#DISINFO2023

EU DISINFO LAB

ANNUAL CONFERENCE

2023

EU DISINFOLAB 2023 CONFERENCE DOSSIER

This Dossier summarises some of the sessions held during the EU DisinfoLab 2023 Annual Conference, which took place on 11 and 12 October 2023 in Krakow, Poland. Over the two days, dozens of experts from the counter-disinformation community shared their expertise on stage with hundreds of participants, and this document comes as a result. This Dossier aims to recap the most salient moments of the conference to build a legacy of what has been discussed, exchanged, and learned. The next pages merely reflect the position of the speakers on the various topics that, given the nature of the conference, are not necessarily exhaustive or equate to an endorsement.

This Dossier is authored by conference rapporteurs **Ani Tsintsadze**, **Arzu Bunyad**, **Gabor Enekes**, and **Irina Gutu** from the College of Europe in Natolin. EU DisinfoLab thanks them, as well as **Mr. Adam Reichardt** and **Mr. Alvaro Garrote Fuentes**, for their contributions.

TABLE OF CONTENTS

THE INCREDIBLE JOURNEY OF A RECOVERING CONSPIRACIST	4
THE TRUTH IS NON-NEGOTIABLE	6
WHAT RUSSIA-UKRAINE TEACHES US ABOUT ATTENTION AND WARFARE	8
EMERGING REALITIES: AI'S IMPACT ON TRUTH, DISINFORMATION, AND OUR PERCEPTION OF REALITY	10
PANORAMA: CASE STUDIES OF MODERN DISINFORMATION	12
IT'S THE ATTENTION ECONOMY, STUPID!	14
TRANSPARENCY PARADOX: HOW CAN DATA KEEP US BOTH INFORMED AND CONFUSED	18
PROACTIVE STRATEGIES FOR PREVENTION & RESPONSE	20
ACTIVATE THE POTENTIAL OF PLATFORM DATA	22
RUSSIAN WAR: A TIPPING POINT TO ACT AGAINST FOREIGN INTERFERENCE?	24
FROM CLICKS TO CLUES: AN ONLINE INVESTIGATION WORKSHOP	26
SHIFTING LENSES: DISINFORMATION FROM A DIFFERENT ANGLE	28
REGULATORY UPDATE & PANEL DISCUSSION	30
HOW DO WE KEEP THE FAITH?	32

THE INCREDIBLE JOURNEY OF A RECOVERING CONSPIRACIST

Chair:
Diana Wallis (President, EU DisinfoLab)

Interviewee:
Brent Lee (Podcast host, "Some dare call it a conspiracy")

Brent Lee's journey as a conspiracist started in 2003 with his curiosity sparked by documentaries on the 9/11 attacks. This later led him to become deeply immersed in conspiracy theories, and after some time, he became convinced that the Twin Towers' destruction was an inside job. Lee ended up believing that external actors, such as secret societies, criminal networks and cults, were ruling the world and orchestrating the global system.

Lee became active in online communities around 2005 when social media was starting to be a hub for digital communities, including those connecting over a shared belief in conspiracy theories. To evidence the lengths that these convictions would go, Lee recounted the idea that the firstborn of Prince William of England and Kate Middleton was the anti-Christ, whose birth would cause the apocalypse.

Today, he questions how he could have ever taken such an extreme fantasy seriously. However, at the time, he said that while the people around him avoided such divisive topics, these were the only things he cared to discuss. As a result, he isolated himself: "They did not leave me, I left them".

The Sandy Hook Elementary School shooting in 2012 marked a major turning point for Lee. Even though he was initially intrigued by claims that the incident was a hoax with crisis actors, he later began to question the narrative that presumed all such attacks were hoaxes. After witnessing real-world events like the rise of Donald Trump and Brexit, he considered that these occurrences contradicted the conviction that a powerful elite could oppose the election of the 45th US President or the detachment of the UK from the EU. Against his belief that leaders were 'selected' and not 'elected', he realised that votes and referendums had power and democracy was not a scam.

After recovering from this problematic past and understanding that the main motive is distrust, Lee now aims to share his experience as a former conspiracist to help others who are going through a similar journey. Brent hosts a podcast titled "Some dare call it conspiracy", where he examines conspiracy theories and helps to explain and demystify them. In his interview, Lee emphasised that it is essential to be aware that even well-informed individuals can fall prey to conspiracies and disinformation. Moreover, people's journey with conspiracy theories is deeply individual; this applies to believing in and recovering from them.

THE TRUTH IS NON-NEGOTIABLE

Chair:
Diana Wallis (President, EU DisinfoLab)

Interviewee:
Emma Le Mesurier (EU DisinfoLab Board Member)

The interview with Emma Le Mesurier delved into the complexities of truth in today's digital age. Emma highlighted her efforts to combat the spread of mis- and disinformation against the White Helmets, rescue organisation in Syria, and against her late husband, James Le Mesurier.

The White Helmets' life saving work and documentation of war crimes in the polarised Syrian war made them, and James – their greatest advocate – a prime target for physical attacks and a vast state-sponsored disinformation campaign. His sudden, tragic death, and its aftermath further emphasised the risks they undertook. Conspiracy theorists targeted Emma and James, accusing them of financial misconduct and speculating about the nature of James' disappearance. A Turkish criminal investigation and a forensic financial investigation cleared her of all wrongdoing but the trail of allegations left their stain.

Emma advocates for the singularity of objective truth. In states of incomplete information and understanding, many perspectives exist simultaneously. These perspectives are not, however, synonymous with the truth. In situations of competing narratives, especially where one or multiple sides deliberately seek to distort reality, the truth is not a "compromise solution" to be found in the middle. Journalistic balance no longer applies when one side is lying. Unfortunately, in journalists' hunger for personal recognition and commercial media outlet's ruthless competition for a share of the public's consciousness, they often blur the boundaries between reality and fiction. Social media distribution can meanwhile amplify specific, often false, narratives. When algorithms prioritise content based on user engagement, they can unintentionally boost these misleading stories. As more people interact with a narrative, it gains undue prominence, further distorting the truth.

A reason for this is that people tend to search for simple explanations when faced with complex situations: lacking a clear and accessible cause to explain James' death, many questioned his integrity. They resorted to conspiracy theories claiming his involvement in fraudulent activities. The media plays a pivotal role in the information ecosystem, but it can also contribute to information disorder. Emma described how the Dutch newspaper De Volkskrant published false and misleading information about James and her after being led by an individual who was morally culpable, and seeking to exculpate himself, for James's death. She sought the removal of the publication after De Volkskrant's investigation had been debunked and discredited by the BBC, The Guardian, De Groene Amsterdammer and Der Spiegel, but they resisted each effort. She encountered numerous hurdles, including a weak Dutch regulator made of up industry professionals as well as complex, and prohibitively expensive, legal procedures.

In a world of misinformation, finding the truth becomes a formidable challenge. The media's influence on public perception is undeniable, highlighting the need to differentiate between fact and fiction. The story of Emma and James serves as a powerful testament to this ongoing struggle and the unwavering pursuit of genuine truth.

WHAT RUSSIA-UKRAINE TEACHES US ABOUT ATTENTION AND WARFARE

Chair:
Maria Giovanna Sessa (EU DisinfoLab)

Speaker:
Emerson Brooking (Digital Forensic Research Lab, DFRLab)

During this session, Emerson Brooking from the DFRLab discussed the evolution of the Russia-Ukraine conflict and focused on the intersection between warfare and digital spaces. On 24 February 2022, the world witnessed the first photographic evidence of intervention, marking a viral event that underscored the powerful role of attention in modern warfare. In this era, wars are fought on the battlefield and in the digital space, where the attention of the global populace is a coveted prize and "attention is all you need."

However, attention is not constant but has a half-life, characterised by "lower highs and lower lows", reflecting its transient and evolving nature. As the war progressed, events like the Bucha massacre demonstrated that "attention demands novelty". In this era, the most shared news often involved lone-wolf heroes or recognisable celebrities, indicating a disconnect where "novelty is not reality".

"Maintaining attention takes capacity", Brooking emphasised, citing the extensive efforts of Russian propaganda in building compelling narratives. This investment in time and resources highlights a profound revelation: disinformation struggles to permeate the public consciousness when organic engagement is high. "You can have it all, just not at once", he cautioned.

A compelling observation followed: this is not only a war for attention but also a war of attrition. While Ukraine seeks continued global focus, Russia has been isolated yet remains potent in the long-term narrative battle. As attention recedes, disinformation thrives, a phenomenon evident in cases like the White Helmets, where disinformation actors found spaces to plant and nurture alternative narratives.

Ukraine will likely emerge as a focal point as the world steers towards the EU elections and beyond. Brooking warned of Russia's anticipated efforts to gain an advantage amidst global distractions. In this complex dance of narratives, companies and media tend to whitewash news, further complicating the landscape of truth and information.

Brooking concluded with reflections on the American civil society's response to Russia's unprovoked attack as an illustration of the organic support base that remains a bulwark for Ukraine and the West against authoritarian forces. This illuminates a reality where the battle for attention is not just about quantity but quality, authenticity, and the organic resonance of narratives in the hearts and minds of the global populace.

The keynote was a poignant reminder of the multifaceted nature of modern warfare, where keyboards and screens are as powerful as guns and tanks and where attention can shape the tides of war and peace.

EMERGING REALITIES: AI'S IMPACT ON TRUTH, DISINFORMATION, AND OUR PERCEPTION OF REALITY

Chair:
Susan Morgan (Independent Consultant)

Speakers:
Thomas Gouritin (AI expert)
Noémie Krack (KU Leuven)
Tyler Williams (Graphika)
Beth Lambert (Logically)

As a diverse tool, AI has become a central element in the general discourse on disinformation and misinformation. Hence, the exploration of the technology's potential and threats in a specific panel.

In his opening speech, Thomas Gouritin, AI expert, consultant, and trainer, outlined the background of how large language models (LLM) like ChatGPT work. Gouritin warned that one of the main problems is that we do not know what kind of datasets these LLMs have been trained on. This can be dangerous as these models "operate like stochastic parrots", meaning they are good at generating convincing language but do not understand the meaning of the language that they process. As a result, they can easily create biased or misleading content by repeating the language used for their training. Gouritin added that AI tools can be useful in content analysis, but content generation should be treated with increased caution for the abovementioned reasons.

Tyler Williams from Graphika highlighted the trend of AI-generated deceptive content becoming more accessible through various apps, making it easier to create fake or misleading content. The challenge lies in detecting fake content, especially when it blends real and counterfeit elements across video, audio, and text formats. In this evolving landscape, the critical concern is not only the generation of entirely fake content but also the blending of real and fake elements, making it essential to develop robust methods for detecting such mixed content. At the same time, debunking must be used more heavily as well.

Beth Lambert from Logically emphasised that AI exacerbated existing issues rather than creating new ones. One of the most relevant examples is a tool called 'CounterCloud', which displayed how easily AI can mass-produce disinformation without human interaction. Lambert also noted that each country has unique disinformation narratives involving distinct actors and vulnerabilities, often influenced by foreign interference. A significant challenge is that AI-generated content led to an information environment dominated by quantity over quality, further polluting the media landscape.

Noémie Krack from KU Leuven presented AI's horizontal and vertical impact on our lives and examined the European Union's approach to addressing these challenges. She outlined various EU strategies, such as relying on existing rules, amending them, or introducing new legislation like the AI Act. She underscored the significance of the Digital Services Act (DSA), which contains provisions concerning algorithms, automated systems, crisis protocols, and addressing systemic risks, especially disinformation. The critical issue at hand is the rapid development of technology compared to the slower pace of legislation. Krack also stressed the need for horizontal regulation across various sectors and applications, emphasising identifying the origin of content. Finally, she called for increased AI literacy campaigns to ensure that experts and end-users take responsibility for effectively managing AI's impacts.

PANORAMA: CASE STUDIES OF MODERN DISINFORMATION

Chair:
Maria Giovanna Sessa (EU DisinfoLab)

Speakers:
"Disinformation trends and case studies":
Aleksy Szymkiewicz (Demagog)
Alejandro Romero (Constella Intelligence)
Cristina López G. (Graphika)

"Forbidden Stories – the 'Story Killers' project: a review of these investigations into disinformation":
Phineas Rueckert (Forbidden Stories)
Christo Buschek (Der Spiegel / Paper Trail Media)

The session was moderated and introduced by Maria Giovanna Sessa, who presented some preliminary results for a project supported by the Friedrich Naumann Foundation for Freedom, consisting of the collection of country factsheets highlighting the disinformation landscape across EU member states. In particular, she focused on the most recurrent deceptive narratives, i.e., health, migration, institutional distrust, the Ukraine war, and climate.

Aleksy Szymkiewicz introduced Demagog's 'Climate Factbot', an educational chatbot designed to serve as a virtual assistant for climate-related inquiries. The project had an impressive repository of 70 climate-related articles, which formed the basis for a comprehensive database containing 400 questions and answers.

Alejandro Romero delved into the critical distinctions between information operations, disinformation, and hybrid threats. Romero highlighted the increased significance of disinformation on the global agenda, citing the World Economic Forum's Global Risks Report 2023. He also underlined the need to integrate cyber and AI capabilities into open-source intelligence analysis to counter disinformation effectively.

Cristina López G. explored the harassment dynamics in the online space with evidence from the Taylor Swift fan community. The fan-driven speculation surrounding Swift's 'Midnights' album led to a deep division in the singer's fandom, notably involving a theory about hidden messages in her work about her queerness. Graphika's research revealed the existence of factions within the fandom. "The various narratives these communities are defending become a big part of their online identity", López said, noting how this case study reflects the operational dynamics in various online communities.

Phineas Rueckert presented the 'Story Killers' project, which unveiled the grim reality faced by journalists confronting disinformation. As an example, he mentioned Gauri Lankesh, who was killed before publishing her new editorial. Rueckert delivered a powerful message, stating, "Killing the journalist won't kill the story," encapsulating truth-seekers' resilience. He warned the audience of the deadly consequences that journalists face as states increasingly turn to disinformation-for-hire services and these mercenaries proliferate.

Continuing with the 'Story Killers' project, Christo Buschek ventured into the secret world of 'Team Jorge', an Israeli company well-versed in employing malicious cyberactivities and orchestrating social media disinformation campaigns. Forbidden Stories and its partners meticulously monitored Jorge's activities for over six months, unearthing the elusive group. Team Jorge wields a variety of tools, including the Advanced Impact Media Solutions (AIMS) software package, which they use to interfere with elections. Undercover journalists, posing as prospective clients, revealed insights into Jorge's operations and recorded their interactions with the group's leader, Tal Hanan.

On Twitter, AIMS disseminated tweets supporting campaigns involving many individuals in over 25 countries. Account verification relies on fact-checking, but the existing methods are found to be insufficient, highlighting the persistent challenges posed by groups like Team Jorge in the ever-evolving disinformation landscape.

IT'S THE ATTENTION ECONOMY, STUPID!

Chair:
Ana Romero (EU DisinfoLab)

Speakers:
"Dormant and persistent networks":
Guillaume Kuster (Check First)
Aleksandra Atanasova (Reset)

"The attention economy stack: tools and ways to act":
Nandini Jammi (Check My Ads)
Clare Melford (Global Disinformation Index)
Sam Jeffers (WhoTargetsMe)

The first presentation focused on the detection of two disinformation operations. Currently, more and more organisations are working on ways to identify automatically created accounts (ACA). These accounts are predominantly anonymous, present in vast quantities, and implicated in activities that contravene Meta's guidelines, such as phishing and intransparent political advertising.

Aleksandra Atanasova, Investigations Lead at RESET, presented how a network of 300 deceptive online ads linked to the 'Doppelganger' operation promoted narratives such as the inefficacy of sanctions against Russia and Western responsibilities in the Ukraine war.

A similar investigation by Check First detected a massive scam involving 1,500+ Facebook ads, leading users to over 160 fake media sites. Guillaume Kuster, co-founder and CEO of Check First, presented the 'Facebook Hustles' operation. Atanasova highlighted issues like the intermittent removal of ACA without a holistic strategy to deter their inception. There is a need for a verification process for ACA, particularly regarding ads usage. Kuster mentioned that the increasing scale of these scams highlights the urgent need for digital advertising regulation. However, the intertwined interests of businesses and advertising pose challenges.

A panel discussion followed on how civil society and researchers deal with challenges posed by data access and continue their highly dependent activities on open data sources. Nandini Jammi, the co-founder and CEO of Check My Ads, highlighted that platforms' supply policies are increasingly robust, making it more challenging for researchers to study digital ads. These policies make it more complicated to check how and by whom digital ads are operated, having negative repercussions, especially for bad actors promoting disinformation and hate speech.

Clare Melford, the co-founder and CEO of the Global Disinformation Index, emphasised the importance of online safety and the economics of disinformation. She suggested taking a narrative approach to fighting disinformation and highlighted that introducing the Dynamic Exclusion List helps counter disinformation risks. Sam Jeffers, co-founder and CEO of WhoTargetsMe, delved into the necessity for political transparency, spotlighting the challenges introduced by recent legislation like the DSA.

FROM HARASSED TO EMPOWERED: A POSITIVE APPROACH TO BUILDING RESILIENCE

Chair:
Anna Gielewska (Reporters Foundation)

Speakers:

"We need to talk about mental health support":
Jochen Spangenberg (Deutsche Welle)
Magdalena Lind (Metis Services)

"Fighting back against harassment":
Nina Jankowicz (Author, Counter-disinformation expert)

This session, chaired by Anna Gielewska from the Reporters Foundation, convened to address the pressing issue of mental health support within a community regularly subjected to various occupational hazards. These hazards encompassed exposure to violent content, online harassment, physical threats, lawsuits, and the ever-present risk of burnout. The primary objective was to acknowledge the extent of harm this community faced and explore actionable solutions for fostering resilience and support.

Jochen Spangenberg of Deutsche Welle initiated the discussion by highlighting the potential psychological repercussions of exposure to distressing content. He stressed the significance of recognising early signs of mental distress, categorising them as "intrusions, avoidance, negative thoughts and emotions, hyperarousal." Spangenberg introduced various measures aimed at trauma management and mitigation.

Magdalena Lind, a respected speaker in the session on mental health support within a community exposed to occupational hazards, shared her expertise on resilience and mental health in high-risk environments. With a background in working with journalists, activists, and civil society organisations, Magdalena Lind offered valuable insights into building and maintaining resilience. Her extensive experience includes collaborating on "Come Back Alive", a handbook for personal security in high-risk contexts, and researching resilience in healthcare systems.

Nina Jankowicz, an accomplished author and recognised expert in counter-disinformation, discussed identifying and countering the spread of false information and disinformation. In her presentation, Jankowicz highlighted the pervasive issue of trolls and digital harassment. Jankowicz emphasised the critical role of social media platforms in addressing this problem, underlining the need for proactive measures to silence trolls and protect users from online abuse. Jankowicz's insights extended to the broader implications of disinformation campaigns, which often seek to silence and intimidate individuals by spreading false narratives and propaganda.

TRANSPARENCY PARADOX: HOW CAN DATA KEEP US BOTH INFORMED AND CONFUSED

Chair:
Mathias Vermeulen (AWO)

Speakers:

"Transparency is no silver bullet":
John Albert (AlgorithmWatch)

"Can we cure our data dependence?":
Brandi Geurkink (Mozilla)
Alicia Wanless (Carnegie Endowment for International Peace)
Kalina Bontcheva (University of Sheffield)

During the panel, John Albert from AlgorithmWatch recalled that in 2016, Facebook overestimated the average viewing time for video advertisements on its platform, and even after discovering the error, the company continued to report false data. This leads to the question of how platforms assess and mitigate disinformation and how disinformation changes the media environment.

According to Albert, transparency reports help illustrate how platforms manage harmful content, but the paradox appears when these reports are manipulated for PR. In this context, the DSA aims to increase platform transparency regarding data risk assessment but limits data access for researchers. The community guidelines, compliance reporting, and governments' content takedown requests can also be restrained and may not be genuinely transparent.

According to Albert, the Code of Practice on Disinformation aims to show tech companies' efforts to counter disinformation; nonetheless, it needs to be improved in quality and efficiency. NGOs and watchdogs have a role in conducting independent research, investigating available information, calling out "transparency washing", and supporting efficient governmental frameworks.

The panel discussion shed light on the limitations of data research, transparency, and the challenges of data research in the digital age. "We have to pull these resources and share data, experiences, and know-how", Prof. Kalina Bontcheva said.

Research ethics and the breach of personal data are also fundamental issues. According to Bontcheva, the community of researchers must come together to solve the legal challenges in the first place. Then again, there is a policy gap with no incentive for researchers to provide policy recommendations, Alicia Wanless from Carnegie added. She elaborated on intentional backslides and the tendency to move away from transparency by touching upon the challenges of finding funding for the research field. To illustrate this, she mentioned the debate in the US about the cut in spending for research in the cases where the researchers choose not to share their results with the state actors.

PROACTIVE STRATEGIES FOR PREVENTION & RESPONSE

Chair:
Sabrina Spieleder (EEAS)

Speakers:
"Avengers, assemble! Volunteer communities countering online disinformation":
Inês Narciso (VOST Europe)

"Tackling foreign interference at a national level, a benchmark of Member States initiatives":
Hervé Letoqueux (Viginum)
Alejandro Gonzalez Fernandez (Spanish National Security Department)

This panel discussion highlighted the need to combat disinformation and its potentially detrimental effects on society and national security. Inês Narciso presented a compelling case of volunteer communities effectively countering online disinformation. She discussed an incident from February 2021 when false information began to circulate on WhatsApp, claiming that Portugal was about to lift its COVID-19 lockdown. The news rapidly gained traction on social media platforms, creating widespread confusion.

However, VOST Portugal successfully collaborated with public authorities to debunk the false information. Their verification efforts highlighted the power of resilient communities working harmoniously with governmental agencies. The case also underscored the challenges of platforms like WhatsApp, with no moderation and limited data for identification, making it a breeding ground for disinformation.

Hervé Letoqueux discussed France's response to foreign digital interference. Viginum, the French government's technical and operational service, was established after several events, including the Macron Leaks in 2017, Samuel Paty's assassination in 2020, and the TV5 Monde hack in 2015, all involving disinformation and foreign actors. Viginum's mission is to detect and characterise suspicious propagation of misleading or hostile content on digital platforms explicitly involving foreign actors.

The third contribution featured Alejandro Gonzalez Fernandez, highlighting the public-private approach of the National Security Department in Spain to counter disinformation in the country. He emphasised the importance of understanding the risks of disinformation, specifically concerning Spanish society and its implications for national security. The Department gathered a diverse group of experts from various fields, including journalism, academia, think tanks, social media platforms, and more. The goal was to improve knowledge of the threat, how to counter it, and increase awareness. It has been actively working on various initiatives, including mapping disinformation research capabilities, developing methodologies for detection and response to disinformation, analysing the fulfilment of commitments by social media platforms in Spain, and studying the psychological effects and radicalisation caused by foreign information manipulation. The Department is also exploring the use of AI and cyber intelligence techniques to combat disinformation effectively.

These initiatives from different countries share a common objective: countering online disinformation that threatens the credibility of information and the security and well-being of their nations. The cases of Portugal, France, and Spain highlight the importance of collaboration between government agencies, civil society, and the private sector.

ACTIVATE THE POTENTIAL OF PLATFORM DATA

Chair:
Raquel Miguel (EU DisinfoLab)

Speakers:

"Designing an Online Operations Kill Chain":
Ben Nimmo (Meta)

"TikTok. Who's there?":
Marc Faddoul (AI Forensics)

The session on platform data provided a valuable business perspective on how Meta and TikTok tackle online disinformation of online operations and solve security and privacy concerns. The first presentation delved into the Online Operations Kill Chain, a framework designed to identify and sequence the phases of online operations. The framework covers a range of operations, including espionage, covert information operations, scams, and frauds. It aims to help teams pinpoint vulnerabilities, allowing them to take action against malicious actors.

Online operations begin by obtaining essential building blocks and creating fictitious personas or websites to make their assets appear legitimate. They continue by coordinating and planning, managing assets and members, training recruits, and using social media automation tools. Furthermore, Ben Nimmo highlighted that these operations are increasingly complex and flexible, facilitating cross-functional cooperation. Moreover, analysing online activities' behaviour to understand their dynamics fully is of primary importance.

The second part was a workshop led by Marc Faddoul from AI Forensics on the challenges of countering disinformation on TikTok. The Chinese platform's algorithms have been questioned for their impact on user content consumption. Faddoul highlighted that algorithmic audits are essential for content moderation, algorithmic amplification, and algorithmic demotion to ensure transparency and user safety. The DSA introduces risk assessment reports and third-party audits to oversee recommender systems.

Faddoul pointed out that researchers face limitations in accessing TikTok data, with the TikTok API only available for academic research and the platform's Ad Library accessible to everyone. Nevertheless, access to the TikTok Ad Library provides limited insights into political advertising and whether platforms adhere to their policies. The TikTok Researcher API has limitations, and researchers must submit projects for approval, which can be restrictive. In addition, the terms and conditions of access make it challenging for productive research.

Faddoul also highlighted that researchers have adopted various approaches, including cooperative audits, data donation, and sock-puppet audits, to study TikTok's algorithms. The TikTok Observatory initiative aims to recommend content based on user locations and understand TikTok's role in disseminating polarising or inaccurate content. AI Forensics stressed the need for the EU's AI Act to focus more on algorithmic auditing and suggested integrating generative AI tools and recommender systems in the new draft.

RUSSIAN WAR: A TIPPING POINT TO ACT AGAINST FOREIGN INTERFERENCE?

Chair:
Jakub Kalensky (Hybrid CoE)

Speakers:

"Disinformation & disruption: An analysis of pro-Russia cyber-Enabled IOs during wartime in Ukraine":
Gabby Roncone (Mandiant),
Alden Wahlstrom (Mandiant)

Panel Discussion: "18 months of sanctions against Russian disinformation actors – what's the impact?":
Vincent (All Eyes on Wagner)
Francesca Arcostanzo (Institute for Strategic Dialogue)
Maxime Audinet (IRSEM)

Gabby Roncone, representing Mandiant, delivered a thought-provoking presentation on the analysis of pro-Russia cyber-enabled information operations during wartime in Ukraine. Roncone shed light on the crucial role of cyber-enabled components in Russia's information confrontation strategy.

Roncone emphasised, "Russia's strategy of information confrontation is instrumental in supporting the ongoing war in Ukraine. It is a multifaceted approach aimed at disrupting various defence systems simultaneously". She elucidated how cyber-enabled components play a prominent role in this strategy, allowing Russia to achieve its objectives effectively. The significant impact of these cyber-enabled information operations on multiple defence systems was also highlighted.

Following the presentation, a panel discussion featured experts who shared their perspectives on the impact of sanctions against Russian disinformation actors. Vincent, from All Eyes on Wagner, commented, "Disinformation actors engage in a cat-and-mouse game, employing repeated tactics similar to RT and Sputnik. They receive funding from state media and operate in accelerated informational spaces". Vincent also provided insights into the impact of sanctions on the Russian international media ecosystem, including the adoption of anti-US narratives and strategies to circumvent sanctions.

Francesca Arcostanzo, representing the Institute for Strategic Dialogue, discussed the EU sanctions on Russian state outlets introduced in March 2022, highlighting their impact on Russian state media accounts on major social media platforms. Arcostanzo delved into circumvention strategies employed by disinformation actors, including mirror domains, rebranding, and expansion on alternative platforms.

Maxime Audinet, from IRSEM, provided an in-depth analysis of Russia's information influence and the involvement of both state and non-state actors in disinformation campaigns. Audinet elaborated on the extensive network of Russian state actors (comprising RT and Sputnik), Russia Beyond, and non-official actors.

The discussion provided a holistic view of the challenges posed by cyber-enabled information operations and the impact of sanctions. The speakers' expertise and perspectives underscored the evolving landscape of disinformation and the need for proactive measures in response to these complex threats.

FROM CLICKS TO CLUES: AN ONLINE INVESTIGATION WORKSHOP

Chair:
Mattia Caniglia, The Brussels Hub, Atlantic Council's Digital Forensic Research Lab

Speakers:

Workshop: "From clicks to clues? An online investigation workshop":
Stefan Voss & **Arne Beckman**, DPA

Presentation "Best practices for OSINT investigations, where to find them and how to apply them":
Givi Gigitashvili, Atlantic Council's Digital Forensic Research Lab;
Sayyara Mammadova, Atlantic Council's Digital Forensic Research Lab

ObSINT is a collaboration of esteemed organisations carrying out open-source investigations to provide the public with factual and objective information.. Mattia Caniglia introduced the Guidelines for Public Interest OSINT Investigations, which was published in early 2023 and consists of five chapters that include the principles, public interest, methodology, outputs, and general work practices. Afterwards, in their presentations, Sayyara Mammadova and Givi Gigitashvili gave insight into implementing these OSINT guidelines in real life.

Sayyara Mammadova presented a case study on the exposition of coordinated pro-Kremlin networks on Telegram. The digital investigation process on Telegram starts by monitoring a suspicious Telegram channel. After the discovery and initial assessment, the connections, amplifiers, content of the posts, and the administrator are investigated, for instance, using tools like Command-Line Interface (CLI) and Graphical User Interface (GUI). As a result of the Digital Forensic Research Lab's (DFRLab) investigations, well-known Telegram channels such as Surf Noise, Info Defense, and Node of Time were found to be posting inaccurate statistics, conspiracy theories, mis- and disinformation about Poland.

Gigitashvili referred to the investigation of the political astroturfing campaign that pushed the anti-Ukraine hashtag #StopUkrainizacjiPolski into Poland's trending list on X (formerly Twitter). The analysis revealed that the operation was partially automated and partially human-made. Also, a specific pattern in the publishing time of the posts was detected.

During the workshop titled "How can I archive this?", the team from Deutschen Presse-Agentur (DPA) described their journey and presented their tips for internet archiving, presenting multiple methodologies to archive content. Stefan Voss and Arne Beckman showed how screenshots are impractical as proof because they are extremely easy to forge or alter. Moreover, it is also possible to archive social media sites such as Facebook and Instagram. Hence, more journalists should be aware of the importance of archiving as this tool could be essential for their work. Although internet archives can be misused, their overall value for journalistic research could outweigh the potential risks.

SHIFTING LENSES: DISINFORMATION FROM A DIFFERENT ANGLE

Chair:
Emerson Brooking (DFRLab)

Speakers:
Lindsay Hundley (Meta)
Théophile Lenoir (University of Milan)

In this session, Lindsay Hundley from Meta and Théophile Lenoir from the University of Milan discussed the complex challenges surrounding the issue of media capture by authoritarian states with a particular focus on Russia. The speakers explored the problems that arise when addressing media manipulation and the potential consequences of various enforcement actions. The session tackled the need for platforms to balance safeguarding information integrity and respecting freedom of expression.

Platforms like Meta face the challenge of defining and identifying state-controlled media. Questions arise about the threshold for state control, such as determining the level of funding required or accounting for mechanisms aimed at preserving editorial independence. “How should platforms like Meta even define and identify state media?” Hundley asked. To address this, a transparency-first approach is proposed, which involves labelling publishers that are “wholly or partially under the editorial control of the government.”

The goal is to empower users to make informed decisions about the content they consume, applying community standards enforcement to state media outlets like individual users. Meta has implemented new enforcement measures against Russian state-controlled media. These actions include blocking ads globally, demonetising pages and accounts, demoting content in feeds, and introducing additional product interventions to enhance transparency.

Théophile Lenoir then explored the complex issues surrounding content policies and the challenges of regulating speech. He noted the complexities of these subjects, emphasising the need for nuanced approaches and careful considerations in the digital age.

Drawing from the work of Donna Haraway, a prominent feminist scholar in science and technology studies, Lenoir delved into the critique of objectivism, which tends to ignore the individual perspectives and contexts in knowledge creation. Accordingly, knowledge is always situated, hence the importance of recognising the subjectivity and context in which information is produced and disseminated.

During the session, Lenoir posed a critical question: “What should be the basis for regulating speech in the digital age?”. This question probes the fundamental principles that guide decisions on content moderation, exploring whether regulations should be anchored in universal human rights or other frameworks. Another key facet of the discussion revolved around protecting groups rather than just individuals. This consideration supports the need for regulatory frameworks that account for the broader societal implications of speech and content policies.

REGULATORY UPDATE & PANEL DISCUSSION

Chair:
Gregory Rohde (EU DisinfoLab Board Member)

Speakers:
Carlos Hernandez (EFCSN and Maldita)
Diana Wallis (EU DisinfoLab)
Trisha Meyer (VUB and EDMO BELUX)
Lubos Kuklis (Expert on digital governance, EU Commission's DSA team)

The panellists discussed crucial updates on EU regulatory and policy initiatives, focusing on the European Media Freedom Act (EMFA), the Digital Services Act (DSA), and the Code of Practice (CoP). Carlos Hernandez, representing EFCSN and Fundacion Maldita, addressed the implementation of the DSA, noting that it is already in place for Very Large Online Platforms (VLOPs) and will extend to Digital Service Coordinators (DSCs) in February 2024.

He stressed the importance of risk assessment and transparency and pointed out that less access to data can be a challenge for researchers. Hernandez also underlined the need for media services to maintain editorial independence, as many currently depend on various institutions. Lubos Kuklis from the European Commission portrayed the DSA as a groundbreaking regulation designed to monitor online content distribution and ensure it adheres to specified standards. Companies are now responsible for assessing risks and implementing mitigation measures, with the Commission monitoring compliance. Kuklis maintained, "The DSA systemically regulates online content to see if the measures of the distribution of content respect certain standards."

Diana Wallis, EU DisinfoLab President and former Vice-President of the European Parliament, underlined the complexity of ensuring media freedom while regulating it, stressing the need for attention from legislators. Trisha Meyer from VUB and EDMO BeLux talked about the significance of transparency in databases and research coordination. “We need to be reflective of the diverse research needs that there are in academia”, Meyer said, pointing out that data access is now worse than before.

During the Q&A session, concerns were raised about the lack of specific definitions for disinformation in the DSA, which leads to supplementary actions and task delegation. The implementation of DSA in candidate countries was also mentioned, as these countries work on legislation to align with the EU. The global nature of disinformation made considering how EU legislation is perceived beyond its borders crucial.

Additionally, the differences in capacity among EU Member States to implement DSA were noted, asserting the need for a system of regulators from the national and EU levels. Lastly, there were discussions about political advertising regulation, with the challenge of correctly labelling ads as political advertising remaining a significant concern. In conclusion, this session provided valuable insights into ongoing EU regulatory initiatives, drawing attention to the complexity of media freedom regulation, the importance of research transparency, and the challenges faced in addressing disinformation trends.

HOW DO WE KEEP THE FAITH?

Speaker:
Imran Ahmed (Center for Countering Digital Hate)

To conclude the 2023 EU DisinfoLab Annual Conference, Imran Ahmed, the founder and CEO of the Center for Countering Digital Hate, gave a powerful speech on the pervasive dangers of disinformation in today's digital age. Ahmed addressed the ethical duty to fight against (online) disinformation and its tangible impact on the real world by encouraging participants to continue their work against disinformation.

Ahmed began by stressing the fundamental truth that the online world is not a detached realm but an integral part of human existence. Events and narratives that unfold online are not limited to the digital sphere, but they have tangible, real-world repercussions: "The online world is an uncontestable experience of human life. [...] What happens online has real-world consequences," he said.

Tapping into the symbolism of holding the conference in Krakow, Poland, Ahmed drew a parallel between the digital age and Auschwitz. The Polish concentration camp stands as a testament to the horrors that can arise from unchecked lies and conspiracies. Today, these lies are not just being spread but are also being monetised online. Disinformation, according to Ahmed, is not merely a technological or legal challenge, it is fundamentally a moral issue. He expressed concern over how major media companies exploit the attention of the younger generation, particularly children. "These companies that colonised our media systems are mines of attention of our children," he argued.

Ahmed's personal motivation to combat disinformation stems from witnessing the harmful effects of digital conspiracies and hate speech. He reflected on the assassination of British politician Jo Cox due to hate speech and disinformation. The corruption of the information system poses a threat to democracy that motivates the urge to educate the public and safeguard democratic values.

Despite the efforts, Ahmed highlighted the backlash faced by those working to counter disinformation, referencing US Congressman Jim Jordan's stance on protecting free speech as an example. Another alarming point Ahmed raised was teenagers' susceptibility to conspiracy theories. Having grown up in the digital age, this age group is at risk of developing a distorted perception of reality and is more prone to believe in disinformation.

Regardless of the challenges, Ahmed emphasised the potential of new regulations focusing on platform accountability and transparency. He also addressed the challenges researchers face, like the prohibitive costs of accessing certain online resources, and called for more inclusive data access regimes. The real change requires collective will, collaboration, partnerships, and strategic legislative flexibility. Ahmed closed his speech with a message to the EU DisinfoLab community: "You must continue to raise your voices and not forget why we are here!".