]

The global disinformation spread related to the COVID-19 pandemic showed how directly and broadly scientific-topic related disinformation can affect global policies and lead to extensive and long-lasting difficulties for governments and the scientific community. As in efforts to counter other forms of disinformation, in COVID-19 disinformation response, States have generally determined that any effective response must be systematic, active, and coordinated globally and together with private industry and the scientific community. Although similar in their systematic approach, States did develop different coping mechanisms depending on political, socioeconomic, and cultural contexts. Some State governments have expanded already-existing regulatory mechanisms or have partnered with social media such as Facebook and Twitter in an attempt to stop disinformation-spreading accounts. Other States had to begin developing these systems from scratch, often coordinating with those States that already had some relevant systems in place.

In addition to defensive actions, the global spread of COVID-19 disinformation has stimulated some governments to campaign actively against disinformation by disseminating publications, rectifications, or clarifications and introducing educational measures in primary and secondary school curricula and promoting health literacy in schools. The disinformation surrounding the COVID-19 pandemic has further demonstrated the importance for governments to establish technical credibility and public trust, and has motivated governments to use technology to bring the State and its citizens closer by establishing official communication channels on social media, such as government information on Facebook and on health ministry websites. Towards this, many European countries have been developing strategies to regain public trust in State institutions by hiring scientists to guide the communication of knowledge on COVID-19 and on precautionary measures and treatment. [13][14]

## 2.2. Trust and Technical Authority

All organizations, including government, international and non-profit ones, need a sufficient level of public trust in order to succeed in their policies and to achieve their goals. In today's highly polarized environment, understanding and handling trust is more significant than ever for an organization to keep its licence to function, lead, and flourish, knowing how the public sector can strengthen this valuable asset. [15] Several theories exist on how trust can be gained. For example, the rational trust theory — measuring how NGOs achieve competence and meet objectives in their contract with donors — increases perceptions of NGO integrity and credibility. [16] Moreover, trust also has a social aspect. Shared identity and common values, membership of a group or community, and a desire to work towards common goals might provide higher perception of trustworthiness though familiarity, for instance, forming a similar identity and political solidarity that can be established by strategic and transparent communication to the public. [17] Perceptions of benevolence and integrity are as important in engendering trust as are perceptions of ability; therefore, both rational and social components of trust are important. [18] The social aspect of trust necessitates ethical behaviour — transparency and validity of sources used for published material open to the public is therefore a requirement.

To establish and maintain public trust, NGOs and international organizations working on nuclear nonproliferation must ensure that they use all best analytical practices, tools, and methods and that they reliably identify disinformation in their analyses. All published analysis products should meet the high standards needed to ensure the organization's reliability regardless of the amount of subject-related mis- or disinformation circulating in the internet. Further, NGOs and international organizations should strengthen the trust that they have gained in their technical authority and acknowledge that trust by actively participating in countering misand disinformation. Actions these organizations could take include contributing scientific analysis to or even partnering with established, credible fact-checking entities. [19] Moreover, NGOs and international organizations could actively identify mis- and disinformation they have assessed, and provide the public and media with suggestions for more credible information alternatives. Approaches focusing on collaboration, such as the EU initiatives, could be taken by NGOs and international organizations in the non-proliferation community to debunk disinformation and to provide verified information for the public. If an organization cannot initiate such a project, partnering with top fact-checking organizations, such as *Bellingcat*, *PolitiFact* or the UN initiative Verified, could be a solution to ensure that scientific analyst expertise is combined with skilful fact-checking.

#### 2.3. Tools and Methods

While very few tools and methods specific to investigating scientific literature in open sources are available, an abundance of practical tools exist aimed at combating general open source dis- and misinformation, particularly for use with news media. These tools vary and can be web-based, optimized for mobile phone platforms, databases, browser extensions, or source labels (or other 'fact-checked' tags). [20] Although developed for general news media or open source information, they can be applied by the non-proliferation community to facilitate countering scientific and technical dis- and misinformation.

#### IAEA-CN-303-269

In addition to the use of tools, sound analytical methods are critical to working with open source information. As with any information, in evaluating scientific literature, the analyst should first evaluate the quality and credibility of the information source itself — is the paper presented in a reputable publication with high peer review standards? Is the institute/researcher that authored the publication well established in that scientific discipline? Is the source of funding for the investigation transparent, and are all conflicts of interest and assumptions explicit? Is the hosting location of the study a verified source — for example, the institute's official website, as opposed an unofficial website or social media?

Once the information source has been thoroughly investigated, the analyst can then move on to evaluating the data contained in the information item; this step can be increasingly complicated in scientific literature, and may require consultation with professionals with relevant expertise. Initial information evaluation can be assisted by some technology tools, such as those able to recognize information of questionable origin or credibility, including information which may have been altered or fabricated. Some AI applications can perform such tasks, using machine learning and natural language processing to rapidly process large quantities of data and compare new information to established source and information credibility models. Some AI tools are assisted by human support to further increase veracity, both through active machine learning and manual source credibility assessments.

### 2.3.1. Disinformation Detection

Tools currently available to easily understand how a particular information item has proliferated are diverse in their function and application and are used primarily in the evaluation of news articles. They could, conceivably, also be used to determine the proliferation of scientific articles. Thus, nuclear non-proliferation analysts could determine the source of disinformation and, thereby, increase the confidence with which they can identify information not based in fact, and ensure that information used for policy proposals is correct. As disinformation campaign strategies continue to evolve, continuous use of tools for training in detection is important. [21] Likewise, gaining an understanding of differences in misinformation proliferation is important, as they require unique approaches. The limitation of such tools is human error as, finally, it is up to the user to benefit from lessons learned and identify the dissemination patterns of dis- and misinformation.

While there are sophisticated AI systems trained to detect text-based hate speech and image manipulation detection algorithms that discern disinformation as it emerges on social media, these algorithms are often isolated from one another and, therefore, cannot easily detect, for instance, complex disinformation that combines both text and images. Researchers have yet to discover systems advanced enough to detect coordinated disinformation campaigns triggering confirmation biases, such as memes. If solely semantic analysis is not enough to discern whether content contains a manipulated image, audio, hate-speech, or meme, AI systems will need to perceive disinformation in, for example, history, humour, symbolic reference, and inference. [22]

### 2.3.2. Information Origin Tracing

Another set of tools can be used for the subsequent step of tracing the origin of information, with different tools adapted to textual or visual data. Tracing the origin of the information, as opposed to examining the veracity of the initially-encountered account, provides an opportunity to evaluate the original news item free of modification and interpretation. It may also provide an indication of whether the item appears to be part of an orchestrated disinformation campaign or a case of unintended misinformation.

Photographs can be traced through using tools that enable reverse image search to find the original posting. These tools may also enable insight into whether the image has been modified during its travel from the initial source. Tracing the origin of a video functions in a similar manner, with tools providing relevant metadata and the ability to reverse image search through the creation of thumbnails of the video content. [23] The origins of text are more difficult to trace and verify, particularly as the wording of the same information may differ between articles. A combination of Google search tools and manual key word entries to follow the news items upstream to the original source remains the most straightforward approach. [24]

A separate set of tools tracks the mass-circulation of disinformation in social media and can be used to discover the origin of a post and the mode of dissemination — whether human or bot. Bots are software applications that run automated tasks emulating human activity on the internet. On social media, these can be used to coordinate amplification of misinformation from inauthentic accounts at a speed that greatly exceeds human ability. The presence of bot activity may indicate intentional disinformation dissemination. Different tools offer the option to either detect and block bot-operated accounts [25] or visualize the spread of a certain piece of information. [26]

#### 2.3.3. Accuracy Evaluation

A third set of tools assists with the verification of information contained in an open source item. The purpose of these tools is to provide users with an indication of the likely factual correctness of specific news items, news platforms, or government statements and reports.

Credibility scoring and fact checking are offered by a variety of tools using different methods. [27] Certain tools rely on human intelligence, either through votes from general users to establish the likely level of credibility or through inaccuracy checks conducted by scientists or researchers, who may also annotate and add context to the information. Other tools rely on a combination of human fact checkers with technology such as blockchain to provide credibility scoring and bias checking of the original source and information, and then to track the information dissemination to ensure authenticity. There are also tools initiated by online media publishers to encourage high journalistic standards, for which an outlet may be provided with a certificate to display on its website. [28] Furthermore, several larger news media platforms work increasingly proactively to counter dis- and misinformation and offer fact-checking services that are open to the public. [29] The main limitation of some of these tools is the time required for accuracy evaluation, in particular if conducted by human fact checkers. However, since several of these tools target media platforms in addition to specific articles, they may still be relevant for recent news items originally posted on those platforms.

For visual media verification, digital image forensics offers an opportunity to establish the authenticity of an image, or of the claim related to the image. Certain tools can provide metadata, such as timestamp and geolocation of the original photograph, which allows the user to test if the time and place match the claims made in the article. Other tools may detect manipulation of the photograph through the use of, for example, magnifying functions, clone detection, and error level analysis. [30]

In evaluating data, analysts must ensure that their own search tools and methods do not themselves introduce bias, for example, through the creation of a filter bubble, in which a user is presented with a limited set of information due to customization filters. [31] One approach that attempts to solve this problem is to create a complete replication of all relevant data, in which an organization can gain unbiased and unfiltered access to the data. This, however, is generally impractical as it would require large-scale information collection and management efforts, extensive information integration and access development work and, likely, more effort and cost than the task may require. Instead, smaller and more straightforward solutions to the filter bubble problem include the use of incognito modes, as available, or search engines or other tools that neither track user data nor customize results. [32] Even these efforts, however, can create a burden for the analyst, as they limit some otherwise helpful tool functionality or reduce the amount of data made available. Therefore, to deal with ever-increasing amounts of data, the analyst and organization will need to find a balance in the use of such tools and in developing appropriate methods to ensure that any such negative side-effects, such as filter bubbles, are addressed and that proper caveats are included in any conclusions drawn from the data.

While analysts, data scientists, and science communicators have developed various software and platforms to counter mis- and disinformation, those countermeasures require analyst awareness and consistent use, and are not widely disseminated among the public. While it may be a relatively simple task for a trained information analyst to assess the accuracy and authenticity of data using such tools and methods, that same data may be widely circulated before any fact-checking has been conducted. Once a false report has spread through the internet, the challenge of correcting the misunderstanding can be insurmountable, especially as the global public do not have the training, time, or inclination to rigorously fact-check every news item.

#### 3. CONCLUSION

Open source misinformation and disinformation can affect the analysis of news items and scientific literature, including that related to nuclear non-proliferation. The impacts could include for example, the misunderstanding of a nuclear fuel cycle activity, resulting in ineffective, inaccurate, or even harmful verification implementation. Due to incorrect understanding of technical realities, bad analysis could even influence organizational-level policies or actions. Further, the general public could form incorrect conclusions based on bad open source information related to nuclear non-proliferation, which could also result in organizations adopting poorly formed or damaging policies.

To counter these negative effects of disinformation and misinformation related to nuclear nonproliferation, organizations should consider possible actions to ensure appropriate treatment of information at both the organizational level and the individual information analyst level.

At the highest levels, organizations should consider the systematic approaches to disinformation that many governments have taken to address the most serious problems. Organizations should note that these examples demonstrate that no single organization can deal with disinformation or misinformation alone but, instead, they must work with other interested parties, private industry, and the public. Also, establishing and maintaining trust and technical authority are required in order to reach the public and discredit disinformation. Further,

organizations that have established technical credibility should find ways to use that credibility to assist the public in clarifying disinformation and misinformation.

At the level of analysts, organizations must ensure that open source information is always addressed in the most professional, transparent, and accurate manner possible. Sources and data must be thoroughly evaluated using appropriate tools and methods, and analytical findings should always be properly caveated given the uncertainties inherent in the use of any open source information. All analysts working with open source information should make efforts to detect disinformation, and to trace and understand its origins, and should thoroughly evaluate the accuracy of both the source itself and of the data contained in the related publication.

## REFERENCES

- DOKMAN, T., IVANJKO, T., Open Source Intelligence (OSINT): issues and trends, INFuture2019: Knowledge in the Digital Age, January 2020, available at: <u>10.17234/INFUTURE.2019.23</u>.
- [2] DOKMAN, T., IVANJKO, T., Open Source Intelligence (OSINT): issues and trends, 7th International Conference The Future of Information Sciences INFuture2019: Knowledge in the Digital Age, January 2020, available at: <u>10.17234/INFUTURE.2019.23</u>.
- [3] MERCADO, S. C., Reexamining the Distinction Between Open Information and Secrets, Central Intelligence Agency, 18 June 2009, available at: https://reusersinformationservices.com/etc/Literature/Reexamining%20the%20Distinction...pdf.
- [4] MEYER, S., Fake News, Real Consequences: The Dangers of WMD Disinformation, NTI, 7 December 2017, available at: <u>https://www.nti.org/analysis/articles/fake-news-real-consequences-dangers-wmd-disinformation/</u>.
- [5] MEYER, S., Fake News, Real Consequences: The Dangers of WMD Disinformation, NTI, 7 December 2017, available at: <a href="https://www.nti.org/analysis/articles/fake-news-real-consequences-dangers-wmd-disinformation/">https://www.nti.org/analysis/articles/fake-news-real-consequences-dangers-wmd-disinformation/</a>.
- [6] KULACKI, G., Fake News about Chinese Nuclear Weapons, All Things Nuclear; Union of Concerned Scientists, 13 February 2017, available at: <u>https://allthingsnuclear.org/gkulacki/fake-news-about-chinese-nuclear-weapons/</u>.
- [7] KULACKI, G., Fake News about Chinese Nuclear Weapons, All Things Nuclear; Union of Concerned Scientists, 13 February 2017, available at: <u>https://allthingsnuclear.org/gkulacki/fake-news-about-chinese-nuclear-weapons/</u>; KULACKI, G., Research in the Internet Age: Karber and China's Nuclear Arsenal, All Things Nuclear; Union of Concerned Scientists, 30 November 2011, available at: <u>https://allthingsnuclear.org/gkulacki/research-in-theinternet-age-karber-and-chinas/</u>; KULACKI, G., The Sources of Karber's Sources, All Things Nuclear; Union of Concerned Scientists, 7 December 2011, available at: <u>https://allthingsnuclear.org/gkulacki/the-sources-of-karberssources/</u>.
- [8] The Henry M. Jackson School of International Studies, University of Washington, Countering Disinformation: Russia's Infowar in Ukraine, 25 October 2017, available at: <u>https://jsis.washington.edu/news/russiadisinformation-ukraine/# ftn29</u>.
- [9] National Security and Defense Council of Ukraine, On Information Security Strategy, 15 October, 2021, available at: <u>https://zakon.rada.gov.ua/laws/show/685/2021#Text</u>.
- [10] European Commission, 2022 Strengthened Code of Practice on Disinformation, Shaping Europe's Digital Future, 16 June 2022, available at: <u>https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practicedisinformation</u>.
- [11] European Commission, European Media Literacy Week, Shaping Europe's Digital Future, 30 March 2020, available at: <u>https://digital-strategy.ec.europa.eu/en/events/european-media-literacy-week</u>.
- [12] European Commission, New rules to boost cybersecurity and information security in EU institutions, bodies, offices and agencies, 22 March 2022, available at: https://ec.europa.eu/commission/presscorner/detail/en/IP\_22\_1866.
- [13] RANGEL SANTOS, M. L., et al., Government actions to address the disinformation crisis during the COVID-19 pandemic, Saúde em Debate, December 2021, available at: https://www.scielo.br/j/sdeb/a/wKn8xnMVLyXB3MMzX93674R/?format=pdf&lang=en.
- [14] POMERANZ, J. L., SCHWID, A. R., Governmental actions to address COVID-19 misinformation, Journal of Public Health Policy 42, June 2021, available at: <u>https://doi.org/10.1057/s41271-020-00270-x</u>.
- [15] TORY, M., The Nonprofit Sector Has a Unique Opportunity to Build Public Trust, Dorothy A. Johnson Center for Philanthropy, 19 January 2021, available at: <u>https://johnsoncenter.org/blog/the-nonprofit-sector-has-a-unique-opportunity-to-build-public-trust/</u>.
- [16] KEATING, V. C., THRANDARDOTTIR, E., NGOs, trust, and the accountability agenda, The British Journal of Politics and International Relations, January 2017, available at: <u>https://www.researchgate.net/publication/311632477\_NGOs\_trust\_and\_the\_accountability\_agenda</u>.
- [17] The 2022 Edelman Trust Barometer, 2022, available at: https://www.edelman.com/sites/g/files/aatuss191/files/2022-01/2022%20Edelman%20Trust%20Barometer%20FINAL\_Jan25.pdf.
- [18] MAYER, R. C., et al., An Integrative Model of Organizational Trust, The Academy of Management Review, July 1995, available at: <u>https://doi.org/10.2307/258792</u>.
- [19] See for example the UN initiative "Verified", available at: <u>https://shareverified.com</u>; "PolitiFact" and "Snopes", focusing on US news media, available at: <u>https://www.politifact.com</u> and <u>https://www.snopes.com</u>; international news media: "Reuters Fact Check" and "BBC News Reality Check", available at: <u>https://www.reuters.com/fact-check</u> and <u>https://www.bbc.com/news/reality\_check</u>.

#### IAEA-CN-303-269

- [20] For an extensive list of tools that fight misinformation online, accompanied by short descriptions of technology used and aim of the tools, see RAND Corporation's database, "Tools That Fight Disinformation Online": <u>https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html</u>.
- [21] Most highly recommended: "Workshops" at Bellingcat, available here: https://www.bellingcat.com/workshops/.
- [22] YANKOSKI, M., SCHEIRER, W., WENINGER, T., Meme warfare: AI countermeasures to disinformation should focus on popular, not perfect, fakes, Bulletin of the Atomic Scientists, 11 May 2021, available at: <u>https://doi.org/10.1080/00963402.2021.1912093</u>.
- [23] Recommended tool for image and video tracing and forensics: "InVID Verification Plugin", available at: <a href="https://www.invid-project.eu/tools-and-services/invid-verification-plugin/">https://www.invid-project.eu/tools-and-services/invid-verification-plugin/</a>; "RevEye Reverse Image Search", available at: <a href="https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf?hl=en">https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf?hl=en</a>.
- [24] Recommended detailed tool guides for information tracing and accuracy evaluation: HIGGINS, R., A Beginner's Guide to Social Media Verification, Bellingcat, 1 November 2021, available at: <a href="https://www.bellingcat.com/resources/2021/11/01/a-beginners-guide-to-social-media-verification/">https://www.bellingcat.com/resources/2021/11/01/a-beginners-guide-to-social-media-verification/</a>; CAULFIELD, M., Web Literacy for Student Fact-Checkers, Pressbooks, 8 January 2017, available at: <a href="https://webliteracy.pressbooks.com/">https://webliteracy.pressbooks.com/</a>; URBANI, S., Verifying Online Information, First Draft, October 2019, available at: <a href="https://webliteracy.pressbooks.com/">https://webliteracy.pressbooks.com/</a>; URBANI, S., Verifying Online Information, First Draft, October 2019, available at: <a href="https://webliteracy.pressbooks.com/">https://webliteracy.pressbooks.com/</a>; URBANI, S., Verifying Online Information, First Draft, October 2019, available at: <a href="https://firstdraftnews.org/wp-">https://firstdraftnews.org/wp-</a>
- content/uploads/2019/10/Verifying Online Information Digital AW.pdf?x75440.
- [25] See "Bot Sentinel", available at: <u>https://botsentinel.com/twitter/get-started</u>.
- [26] See: "Hoaxy", available at: <u>https://hoaxy.osome.iu.edu/#query=nuclear&sort=recent&type=Twitter&lang=</u>.
- [27] Recommended detailed tool guides for information tracing and accuracy evaluation: HIGGINS, R., A Beginner's Guide to Social Media Verification, Bellingcat, 1 November 2021, available at: https://www.bellingcat.com/resources/2021/11/01/a-beginners-guide-to-social-media-verification/; CAULFIELD, M., Web Literacy for Student Fact-Checkers, Pressbooks, 8 January 2017, available at: https://webliteracy.pressbooks.com/; URBANI, S., Verifying Online Information, First Draft, October 2019, available at: https://firstdraftnews.org/wpcontent/uploads/2019/10/Verifying\_Online\_Information\_Digital\_AW.pdf?x75440.
- [28] See RAND Corporation's database, "Tools That Fight Disinformation Online", filter: "fact-checking", available at: https://www.rand.org/research/projects/truth-decay/fighting-disinformation/search.html#q=fact-checking.
- [29] For examples, see: "Reuters Fact Check", available at: <u>https://www.reuters.com/fact-check;</u> "BBC News Reality Check", available at: <u>https://www.bbc.com/news/reality\_check</u>.
- [30] Recommended tool for image and video tracing and forensics: "InVID Verification Plugin", available at: <u>https://www.invid-project.eu/tools-and-services/invid-verification-plugin/;</u> "RevEye Reverse Image Search", available at: <u>https://chrome.google.com/webstore/detail/reveye-reverse-image-sear/keaaclcjhehbbapnphnmpiklalfhelgf?hl=en;</u> "Image Verification Assistant", available at: <u>https://mever.iti.gr/forensics/</u>.
- [32] Recommended tool (website and chrome extension): <u>https://duckduckgo.com/</u>.