Mis-and Disinformation:
Extremism in the Digital Age
Report 2023

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK


130 KiB/s
24.2 KiB/s
10.1 KiB/s
8.66 KiB/s
2.17 KiB/s
906 B/s
Screen must be at least 4 rows in height
Floating point exception (core dumped)
0 directories, 1 file
249 KiB/s
4.48 KiB/s
2.03 KiB/s
710 B/s

Mis-and Disinformation: Extremism in the Digital Age

Contributors and Reviewers

Elisabeth Braw (Reviewer)
Senior Fellow, Foreign and Defense Policy
American Enterprise Institute

Karen Monaghan (Author)
Senior Consultant, Homeland Security and
Emergency Management Agency, Washington DC

Judy Pal (Reviewer and Contributor)
Independent Communications Expert
Former Assistant Commissioner, New York Police Department

Dr Christopher Rodriguez (Author)
Director, Homeland Security and
Emergency Management Agency, Washington DC

Alex Townsend-Drake (Editor)
CTPN Head of Programme
Counter Terrorism Preparedness Network

Dr Jessica White (Reviewer and Contributor)
Senior Research Fellow, Terrorism and Conflict
Royal United Services Institute

Table of Contents

Mis-and Disinformation: Defining the Problem

Spreading false information, conspiracies, and propaganda is a tried-and-tested strategy to mislead the public while seeking to undermine an opponent's position and/or elevate one's own reputation. Some hostile states consider disinformation as integral to their military doctrine, strategy, and wartime capabilities. Prior to the internet, however, it took weeks, months, and even years to reach a worldwide audience. Today the widespread use of the internet alongside global penetration of social media and messaging platforms, coupled with the 24/7 news cycle, have accelerated its spread.

The digital age means that access to this information is easier and faster than ever. The online data portal Statista notes that about 68% of the world's population owns a smartphone suggesting that the majority of individuals worldwide can access omnipresent sources of social and mainstream media.[1] These devices can also be used to create and upload original content.

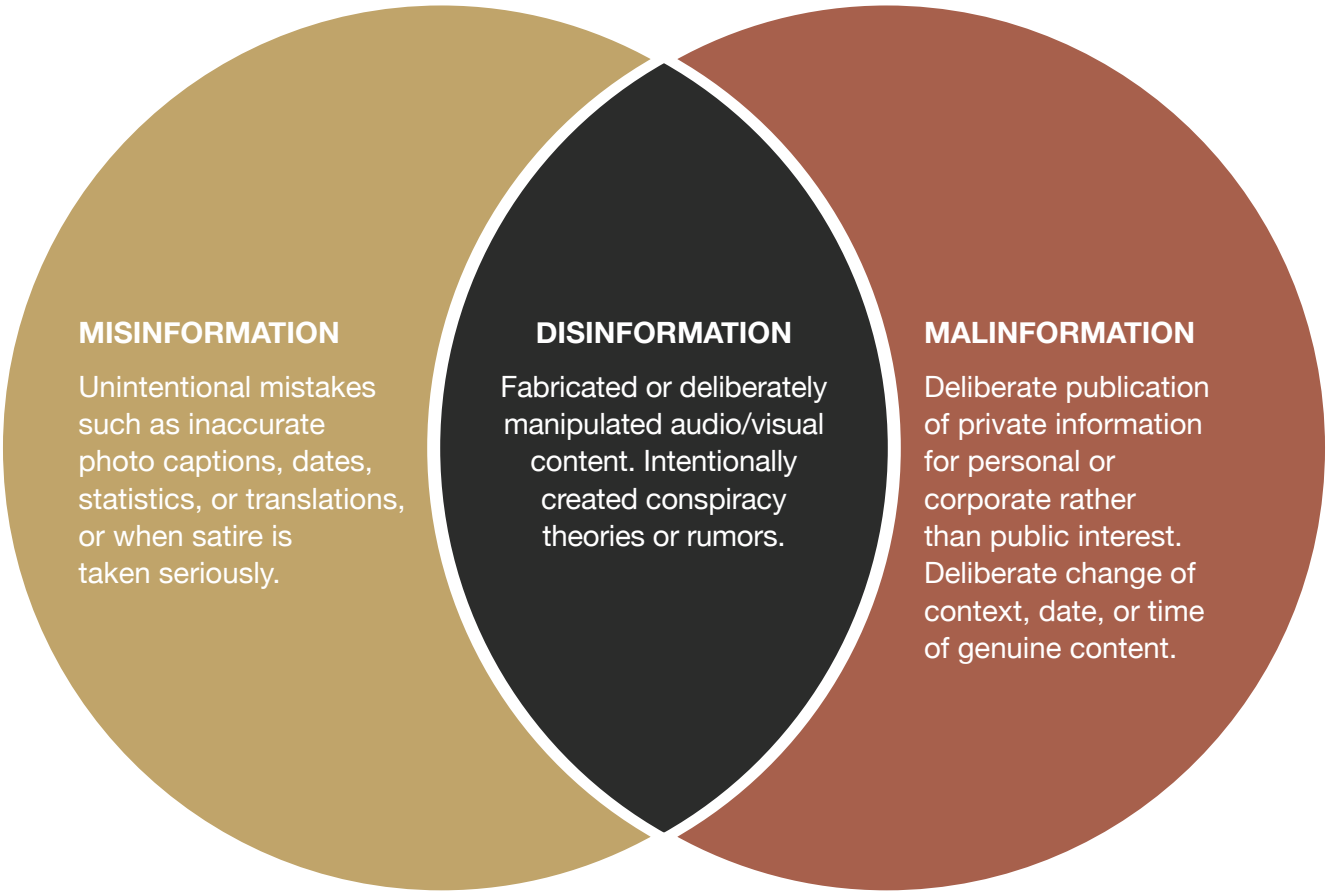
Most mis-and disinformation is posted and spread on social media and messaging apps. Early research suggested that individuals facilitated the spread of disinformation more than algorithms or bots. For example, in 2018, researchers at the US-based Massachusetts Institute of Technology found that people were more likely to spread false stories on platforms like Twitter than automated bots. In addition, false news stories were 70 percent more likely to be retweeted than true ones.[2]

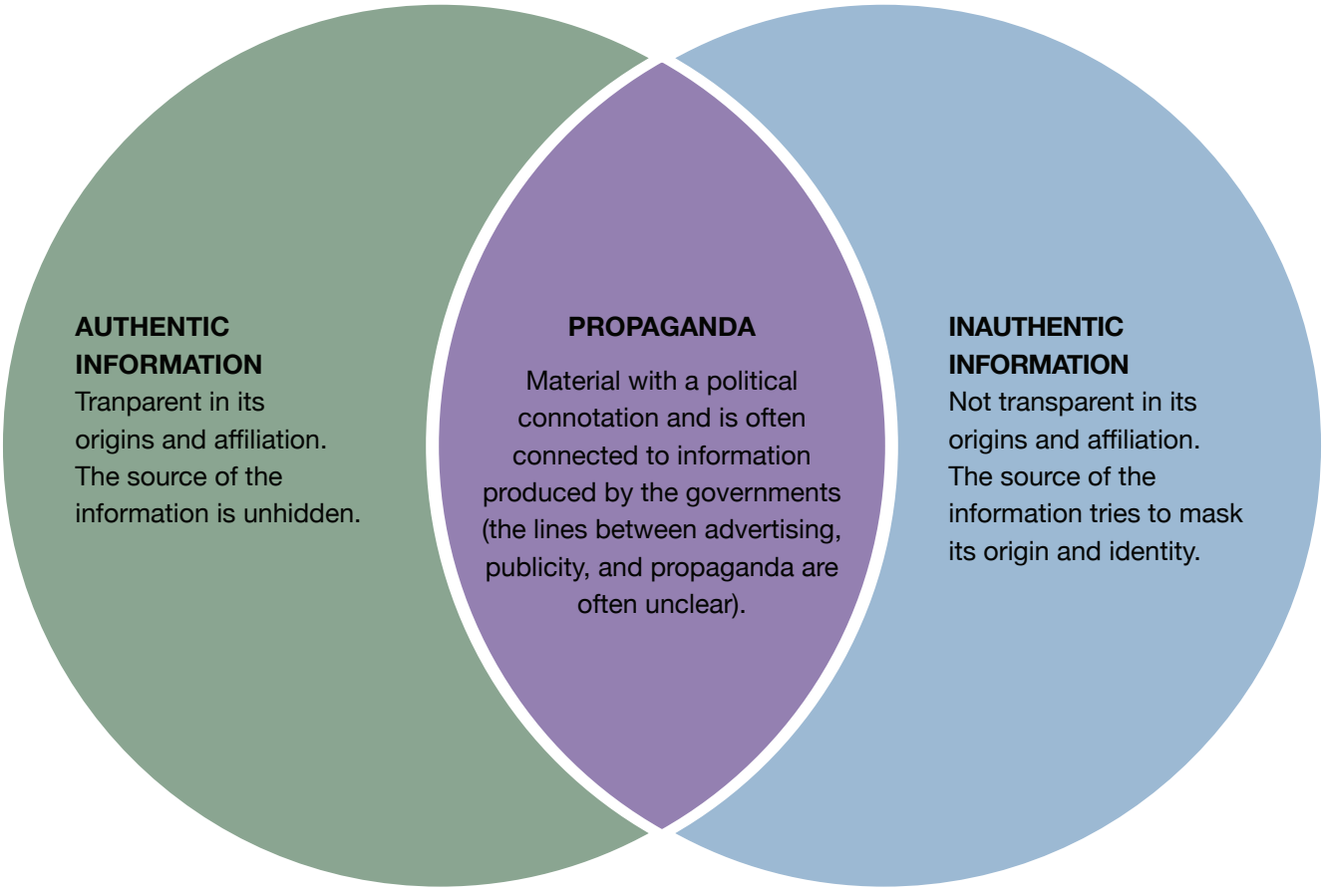
Recent studies note that advances in Artificial Intelligence, natural-language processing, and machine learning mean some bots can more closely mimic human behavior, generating original language and content.[3] Researchers warn these "chatbots" can be "weaponised by malign actors to spread misinformation at an unprecedented scale, delivered in a more knowledgeable, persuasive, and dangerous manner."[4]

A 2022 Reuters Institute global survey found 54% of respondents in Africa, the Americas, Asia Pacific, and Europe were concerned about false information online, with higher concerns (61%) among those who relied on social media for news.[5] Edelman, the global communications firm, in its 2022 Trust Barometer also showed 76% of respondents worried false information or fake news was being used as a "weapon."[6]

In practice, there is a delineation between information that is intentionally and unintentionally misleading. Experts commonly categorise false information based on the intent of the creator or spreader—as either unintentional or intentional. Therefore, misinformation refers to false information inadvertently used or shared, while disinformation is the deliberate creation, dissemination, and/or sharing of false information to cause harm.[7] Malinformation also has its roots in malign intent, although it generally involves leaks of true information, such as personal identifiable information.

Types of Information





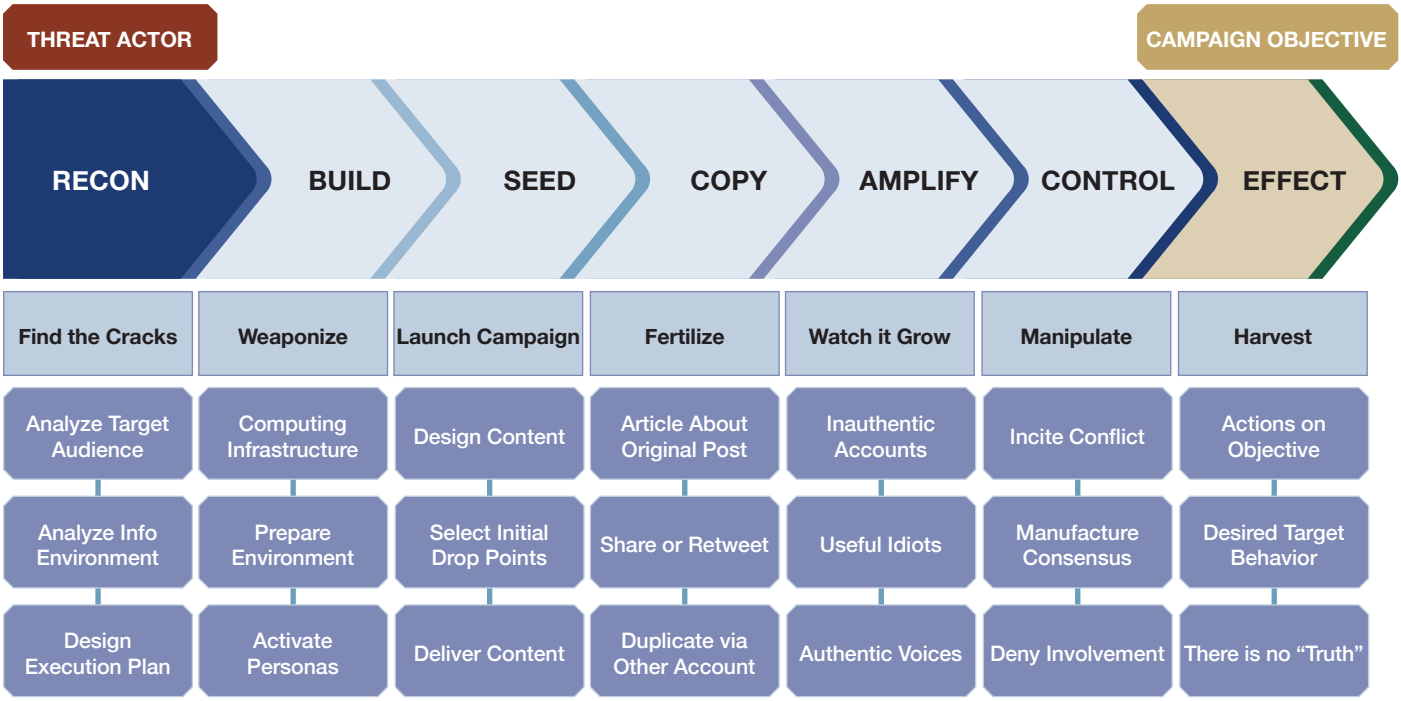
Referring to the trucker rally in Canada in early 2022, which paralysed that nation's capital, Peter Sloly, the former Chief of the Ottawa Police Service, said "A handful of people, with their sophisticated use of social media, can turn an idea into an ideology into a funded movement that can move thousands of vehicles and tens of thousands of individuals to a specific location…while also raising millions of dollars in days. That couldn't happen 5 or 10 years ago, and police chiefs didn't have to worry about that happening. We have to worry about it now."[8]

As the following infographic illustrates, threat actors advancing disinformation go through a strategic process of building and seeding their narratives, then spreading and amplifying their messaging with a view to controlling or effecting an outcome that can include violence.

To counter this, critical thinking skills are essential to discerning what is true and what is manipulative. A Rand Corporation study identified the drivers behind the public's tendency to blur facts and opinions as: 1) cognitive biases; (2) changes in information sources to include news derived from social media and the 24/7 news cycle; (3) a lack of educational focus on developing critical thinking skills, and; (4) political and social polarisation.[9] Extremists can capitalise on this and be sophisticated in their approach.

As societies become increasingly digitalised and the thirst for, and dependence upon, information continues to accelerate, mis-and disinformation poses a real security threat with implications at all levels. This will be explored with reference to state-sponsored disinformation; extremism in the digital age; and how this could be managed by authorities at a local level. This brief will further consider implications for counter-terrorism, and arrangements relating to preparedness and response.

Disinformation Kill Chain



Note: A disinformation threat actor may skip steps in the kill chain process. However, doing so may reduce the effectiveness of the campaign and create protections aimed at obfuscating the identity and objetives of the actor.

Source: Adam Cambridge at The MITRE Corporation

State-Sponsored Disinformation

State-sponsored disinformation, whilst viewed separately from extremism, is a major challenge. Since the Russian disinformation campaign against the US presidential election in 2016, the West has increased its focus on state-sponsored initiatives. State-sponsored disinformation campaigns feed into local grievances and are used by partisan groups to maximise impact often with the aim of influencing public opinion, electoral or other political outcomes. The scale of the issue was highlighted by an Oxford University study in 2020 which found evidence in 81 countries where propaganda and disinformation on social media was employed to manipulate public opinion.[10]

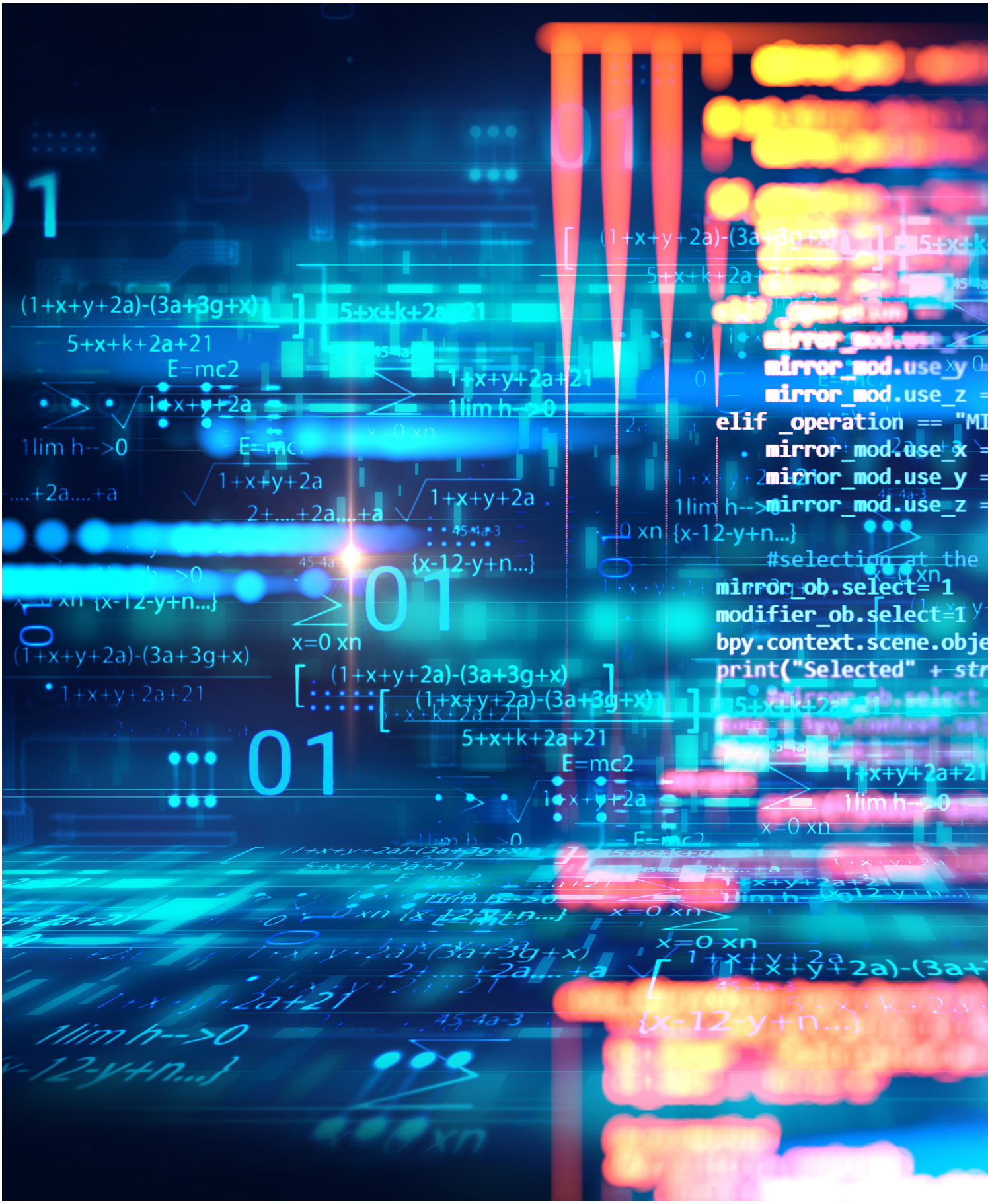
For example, Russian disinformation campaigns have been linked to the 2016 Brexit vote, the 2017 Catalonia vote for independence, the 2018-19 yellow vest protests in France, and the 2019 European Parliament elections.[11] During COVID-19, Russia and China exploited lingering suspicions about US biological research by spreading disinformation that the virus was developed in a US military laboratory, which reignited a decades-old Russian conspiracy (Operation Infektion) on the origins of HIV-AIDS.[12]

Foreign governments also utilise proxies, fronts, and cutouts to spread disinformation.[13] For example, Russia has stepped up proxy activities since invading Ukraine on 24 February 2022, asserting baseless claims about Ukrainian neo-Nazi leadership and US support for manufacturing biological weapons in Ukraine.[14] They have also outsourced some operations to proxy organisations and troll farms.[15] Moscow uses pseudo-academic front groups such as the Strategic Culture Foundation, Global Research, New Eastern Outlook, and News Front to push Kremlin narratives.[16] News outlets that repeat information from these seemingly "legitimate" organisations lend credibility to government propaganda and disinformation. Redfish is another example of a media company based in Germany that is a Kremlin media front operated by former employees of the state-sponsored periodical Russia Today.[17]

China reportedly uses Chinese Communist Party proxy front organisations in Taiwan, Singapore, and other countries to spread anti-Taiwan and pro-Beijing narratives and disinformation on traditional and social media.[18] In addition, official Chinese media outlets like Xinhua have licensing deals with local language news outlets in Asia and Africa, providing further outreach.[19 20 21]

Iran and North Korea (DPRK) have conducted disinformation campaigns to spread propaganda and promote policies favored by their governments.[22] A 2018 Reuters investigation uncovered a Teheran-based news agency linked to 70 websites that spread pro-regime propaganda to 15 countries, including the US and UK.[23] As of 2018, DPRK agents have been known to spread pro-regime messages using fake online accounts targeting South Korean audiences.[23]4

State-sponsored disinformation is a significant problem, and these types of tactics are increasingly adopted by extremists operating within the online space. In several Western countries, extremist groups have even parroted Russian disinformation campaigns opposing NATO and Western financial, humanitarian, and military support for Ukraine; this has been particularly notable in Canada, home to the second-largest Ukrainian diaspora in the world.[25]


(1+x+y+2a)-(3a+3g+x)
5+x+k+2a+21
E=mc2
1+x+y+2a
1lim h-->0
{x-12-y+n...}
x=0 xn
mirror_mod.use_x
mirror_mod.use_y
mirror_mod.use_z
elif operation == "MI
#selection at the
mirror_ob.select= 1
modifier_ob.select=1
bpy.context.scene.obje
print("Selected" + str

Extremism in the Digital Age

In liberal democratic societies, extremists frequently post violent rhetoric with impunity, taking full advantage of local civil liberty and freedom of speech protections. Social media is being used to spread extremist messages, recruit adherents, and gain public, financial, and political support. Extremists see social media as an effective medium to spread their beliefs, radicalise individuals, and encourage action including violence. Extremists have benefited greatly from the internet and social media because of its ability to spread propaganda and communications quickly and easily, and they are well-versed in using mis- and disinformation tactics to amplify their impact.

According to a 2021 study completed by New York University-based Cybersecurity for Democracy, the extreme right-wing utilises and benefits from disinformation campaigns more than any other group.[26] There are also some examples where extreme left-wing groups have spread disinformation and conspiracy theories that overlap with far-right counterparts, namely antisemitic narratives, falsehoods about the invasion of Ukraine, and COVID-19 conspiracies.[27]

An additional challenge that has become increasingly concerning over recent years is the amplification of mis-and disinformation through conspiracy. It is worth noting that a 2019 YouGov-Cambridge Globalism Project survey poll conducted in 19 countries showed populists are more likely to believe in conspiracy theories that science or factual evidence contradict.[28] QAnon, for example, is a conspiracy theory with US origins that attained global reach and resonance based on disinformation about a powerful "global elite." QAnon adherents shared and amplified the conspiracy on multiple social media platforms and messaging apps in multiple languages across the world. During the pandemic, QAnon supporters also spread the false claim that 5G technology was linked to the spread of COVID-19, thus showing how these threats are commonly combined to increase their impact.[29] It is important to note, however, that not all conspiracy is extremism and vice versa. It can simply be recognised as a form of disinformation.

Disinformation can be spread and generated by extremists from across the ideological spectrum and is often intertwined with conspiracy, therefore accelerating the threat in the digital age, and increasing its reach and impact. This can be compounded by the mainstreaming of extremist ideologies combined with partisan social and political ideas. Extremists can easily exploit online and media echo chambers to target disinformation toward susceptible audiences; where people self-select platforms with views and beliefs that match their own. Here, they are unlikely to be exposed to alternative or opposing views or to critically evaluate the information they might be receiving.[30] Extremists may also infiltrate as many spaces as possible to distort conventional narratives.

The overt approach of extremists to spread disinformation often happens on known extremist websites and discussion forums such as Stormfront and Rumble, targeting an identified base of supporters and sympathisers. The more covert, low-key, approach focuses on social and mainstream media and gaming sites—utilising conspiracies, memes, videos, and other surreptitious means to radicalise susceptible audiences.[31] This approach relies on disinformation, deception, and the normalisation of radical ideas to lure vulnerable populations. The use of popular websites, social media, and gaming platforms can make extreme messages seem more acceptable and mainstream.[32]

CASE STUDY
Gaming: A Key Vector for Spreading Extremist Disinformation

Gaming is a rapidly growing online ecosystem with almost three billion users globally. Online gaming environments include the games themselves and adjacent platforms (such as Steam, Discord, DLive, Twitch, etc.) where people gather in online communities around the topic of gaming, and the expansive range of supporting industry that feeds this environment.

This is an industry that already nets more income than any other form of media and continues to grow as a focal point for potential exploitation by extremists to spread disinformation. Whilst serving as a positive space for the majority of gamers, in some cases extremists have been able to exploit this ecosystem to spread disinformation through the many gamer platforms, forums, and communities.

One of the practical ways in which online gaming is exploited to help spread extremist disinformation is through the employment of gamification. Mass shooters have used gaming and gaming-adjacent platforms to chronicle their extremist views and "glorify" their violence. For example, the perpetrators of violence in Christchurch, New Zealand and Buffalo, New York live-streamed their attacks on popular gaming sites, thus gamifying their violence. This type of gamification allows an increase in the spread of related extremist disinformation by making it visually styled as though it were a video game simulation, thus encouraging engagement with the content. This makes the attack easy to replay while also associating competitive leader boards and points systems with elements of the violence.[33]

Another practical way the gaming ecosystem is exploited to help spread extremist disinformation is through adoption of gamer culture and symbology. Radical Islamist groups, such as Daesh, successfully designed much of their propaganda in line with the aesthetics and culture of particularly popular games to amplify recruitment and spread propaganda disinformation.[34]

CASE STUDY
A Mis-and Disinformation Fueled Attack on the US Capitol

In the lead-up to the attack on the US Capitol on January 6, 2021, mis-and disinformation was amplified on online forums and social media platforms. This drove the narratives, tools, and audiences that perpetuated the violence that day. These virtual safe havens were particularly causal because they reinforced conspiracy theories and false messaging that the 2020 US presidential election was "stolen", and that violence was the best way to redress grievances.

Those who participated in the attack on January 6 included right-wing extremist and conspiracy groups such as the Oath Keepers, QAnon, Proud Boys, Patriot Prayer, and the Three Percenters. According to the US Department of Justice, over 1,100 individuals have been arrested as of September 2023 in nearly all 50 US states for crimes related to the attack.[35]

The impact of foreign influence on violence at the US Capitol, as well as misperceptions of the 2020 US presidential election, cannot be overstated. Russia, for example, leveraged far-right social media outlets leading up to the election, and in October 2020, US social media analytics firm Graphika uncovered a Russian operation targeting users of far-right platforms Gab and Parler that focused on violence and racial tensions in the United States, "present[ing] minorities and liberals in a negative light."[36]

Managing the Threat of Mis-and Disinformation

Mis-and disinformation is a driver for extremism and, by extension, group mobilisation and acts of violence at different levels. This has significant implications for authorities that span multiple risk areas including counter terrorism and security. Most mainstream social media companies have content moderation policies barring posts that encourage violence, are sexually explicit, and contain hate speech—the latter of which is defined as attacking a person for their race, gender, or sexual orientation. However, there are many challenging nuances to moderating grey-area content that might be responsible for spreading mis-and disinformation, and this type of activity can often clash with company business models designed to prioritise and monetise engagement.

Some platforms have addressed disinformation with fact-checking posts and labeling state-run media accounts.[37, 38] But loopholes frequently open given the volume of content, stretched resources of teams, and extremists' ability to work around terms of service and content moderation.[39] Governments and regulators are also constantly playing catch-up as new, less regulated, platforms like TikTok emerge and advanced technologies such as generative Artificial Intelligence become more popular.

A lack of consensus among major Western governments on how, what, and where to regulate with regard to social media platforms also presents a problem, as do the challenges of content moderation and tracking information flows online. Expectations and regulations upon internet companies and social media platforms do need to be increased to drive both responsibility and accountability.

The UK Government has introduced the Online Safety Bill to place an onus upon social media giants to remove illegal content. It is a new set of laws designed to help protect children and adults online. It aims to make social media companies more responsible for their users' safety on their platforms.[40] The regulation of online spaces is one of today's most critical challenges and needs to remain in focus as one of the elements necessary to combat the spread of mis-and disinformation.

It follows that the threat is also directly relevant to the prevent agenda with ample room to consider how awareness and security can be raised—such as through official public information campaigns, employer-led training, and school and community group sessions. Targeted initiatives aimed at audiences that may be more vulnerable or susceptible to online extremist content may also help to counter the threat.

Potential Local Initiatives

Digital and media literacy training.

Individuals often have difficulty distinguishing between verified media and mis-and disinformation. Studies show people tend to believe information that is repeatedly spread; the so-called illusory truth effect. Digital and media literacy programmes can teach people how to evaluate information online.

Public-private partnerships and training with journalists, nonprofit organisations, businesses, and educational institutions can help foster digital literacy.

Establish rumour control pages on official websites.

Local government can encourage citizens to report false or misleading information. Encouraging grassroot efforts to monitor mis-and disinformation can be the most effective way to counter the associated threats, and an online reporting portal can help facilitate this.

Content moderation and social media listening.

Content moderation is a recommended best practice for combatting mis-and disinformation online. In lieu of related policies, local officials should develop public-private partnerships and regular engagement with platforms to facilitate the referral, review, and removal of harmful content.

Geo-fencing and reverse image searches could also be used. Those monitoring social media should utilise tools to establish where false information is coming from. Software is available to determine where posts are uploaded and if images are being re-purposed for disinformation campaigns.

Evidence-based narratives.

Evidence-based narratives that target disinformation aim to provide facts that disprove false information. This method ideally targets disinformation before it spreads and can be implemented at a local level. Local governments can also identify trusted community voices who can connect and provide alternative views and messages. Broader engagement through funding and building dedicated offices staffed by those who are focused on this task can help offer credible information instead.

There is a need to consider how the resulting threat and impact of mis-and disinformation can be managed in the real world; and how the capabilities of organisations and cities can be developed to do so. This means we must also prioritise preparedness.

Preparedness hinges upon the capacity and capability of any given agency or group of agencies to assess and respond to mis-and disinformation in real-time, both online and in public. This demands well-resourced, trained and qualified, teams of experts; strategic communication plans that have been tested and exercised against various scenarios to include the processes and procedures for proactive and reactive messaging; and credible, verified, and authoritative avenues for dissemination that counter, correct, and outweigh sources of mis- and disinformation.

The importance of timely, clear, concise, and visible online messaging by authorities cannot be overstated. Likewise, nor can the role of senior public-facing figures and spokespersons. Here it is critical to harness the mainstream media and local influencers as well as multi-agency partners by taking an open and transparent approach. In fact, an open and transparent approach is widely considered fundamental to achieve public engagement and trust.

A multi-agency table-top exercise in April 2023 highlighted that open and honest, action-orientated, statements that sought to harness the media as a partner were widely considered to be one of the most productive ways to engage the public. It was noted how being clear about the work being done in response to an incident may be more appropriate than not sharing enough information, which risks creating a vacuum that can be filled with speculation and false narratives.

Likewise, early, frequent, and proactive evidence-based statements online, via official social media channels, were equally important.[41] However, there is a need to assess the likely impact of any mis-and disinformation in the first place to judge whether it is even worth engaging in, or if the best response is not to respond.

This links back to the need for well-resourced teams of experts and underscores the requirement for pre-agreed structures to facilitate the response. The London Resilience Communication Group, for example, "brings together the heads of communication or their designated deputies from different organisations to plan for and co-ordinate the communication response to a major incident, crisis or significant event impacting on London".[42] It recognises that the communication aspects of preparing for and handling an incident or crisis can be among the most crucial, and the most challenging, that an organisation can face.

By their very nature, when implemented correctly, these types of multi-agency groups can ensure oversight and consistency when warning and informing the public. This joint approach can also provide a collective authority in support of sharing accurate, timely, and credible narratives. Well-established communication mechanisms are critical to maintain stability during and after an incident, yet there remains ample room to further develop approaches towards countering mis-and disinformation in real-time. The UK Government offer a toolkit for countering disinformation which can be accessed online.[43]

This translates to wider response structures, arrangements and capabilities to monitor, moderate and counter online content that may generate extremist or other mis-and disinformation threats; pose a risk to ongoing investigations or operations; and be detrimental to the reputation and credibility of an agency.

Conclusion and Recommendations

The idea that "falsehood flies and the truth comes limping after"[44] has been exploited by hostile states and extremists—and many groups promoting various causes—through time. This remains the case today. As explored above, the spread of mis-and disinformation can amplify the impact of extremism across the ideological spectrum.

The complexities in monitoring and moderating overwhelming amounts of rapidly changing content, and the challenges in tracing and identifying users to attribute responsibility, creates significant problems. Inaccurate content and, in particular, public belief in such content not only influences public opinions and actions but can also undermine democratic societies and drive extremism.

The threats posed by mis-and disinformation are accelerating online where proxy pseudo-websites, social media platforms, fringe forums, and messaging outlets are increasingly being used to promote extreme narratives and causes, rally supporters, and encourage actions including violence. A digital generation is accessing and pushing unquantifiable volumes of unfiltered and unverified information on a 24/7 basis.

To date, efforts to monitor or remove such information have been ineffective at best and complicit at worst. Platforms offer all the benefits—audience, amplification, monetisation, glorification—for extremists to influence, rally, recruit, and radicalise.

Whilst years of research on radicalisation and violent extremism have made it that clear there is no one-size-fits-all approach for its prevention—the pathways and contributors towards radicalisation are too diverse, complex, and far-reaching—it must be recognised that mis-and disinformation are important and influential parts of a much bigger picture.

There are ways in which this threat can be better managed. In its truest form, this requires political leadership, robust legislation and regulation, as well as mandated public-private cooperation and education in this space. At a city-level, however, there are opportunities to increase awareness and understanding; develop the relationships, arrangements, and capabilities needed to prepare and respond; and enhance approaches towards both proactive and reactive public education and communications.

Recommendations

1	Conduct country and city-specific research and analyses to understand the local threats in the context of online groups, traditional and social media outlets seeding mis-and disinformation.
2	Establish a local governance structure and associated documentation to inform and guide policy initiatives, campaigns, interventions, and projects as identified based on need.
3	Invest in the development of appropriately resourced and trained teams that can monitor and assess mis-and disinformation for multi-agency situational awareness and planning.
4	Assess the potential impact mis-and disinformation could have on ongoing operations and investigations or the reputation of an organisation, and put mitigation measures in place through the formation of a partnership-based multi-agency communications group.
5	Review strategic communication plans and procedures for both proactive and reactive public messaging. These should consider both online and public platforms, as well as connectivity with partners, specialist crime agencies, fusion centers, and the private sector as appropriate.
6	Enhance arrangements through mis-and disinformation scenario-based exercises and engage the mainstream media as partners in this process (both single and multi-agency).
7	Deliver targeted initiatives such as digital and media literacy training within organisations, schools, and community groups; and the creation of rumor control pages on local government websites to encourage citizens to report false or misleading information.
8	Share learning, knowledge, experiences, and practices with counterparts internationally to continue to progress the agenda at a city-level and beyond.

References

[1] Laricchia, F. (2023, May 24), Smartphone penetration worldwide as share of global population 2016-2022, Statista. Accessed Online.

[2] Dizikes, P. (2018, March 8). "Study: On Twitter, false news travels faster than true stories Research project finds humans, not bots, are primarily responsible for spread of misleading information," Massachusetts Institute of Technology (MIT) News. Accessed Online.

[3] Goldstein, J. A., Sastry, G., Musser, M. et al, (January 2023), Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations Georgetown University's Center for Security and Emerging Technology, OpenAI, and Stanford Internet Observatory. Accessed Online.

[4] Arvanitis, L., Sadeghi, M., Brewster, J., (March 2023) "Despite OpenAI's Promises, the Company's New AI Tool Produces Misinformation More Frequently, and More Persuasively, than its Predecessor," NewsGuard Misinformation Monitor. Accessed Online.

[5] Newman, N., Fletcher R, Robertson, C, et al. (2022) Digital News Report 2020, Oxford: Reuters Institute for the Study of Journalism. Accessed Online.

[6] Edelman Trust Barometer (2022). Accessed Online.

[7] Gebel, M. (2021, January 15). Misinformation vs. disinformation: What to know about each form of false information, and how to spot them online. Business Insider. Accessed Online.

[8] Police Forum (2022) In conversation with Chuck Wexler at PERF. Accessed Online.

[9] RAND Corporation (2022). About Truth Decay. Accessed Online.

[10] Samantha Bradshaw, S., Bailey, H., and Howard, P.N. (2021) Industrialized Disinformation: 2020 Global Inventory of Organised Social Media. Manipulation. Working Paper 2021.1. Oxford, UK: Project on Computational Propaganda. Accessed Online.

[11] Legucka, G., (2020, March 19) Russia's Long-Term Campaign of Disinformation in Europe, Carnegie Europe. Accessed Online.

[12] The New York Times. (2018, November 19). Meet the KGB spies who invented Fake News | NYT Opinion. YouTube. Accessed Online.

[13] Clark, B., Doran, M. (2022, January 27). Why Russia and China Build Up Iran. The Wall Street Journal. Accessed Online.

[14] Dwoskin, E. (2022, April 8). China is Russia's most powerful weapon for information warfare. The Washington Post. Accessed Online.

[15] Silverman, C. and Kao, J. (2022) Infamous Russian Troll Farm Appears to Be Source of Anti-Ukraine Propaganda, ProPublica. Accessed Online.

[16] Global Engagement Center. (2020, August). Pillars of Russia's Disinformation and Propaganda Ecosystem. U.S. Department of State. Accessed Online.

[17] Davis, C. (2018, June 19). 'Grassroots' Media Startup Redfish Is Supported by the Kremlin. Daily Beast. Accessed Online.

[18] Chen, K. W. and Cole, J. M. (2019) "CCP and proxy disinformation: Means, practices, and impact on democracies." Accessed Online.

[19] Mwakideu, C., (2021, January 29) China's Growing influence on Africa's media, Deutsche Welle (DW). Accessed Online.

[20] Eisenman, J., (2023, March) China's Media Propaganda in Africa: A Strategic Assessment. Accessed Online.

[21] Cook, S., (2020) Special Report 2020 Beijing's Global Megaphone: The Expansion of Chinese Communist Party Media Influence since 2017. Accessed Online.

[22] Nemr, C and Gangware, W, (2019), Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age. Accessed Online.

[23] Stubbs, J. And Bing, C., (2018, November 30) Special Report: How Iran spreads disinformation around the world. Accessed Online.

[24] Kang, T., (2018 July 25) North Korea's Influence Operations, Revealed, The Diplomat. Accessed Online.

[25] McQuinn, B., Kolga, M., Buntain, C., Courchesne, L., (March 2023) "Enemy of My Enemy: Russian Weaponization of Canada's Far Right and Far Left to Undermine Support for Ukraine," Conflict Report Series. Centre for Artificial Intelligence, Data, and Conflict.

[26] Martin, M. (2021, March 6). Far-Right Misinformation Is Thriving On Facebook. A New Study Shows Just How Much. NPR. Accessed Online.

[27] Network Contagion Research Institute, (2020) Antisemitic Disinformation: A Study of the Online Dissemination of Anti-Jewish Conspiracy Theories. Accessed Online.

[28] Lewis, P., Boseley, S., Duncan, P., (2019) "Revealed: populists far more likely to believe in conspiracy theories," The Guardian. Accessed Online.

[29] Heilwell, R., (2020 April 24) How the 5G coronavirus conspiracy theory went from fringe to mainstream, Vox. Accessed Online.

[30] Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., Starnini, M. (2021). The echo chamber effect on social media. PNAS. 118(9). 1-8. Accessed Online.

[31] Liang, C. S. and Cross, M.J. (2020) White Crusade: How to Prevent Right-Wing Extremists from Exploiting the Internet. Geneva Centre for Security Policy JULY 2020 | issue 11. Accessed Online.

[32] Liang, C. S. & Cross, M. L. (2020). White Crusade: How to prevent right-wing extremists from exploiting the Internet. Geneva Centre for Security Policy. Accessed Online.

[33] Lakhani, S., White, J., and Wallner, C. (2021), The Gamification of (Violent) Extremism: An Exploration of Emerging Trends, Future Threat Scenarios and Potential P/CVE Solutions. Radicalisation Awareness Network, European Commission. Accessed Online.

[34] Englund, G., and White, J. (2023). The Online Gaming Ecosystem: Assessing Digital Socialisation, Extremism Risks and Harms Mitigation Efforts. Global Network on Extremism and Technology. Accessed Online.

[35] US Department of Justice (2023, September 6), 32 Months Since the January 6 Attack on the Capitol. Accessed Online.

[36] Graphic Team (2020 October), Step Into my Parler: Suspected Russian Operation Targeted Far-Right American Users on Platforms, Including Gab and Parker, Resembled IRA-Linked Operation that Targeted Progressives. Accessed Online.

[37] Gleicher, N. (2020 June 4) Labeling State-Controlled Media On Facebook. Accessed Online.

[38] Meta, (2022 October 4) Updated: How fact-checking works. Accessed Online.

[39] Center for Information Technology and Society (2021) Protecting Ourselves from Fake News: Fact-Checkers and their Limitations. Accessed Online.

[40] UK Government (2022). Online Safety Bill. Accessed Online.

[41] Counter Terrorism Preparedness Network and United Nations Office of Counter Terrorism (2023) 'CBRNE Post-Exercise Report'.

[42] London Resilience Communications Group Framework (2021). London Resilience Partnership, p.6.

[43] UK Government Counter-Disinformation Toolkit (2021). RESIST 2. Accessed Online.

[44] Notable quotations about how quickly falsehoods spread have been attributed to several famous people, such as Mark Twain and Winston Churchill, however, scholars note the earliest aphorism to Jonathan Swift writing for The Examiner in 1710.

CTPN
COUNTER TERRORISM
PREPAREDNESS NETWORK