Monitoring & responding to information ecosystem incidents: A conceptual framework understanding information ecosystem risk and leveraging academic expertise for information incident response

Jennie Phillips
Media Ecosystem Observatory
McGill University
jennie.phillips@mcgill.ca

Esli Chan
Media Ecosystem Observatory
McGill University
esli.chan@mcgill.ca

ABSTRACT (150 words)

Our digital information ecosystem shapes the flow of information, the spread of disinformation, the power of adversarial actors, truth, trust, and democracy itself. Characteristics of this ecosystem impact crisis prevention, mitigation, preparedness and response; yet, research on the intersection between digital information ecosystems and crisis and emergency management is scarce. The capacity to deliver and respond to incidents in the information ecosystem is crucial in combating emerging digital threats, such as foreign influence, misuse of generative AI, and online extremism. This paper addresses these challenges by defining the digital information ecosystem and information incidents as they relate to crisis and emergency management and provides an interdisciplinary information incident response framework that integrates conceptual academic research with practitioner perspectives for improved crisis response.

Keywords

Information ecosystem, information incident, social media, social network analysis, crisis response, interdisciplinary

INTRODUCTION

Our information ecosystem shapes the information we receive, how much we receive, and who we receive it from. It dictates the information we see and don't see, the dominant versus marginalized voices, and the ability for disinformation to spread. In a crisis context, the nature of our ecosystem determines our ability to disseminate life-saving information, to communicate with the public, and mitigate the spread of harmful messaging. A recent federal investigation indicates that disinformation, endemic to the online information environment, is the "single biggest risk to our democracy" if it remains unaddressed (Hogue, 2025). Threats, like disinformation, as well as generative AI, or influence from foreign and domestic actors, possess the potential to become *information (ecosystem) incidents* (defined later), which can trigger a cascade of deleterious consequences with minor to severe outcomes. During an election, for example, foreign interference may involve spreading false narratives about the security of the election process or technologies or blackmailing and suppressing transnational diaspora groups to influence their vote (Privy Council Office, 2024). These information incidents pose a significant threat to peaceful, free and fair democratic elections and the integrity of the election process. In other scenarios, such as in the United Kingdom, misinformation played a fundamental role in a nationwide surge of far-right protests that occurred following the Southport stabbings in July 2024 (Murray et al, 2024; Otis, 2024).

While the body of research is significant on the intersection between crisis and emergency management with social media, less is known about the relationship with the wider digital information ecosystem and its impact on public life. Combined, detecting and studying information incidents is challenging and requires collaboration between academics, researchers, and practitioners. In response to this challenge, we develop a conceptual yet practical framework by leveraging interdisciplinary expertise to respond to information incidents in the digital ecosystem. Our approach lies at the intersection of disaster and emergency management, information ecosystem studies and knowledge management. It expands on existing digital and information ecosystem literature by pinpointing the lifecycle of information incidents and how they can disrupt online networks and impact everyday life. It implicates the importance of the digital ecosystem in the information systems for crisis response and management (ISCRAM) community by introducing a new conceptual and practical framework to address evolving information incidents.

A. Defining the Digital Information Ecosystem

What is information?

We describe information as content created by an individual or organization that can be shared. Information can vary from an evacuation alert regarding a natural disaster to a press release regarding a planned political protest. The timing and accuracy of information can dictate social instability and public safety. The information we create, share and consume has the ability to mobilize and empower some communities or disempower and marginalize others. Information does not exist in isolation - it evolves in the relationships and ecosystem constructed between its creators, disseminators, and consumers.

What is an information ecosystem?

Ecosystems consist of a collection of complex relationships and networks between subsystems that coexist to achieve a central purpose. We define an *information ecosystem* as the sum of complex, yet analyzable entities (individuals or organizations) and relationships found in and enabled by the platforms that enable the creation and sharing of and engagement with information (Bridgman et al, 2023). Entities shape but are also shaped by others within the ecosystem. Relationships between entities are innately complex, as each entity exists within multiple communities and across multiple platforms. For example, a politician like Chrystia Freeland is part of a federal government and a Liberal Political Party; she may also be part of local communities, interest blogs, or a fitness group.

What is a digital information ecosystem?

The focus of this paper is on digital information ecosystems - the entities and relationships that exist online that are technologically enabled by digital and legacy media platforms. Digital platforms include social media sites like X, Instagram, YouTube or Facebook, podcasts, blog posts, and online news sites. Previous literature has already

highlighted how the digital nature of the creation and distribution of information shapes information itself and interpretations of reality (McLuhan, 1964; Postman, 1968 as cited in Strate, 2021). Digital and media systems impact the flow of attention and relationships in an ecosystem (Zuckerman, 2023). Much of this existing literature is limited in its assessment of the intervention of information incidents, where pieces of information can disrupt the ecosystem and negatively shape public life. Through integrating emergency and crisis management literature into the study of digital ecosystems, we intervene by providing an interdisciplinary and practical framework to analyze and assess disruptions in the digital information ecosystem.

B. Structural and Dynamic Dimensions of Digital Information Ecosystems and Risk

The structural and dynamic dimensions of digital information ecosystems shape incident response. The *structural dimension* refers to the placement of entities in relation to one another. Entities that are close together have a strong relationship by sharing and discussing similar issues. Entities that are larger than others receive more engagement than others, such as politicians or influencers. Groupings and clusters of entities represent an online community, formed around political affiliations, ideologies, or geographic location. *Dynamic dimension* refers to factors that influence the fluid and evolving nature of our information ecosystems - such as how entities and relationships change over time, the rate and spread of information depending on its content and context, the accumulation, growth and collapse of community, and country or platform-specific regulations that restrict or enable information flow.

Evaluating both of these dimensions sheds important insights on how external influences or specific individuals disproportionately hold power over the digital information ecosystem and the broader public. In particular, the Canadian digital information ecosystem has very high engagement with the Canadian public – four out of five Canadians are actively on social media (Canadian Digital Media Research Network (CDMRN), 2024a). Yet, analysis of information sharing power dynamics highlights a drastic inequity in voices. The Gini coefficient, a measure typically used to measure income distribution, represents the distribution of information and engagement when applied to the Canadian information ecosystem. Ongoing study shows that 90% of the online conversation in Canada stems from 10% of the accounts in the ecosystem, representing a massive power imbalance in the conversation (Ibid).

Monitoring and understanding the structural and dynamic dimensions of the information system offers invaluable insights on preventing, mitigating and responding to crises or disasters. For example, evaluating the structure of clusters of anti-vaccination communities enables insight into the scale of their conversations, the extent conversations occur in isolation of echo chambers or are transposed into other communities, and the scale and scope of the individuals and organizations included in that conversation. Additional dynamic dimensions such as online polarization, toxicity and segmentation can be indicative of increasing public tensions and escalating risk of civil unrest. These insights can be used to gauge and anticipate the associated behaviours of a community (or cluster).

C. Information Incidents

Digital information ecosystems are frequently at risk of disruption – whether it's the spread of divisive narratives by a foreign state actor, the release of AI-generated false images of a disaster area, or conspiracy theories that trigger a shift in public behaviour like the anti-vaccination movement during COVID-19. These stories and events are *information (ecosystem) incidents.* These incidents disrupt the information ecosystem by significantly impacting the regular flow or integrity of information, leading to potential or actual harm to the public, government, democracy, or the broader information ecosystem. Information incidents are not to be confused with cyber incidents, such as DDOS, ransomware, and malware attacks, hacking, and phishing scams. Cyber incidents particularly target the infrastructure of online systems, rather than informational content.

Information incidents are the by-product of threats to and vulnerabilities that exist within our information ecosystem. A *threat* is a potential event in the information ecosystem that may cause harm to individuals and/or their communities, or to the broader population, to social stability and trust, or to democracy itself. A typology of threats, for example,

would include mis- and disinformation, malinformation, foreign influence, the use of AI to manipulate media and/or generate deep fakes, extremism online, bots, and platform censorship. For example, online astroturfing, the disguise of corporations as grassroots or non-profit organizations on social media platforms, is an exemplary threat to the information ecosystem. Climate change astroturfing, for example, where oil and gas corporations masquerade as grassroots social movement actors to advance extractive interests, can mislead the public by creating a false sense of social civic mobilization (Solomun et al, 2025).

Vulnerabilities are characteristics within the information system that render it susceptible to threats. A typology of vulnerabilities includes the extent of online presence of existing contentious figures and communities that can sow social division and polarization, lack of platform regulations or cybersecurity measures, weak digital literacy, or poor public communication protocols when it comes to disinformation. Polarization, a dynamic characteristic of ecosystems, can be a vulnerability. For example, the more an information ecosystem is divided into isolated, non-overlapping communities, the less entities are exposed to diverse viewpoints and information sources. This homogenization can lead an ecosystem to segment into self-reinforcing communities, such as echo-chambers, and an increase in the concentration and spread of disinformation (Törnberg, 2018).

What are characteristics of information incidents?

Scholars have presented a variety of criteria that allow responders to evaluate the relevance, urgency, and impact of incidents. We assess the following aspects as crucial to assessing and triaging information incidents: timeframe, engagement, intervention efforts, scale, scope, impact, severity, likelihood, uncertainty, actor type, actor motive, learning potential, and complexity. Timeframe particularly assesses the rate of which an event occurs, the rate the incident spreads and escalates and is "spreading throughout the ecosystem" (CDMRN, 2024b), while engagement describes the key actors that are responsible for responding to an incident. Intervention efforts evaluate the resources that would be required to respond to the incident (Ibid). Scale refers to the size of the population potentially impacted (Ibid; Public Safety Canada, 2024), while scope evaluates the nature of this population (CDMRN, 2024b). Impact measures the nature of harm (Amazeen, 2023), and severity measures the degree of harm that the incident may cause (National Institute of Standards and Technology, 2012). Likelihood evaluates the chance or probability that the incident may occur (Hillson & Hulett, 2024), linked to uncertainty - the amount of information available to assess the incident (Ibid). Actor type and motive consider the type of actor or source of the incident and their intentions related to the incident (Terp & Breuer, 2022; Lif et al, 2020). Learning potential considers how the incident may be an opportunity to prepare for future incidents and its ability to strengthen the overall information ecosystem (CDMRN, 2024b), while complexity considers how all these various elements are intertwined, making a potential incident response more difficult (Ibid). Together, these characteristics enable incident responders to better parse and understand the nature of information incidents and make informed decisions in their incident monitoring, detection, and response. These characteristics inform the basis of the "Detect" section of the information incident response framework, and the decision matrix for incident declaration and triage (Table 1).

A CONCEPTUAL FRAMEWORK FOR ACADEMIC-LED INFORMATION INCIDENT RESPONSE

This framework outlines an innovative and practical approach to detecting and responding to information incidents. It parses out specific steps, resources required, and stakeholders required at different processes to address the evolving nature of information incidents. Our approach prescribes a method to enable academics and practitioners to conduct and deliver results for information incidents in near-real-time and respond to targeted needs as they should emerge and evolve.

Methodology

This framework is developed by combining best practices from information ecosystem studies, real-time media monitoring practices, and the media and communications literature, with theory and operational approaches from the field of disaster and emergency management. Specifically, this framework is constructed on many building blocks

associated with creating an emergency management program. It leverages many standard procedural and operational techniques, including the development of an incident response protocol and standard operating procedures, establishing roles & responsibilities, surge capacity identification, building an incident notification system, and identification of activation thresholds. Risk management theory is used to generate a variation of a risk assessment matrix, our decision-making matrix for incident declaration & triage classification and triage matrix (see table 1). Findings from case study research on digital humanitarian and digital advocacy networks is used to generate and conceptualize the model for distributed situational awareness and investigation, i.e. leveraging an academic network to collectively monitor the information ecosystem for incidents, and forge temporary remote research teams to microtask the research process and enable more timely response (Phillips & Verity, 2016; Phillips, 2018).

Enabling Infrastructure

This conceptual framework begins with a non-exhaustive list that serves as critical infrastructure and resources essential to enabling aspects of the information incident response:

- **Information Ecosystem Monitoring & Detection Capacity:** The ability to conduct distributed situational awareness through a network (i.e. crowdsourced reporting), internal social media monitoring, social media analysis through digital observation, and ongoing evaluation of population attitudes, perceptions and information consumption habits.
- **Public notification system:** A structured system to notify the public through online presence (e.g. social media, website) and through amplifiers: entities that can share notifications and updates to a broader yet targeted network. Amplifiers are considered to be influential contacts, whether independent individuals, media, or civil society organizations.
- **Internal Response Capacity**: Internal response capacity relies on three primary roles: incident commander, an incident command team, and communications staff. The *incident commander* must be able to provide decision-making regarding declaration, classification and scale of an incident, declaration of a response, overall design and coordination of the investigation, research advisory and feedback, investigation synthesis and summary into debrief. The *incident command team* should be individuals with subject-matter expertise, are social media savvy, and possess the capacity to conduct rapid research and analysis in line with the overarching purpose(s) of their investigation. *Communications staff* should be individuals who share incident notification, updates, contacts, key findings quickly and to a large audience; disseminate investigation findings through media contacts and influential entities in the information ecosystem.
- **Surge Response Capacity**: This includes the capacity to rapidly scale and disseminate research, fundamental to expert-led, rich investigation on a short turnaround basis. This capacity can be built through the concept of a *coalition*, i.e. a vast, interdisciplinary network of academic and practitioner experts that can facilitate a) *detection and monitoring* through information ecosystem monitoring & detection capacity, b) *response* through collaboration and investigation, c) *amplification* through dissemination of research findings to broader networks, and d) *education* through sharing public awareness and education content. Core to the coalition is the *incident response team*. Team members should possess subject-matter and research expertise and the capacity to conduct and share research quickly.
- **Policies, Protocols and Templates:** A series of policies and protocols are fundamental to guide the incident response process, data collection approaches, communications products and collaboration. Examples of key documents include: *Information Incident Protocol* - outlines all steps and requirements needed to respond to incidents, *Memorandum of Understanding* - mutual agreements on the management of intellectual property, expectations for collaboration, and compensation if applicable; *Communications Protocol* - outlining communications process aligned with the incident response process, core communications tools and platforms, and media outreach guidance; *Rapid Response Survey Protocol* - to activate and launch a rapid response survey as described in latter sections); *Incident Response Team Guidance* - key questions to address first activation and purpose; *Research Plans and Timelines*; and *Incident Response Templates* - for incident notification and update to share findings throughout the investigation.

The Five Stages of Information Incident Response

This information incident response process consists of five stages:

1. **Monitor & Detect** - ongoing observation of the information ecosystem for contentious topics, trending stories, and vulnerable or threatening entities online that could trigger an incident;
2. **Declare** - decision making to determine whether to declare an incident and activate a response, based on the characteristics of the incident;
3. **Activate** - initiating response by aggregating incident response team members to design and plan the investigation, notifying the public that an investigation is in process and beginning data collection;
4. **Investigate** - conducting and sharing investigation updates in near real-time to shed insight on the nature, cause and potential impacts of an incident;
5. **Debrief** - synthesizing all research findings into a debrief of the full investigation to provide a bird's-eye summary of the incident and lessons learned.

1. Monitor & Detect

Monitoring and detection involve conducting ongoing observation of the information ecosystem to identify ecosystem threats that could become incidents. While monitoring, threats include anything from trending stories to contentious topics that could trigger or relate to an incident. While real-time detection of incidents is difficult without a heavily resourced organization, this approach leverages a distributed approach to data collection to achieve detection as close to real-time as possible.

Observation is conducted through a blend of data collection methods outlined as follows:

- **Crowdsourced reporting** - establishing relationships with research networks and coalitions to identify a potential or actual incident (see the discussion about *the coalition* above)
- **Digital Threat Tipline** - an open form for the general public to report on emerging threats and incidents as they see them – the "see something, say something" approach
- **Manual In-House Social Media Monitoring** - ongoing manual data collection of the social media and news outlet ecosystem through individual monitoring across all major social media platforms and accounts to detect emerging threats and incidents
- **Ongoing tracking survey** - monthly nation-wide survey seeking to detect shifts in population level attitudes, beliefs and information consumption habits, combined with capturing awareness of impact high profile stories in the ecosystem
- **Automated Social Media Monitoring -** using an ecosystem observation approach through near real-time data collection and analysis of information shared and engagement with the most influential accounts across social media platforms.

Depending on the state of current affairs, e.g. normal operations or event specific operations (situations where the likelihood of simultaneous or consecutive incidents is likely, like an election), the incident command team meets daily to weekly to review incoming reports and observations of the ecosystem to detect incidents.

2. Declaration

Once a potential incident is detected, the incident commander in collaboration with their research team, embarks on the following decision making process:

A) Declaration of an incident - A potential incident is declared on a case-by-case basis using the decision making matrix identified in table 1. Criterion for evaluation include:

- **Spread** - the veracity (speed), scope (across platforms and communities) and scale (level of engagement)
- **Incident Complexity** - the extent an incident seems to be a one-off (acute) versus part of a more sophisticated and/or coordinated intervention over time (complex)
- **Potential for harm** - anticipated level of risk to the safety and security of individuals and communities exposed to (or potentially exposed to) the incident
- **Response requirement & complexity** - ability to provide valuable and timely insights, and scale of resources required

Table 1. Decision making matrix for incident declaration & triage

Criterion	Level 1 (Minor)	Level 2 (Moderate)	Level 3 (Major)
Spread	Slow spread and activity localized or niche communities only.	Medium spread with noticeable engagement and activity across one or two platforms with some media and influencer attention.	Rapid or viral spread and activity across multiple platforms with major media and influencer attention.
Incident complexity	A single simplistic misleading claim or manipulation.	Moderately deceptive claims or manipulations that may include partial truths mixed with falsehoods.	A sophisticated and coordinated overlapping set of claims or manipulations.
Potential harm and impact	Minor risk to any group or the public at large.	Could cause moderate public concern or confusion, with potentially significant risk to specific groups.	Could undermine election integrity, incite violence, or severely destabilize public trust.
Response requirement and complexity	Contextualization and clarity are sufficient to address.	Requires a multi-disciplinary team to address.	Requires immediate large-scale mobilization of a wide team.

B) Triage of the incident - The severity of the incident, i.e. the anticipated impact of the incident on the information ecosystem, is triaged into one of three levels (using the assessment criteria listed above):

Level 1: **Minor Impact,** no activation of the incident response team
Level 2: **Moderate Impact**, small incident response team is activated (3-4 individuals)
Level 3: **Major Impact,** large incident response team is activated (5-7 individuals)

C) Categorization of the incident - Once an incident is declared, it is categorized into an incident type. Examples of potential types of incidents include:

Foreign influence: Efforts by external state or non-state actors to influence discourse in Canada.

Domestic manipulation: Organized campaigns by Canadian actors to distort public perception or suppress divergent views.

Disinformation: Deliberately false or manipulated information.

Misinformation: False information shared without the intent to deceive (while important, misinformation often falls outside the "covert manipulation" scope unless amplified by coordinated manipulative tactics).

Conspiracies and propaganda: Content leveraging ideological or conspiratorial beliefs to shape narratives with specific objectives.

Platform manipulation: Use of bots, coordinated inauthentic accounts, or malicious techniques to artificially inflate engagement metrics. Platform-led manipulation is also in scope.

Synthetic media: Audio-visual content convincingly altered or generated to misrepresent reality, includes text, video, audio, and images.

Extremism online: Use of disinformation to advance radical or extremist ideologies, often linked to calls for violence or real-world harm.

Table 2 below provides an example of how some of these threats can manifest during different types of events:

Table 2. Example Information Ecosystem Threats for Election and Natural Disaster Events

Threat	Election Period Example	Natural Disaster Example
Bot activity	Surge of manufactured online support during a political campaign	Surge of manufactured climate denier narratives drowning out wildfire mitigation campaign
Generative AI / Large Language Models (LLMs)	Deep fake photo defaming a political leader	Deep fake video showing false footage of a disaster affected area
Foreign Influence/Interference	Disinformation campaign designed to undermine democracy	Leaked documents exposing gaps in emergency response designed to undermine public trust in public officials
Extremism online	Surge of extreme-right narratives during an election promoting white supremacist attitudes	Surge of white supremacist narratives targeting vulnerable communities affected

Categorization is used to guide the selection and mobilization of resources. A Level 1 bot-related incident response, for example, involves sharing awareness raising and learning content about bots, how to to detect and "when to care" content, combined with key contacts to reach out to for support on how to respond or learn more, are shared.

D) Declaration of response activation - The decision to declare a response activation is made if all the criteria (at minimum) are met:

- Little to no risk to researchers, organization, incident response team members and coalition members (see description above under *surge response capacity*);
- Ability to make a positive impact, i.e. the anticipated outcomes of the investigation can:
  - A) Can minimize the impact of the incident;
  - B) Fill an information gap and enable decision making about the incident in a timely fashion, i.e. shed new insights on the nature, cause or impact of an incident;
  - C) Enable recovery and further prevent potential issues, and enable planning for related events by providing a unique perspective on lessons learned.
- Research does not risk amplifying or worsening an incident, i.e. the risk of drawing more attention to an incident (or latent trending story) is lower than the perceived value added of responding to the incident;

E) Public notification of incident - A public notification is shared through the organization's information dissemination platform (see description of *public notification system* above) to inform the public that an incident has been detected and a response has been activated to conduct an investigation of the incident.

3. Activation

Once declaration of an incident and response is made, activation of the response process involves the following four activities:

A) Activate incident-specific incident response team (IRT) - coalition members with expertise specific to the incident will be solicited for engagement in the response investigation (e.g. individuals and/or organizations with expertise in generative AI will be contacted to engage in response to a generative AI incident),

B) IRT Plan the investigation - the incident command team and specialized coalition members meet within 24 hours of declaration to decide upon the purpose of the investigation, identify and delegate research questions to address to evaluate the nature, cause and impacts of the incident, and a rapid turnaround research plan is developed. Each member on the incident response team is assigned one or more research questions to address in the investigation.

C) Public Notification - A summary of the incident, live timeline (kept up-to-date as the incident progresses) and subject matter expert names, areas of expertise and contact information is shared online via the information dissemination platform.

D) Data Collection Begins - Data collection begins to establish a baseline of the incident through a) incident response survey to assess awareness of, perceptions about and potential impacts of the incident, b) automated social media data collection, and c) manual social media data collection.

4. Investigation

The response to an incident consists of a distributed investigation, i.e. each IRT member leads rapid research and delivers research findings as it happens through *research updates*. An entire investigation is ultimately conducted using this iterative approach, where multiple aspects of research findings are released as they emerge. Once an update is prepared, it is shared with the IRT for peer-review and edit. Each update undergoes two rounds of review before being released through the organization's public notification system.

Investigation also involves expanding the existing data collection approach as new information evolves or is identified. Additional accounts may be added to the dataset to follow and understand. More targeted manual social media research (qualitative) might occur.

5. Debrief

Once an incident has concluded or the IRT agrees that no further investigation is needed or can add additional insights, a debrief is drafted for wide scale distribution. The debrief involves conducting an overall review and analysis of all incident updates (i.e. all pieces of the investigation shared over time) and synthesizing the overall investigation into a short debrief report. This report summarizes the incident, highlights the main findings as it relates to the nature, cause, and impact of the incident, and then provides a series of lessons learned.

Practical Application - Case Study: Federal Elections Monitoring, Detection & Response at the Media Ecosystem Observatory, McGill University

The Media Ecosystem Observatory (MEO) used this framework for their Canadian Federal Election Monitoring & Response project in 2025. The application of this framework is described for each step below:

1. **Monitor & Detect** - MEO prepared various data sources to enable information ecosystem monitoring, including a public digital threat tipline, an automated social media analysis pipeline and manual social media analysis through multiple analytical teams, as well as an internal workflow process to distribute monitoring across teams and encourage information sharing through daily situation reporting.

2. **Declare** - Narratives and emerging stories identified during the monitoring & detection stage, were evaluated and triaged on an ongoing basis as either non-incidents or potential, minor, moderate or major incidents. An exemplary incident detected was the case of AI-generated fake news. Researchers detected a surge in (AI-generated) ads masquerading as legitimate news sources and linked to cryptocurrency scams (mostly on Facebook). This discovery was originally classified as minor, given the volume, scale of engagement and nature of the case, i.e. it was deemed to be more financial than political in nature and ultimately low risk to the electoral process. However, as days remaining within in the election period narrowed, research detected a surge in volume, a shift in the nature of the content from financial to more political (especially linked to the election) and more sophisticated (humourous deep-fakes turned into minutes long videos branded under official news sources like the CBC in Canada). The incident was escalated, and a moderate level incident was declared.

3. **Activation** - In this scenario, activation involved inviting subject matter experts in the network that were specialized in generative AI and social media data collection, especially on Facebook, to join our incident response team (IRT). A meeting was scheduled within 24 hours for experts available to contribute to the IRT, all members were briefed on the current investigation, and a rapid research plan was defined and delegated between IRT members to address some of the questions that emerged about the case. They were also all added to a Slack channel to enable synchronous discussion during the response. Once the IRT was developed, public notification of response activation was initiated through preparation and population of an incident page.

4. Investigation - Investigation began immediately following the IRT meeting, with the first update on the incident released in three days. IRT members contributed in different capacities ranging from digital trace/social media scraping to manual evaluation of all fake news ads collected and analysis capability to advisory on the broader investigation design and findings. The first update was significantly detailed, addressing questions including how the scam was different from related ones, how widespread and influential the incident was (especially for the election), the ability of Canadians to detect it, techniques used to spread it, and Meta's (the proprietary company of Facebook) response? Following this update, subsequent updates were produced within days addressing additional questions related to attribution (who was behind these ads), impact and the legality of these ads and Meta's obligations.

5. Debrief - The debrief aimed to tie all investigations conducted, addressing various research questions into a single post-incident report that summarized and synthesized all incident updates and the relationship between them to provide insights on the origins, character and impact of the incident.

LIMITATIONS

The focus of our framework excludes the physical dimensions of information exchange related to the study of emergency management and public safety; cyber elements of information related to infrastructure management and cyberattacks; and business elements of the digital space such as e-commerce, consumer and financial system. However, we recognize that our framework is still interdisciplinary in nature and may connect with other fields of studies. We also assess that the offline and online spheres are increasingly intertwined, we largely assess the digital dimensions of media to further understand its implications on offline political life and public policy. Further research is also required beyond the response phases of crisis management (i.e. to support preparedness and mitigation, and broader resilience development).

The evolution of this framework is heavily reliant on addressing many associated challenges. For example, the ability to deliver near-real-time awareness through automated social media data collection and analysis is nearly impossible without a substantial shift in platform regulations to enable researchers with more data access. In addition, the need to deliver quality research on a short turnaround in its raw form is, in many ways, counter to academic culture. Researchers are accustomed to working along the time scale of months to years on research projects. Combined, the delivery of research in a fast-paced environment implies the potential for inaccuracy as higher than normal. There remains a need to enhance timely access and quality assurance to research.

CONCLUSIONS & NEXT STEPS

This paper contributes to the three primary areas of scholarship and practitioner development. First, we address the need for a better understanding of digital information ecosystems, information incidents, and the impact on crisis and emergency management. We highlight the need for the conceptualization of information incidents ahead of developing a response framework. Second, we build a conceptual bridge between digital information ecosystem monitoring and response with crisis and emergency management processes. Third, we provide a pathway for identifying and mobilizing a network of academic subject matter experts to design and conduct distributed rapid research. Given the rate at which our digital information ecosystem is changing, the threats to our ecosystem and the cascade of consequences are critical to understand and account for in the crisis and emergency management discipline. It is hoped that this paper sheds light on how threats in the online information ecosystem are interconnected with the evolution of crises to emergencies, and that our framework enables academics and practitioners across disciplines to collaborate on detecting, responding to and sharing timely insights on information ecosystem incidents as they occur.

REFERENCES

Amazeen, M. A. (2024). The misinformation recognition and response model: an emerging theoretical framework for investigating antecedents to and consequences of misinformation recognition. *Human Communication Research*, *50*(2), 218-229. https://doi.org/10.1093/hcr/hqad040

BBC. (2018, January 14). Hawaii false missile alert: 'Wrong button' pushed. BBC News. https://www.bbc.com/news/world-us-canada-42677604

Booth, R. (2025, January 7). Ditching Facebook fact-checkers a major step back for public discourse. The Guardian. https://www.theguardian.com/technology/2025/jan/07/ditching-facebook-factcheckers-major-step-back-public-discourse

Bridgman, A. Abrahams, A., Bergeron, T., Galipeau, T., Lee-Whiting, B., Naushan, H.l, Philips, J., Pehlivan, Z., Park, S., Parker, S., Steel, B., Loewen, P., Owen, T. (2023). *The Canadian Information Ecosystem.* Media Ecosystem Observatory.

Canadian Digital Media Research Network (CDMRN). (2024b). Information Incident Response Protocol. *Project on Information Ecosystem Resilience.*

Canadian Digital Media Research Network. (2024a). *Incident Debrief: Russian Funding of US and Canadian Political Influencers.* Canadian Digital Media Research Network. https://static1.squarespace.com/static/65427f5b140649321cd829e9/t/675860f3c8ffb13de64d8916/1733845241887/MEO-CDMRN-Tenet-Media-Russia-Incident-Report_2024_final.pdf

Harb, A. (2023, August 29). 'Stupid and dangerous': Meta's news ban fuels anger amid Canada wildfires. Al Jazeera. https://www.aljazeera.com/news/2023/8/29/stupid-and-dangerous-metas-news-ban-fuels-anger-amid-canada-wildfires

Hillson, D. & Hulett, D.T. (2004). Assessing risk probability: Alternative approaches. *PMI Global Congress 2004 - EMEA.* http://www.projectrisk.com/white_papers/Assessing_Risk_Probability-Alternative_Approaches.pdf

Introne, J., McKernan, B., Corsbie-Massay, C.L., Rohlinger, D., Tripodi, F.B. (2024). *Healthier information ecosystems: A definition and agenda.* Journal of the Association for Information Science and Technology, *75(10), 1025-1040. https://doi.org/10.1002/asi.24949*

Lif, P., Varga, S., Wedlin, M., Lindahl, D., & Persson, M. (2020). Evaluation of information elements in a cyber incident report. *2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 17-26. IEE. https://doi.org/10.1109/EuroSPW51379.2020.00012

McLuhan, M. (1964). *Understanding media: The extension of man.* New American Library. New York.

Murray, J., Al-Othman, H., Halliday, J. (2024, July 30). *Police name three girls killed in Southport stabbing attack.* The Guardian. https://www.theguardian.com/uk-news/article/2024/jul/30/people-in-critical-condition-southport-attack-stabbings

National Institute of Standards and Technology. (2012). *Guide for Conducting Risk Assessments (NIST Special Publication 800-30)*. U.S. Chamber of Commerce. https://csrc.nist.gov/pubs/sp/800/30/r1/final

Otis, J. (2024, August 09). *Covering the U.K. Riots Amid Disorder and Misinformation.* NY Times. https://www.nytimes.com/2024/08/09/insider/uk-riots.html

Privy Council Office. (2024). *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions - Initial Report.* Privy Council Office. https://foreigninterferencecommission.ca/fileadmin/user_upload/Foreign_Interference_Commission_-_Initial_Report__May_2024__-_Digital.pdf

Hogue, Marie-Josée. (2025). *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions - Volume 1 Report Summary.* Privy Council Office. https://foreigninterferencecommission.ca/fileadmin/report_volume_1.pdf

Parker, S., Park, S., Pehlivan, Z., Abrahams, A., Desblancs, M., Owen, T., Phillips, J., & Bridgman, A. (2024). When journalism is turned off: Preliminary findings on the effects of Meta's news ban in Canada. Media Ecosystem Observatory. https://meo.ca/work/cdmrn/when-journalism-is-turned-off

Phillips, J. (2018). Risk in a digital age: understanding risk in virtual networks through citizen-driven digital response networks (DRNs). *International Development Planning Review*, 40(3), 239–272. http://doi.org/10.3828/idpr.2018.18

Phillips, J; Verity, A. (2016). Guidance for developing a local digital response network (DRN*). Digital Humanitarian Network & Office for the Coordination of Humanitarian Affairs, United Nations.* Retrieved from https://app.box.com/s/gj67rid8ys1hdwmst8p05hl3om0d1b75

Public Safety Canada (2024). Federal Cyber Incident Response Plan. https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/fdrl-cbr-ncdnt-rspns-pln-2023/index-en.aspx#sD

Ross, C., Phillips, J., Park, S., Bridgman, A., Chan, E., Zhu, J., Abrahams, A., Bohonos, D., Bergeron, T., Vu, A., Pehlivan, Z., Desblancs, M., Steel, B., & Borges Monroy, I. (2024). British Columbia election information ecosystem project: Baseline report. Media Ecosystem Observatory. https://meo.ca/work/british-columbia-election-information-ecosystem-project-baseline-report

Russill, C., Bridgman A., Hayes, H., Khoo, M., Alrasheed, G., Tollefson, H., Ross, C., Peterson, L. (2024). *Flame Wars: Misinformation and Wildfire in Canada's Climate Conversation.* Re.Climate\https://reclimate.ca/wp-content/uploads/2024/06/Re.Climate-Report-Wildfire-Misinformation-2024.pdf

Solomun, S., Monroy, I. B., Bugiel, J., Chan, E., Gowd, N., Hayes, H. A., Jayme, N. H., Kim, S., Ross, C., & Tollefson, H. (2025). *Climate obstruction: The state and spread of climate disinformation in Canada*. The Centre for Media, Technology and Democracy. https://static1.squarespace.com/static/5ea874746663b45e14a384a4/t/67afa03775c04c3e9cbc2b92/1739563070273/Final+Climate+Obstruction+Report.pdf

Stolberg, S. G., & Perez-Pena, R. (2018, January 13). Hawaii panics after alert about incoming missile is sent in error. The New York Times. https://www.nytimes.com/2018/01/13/us/hawaii-missile.html

Strate, L. (2021). Understanding 'Medium' in the Context of the Media Ecology Tradition. In *MEDIA* (pp. 87-98). Intellect

Sultan, M., Tump, A.N. Ehmann, N., Lorenz-Spreen, P., Hertwig, R., Gollwitzer, A., & Kurvers, R.H.J.M. (2024). *Susceptibility to online misinformation: A systematic meta-analysis of demographic and psychological factors.* Proceedings of the National Academy of Sciences, 121*(47).* https://doi.org/10.1073/pnas.2409329121

Terp, S., & Breuer, P. (2022). DISARM: A framework for analysis of disinformation campaigns. In *2022 IEEE Conference on Cognitive and Computational Aspects of Situation Management (CogSIMA)* (pp. 1–8). IEEE. https://doi.org/10.1109/CogSIMA54611.2022.9830669

Törnberg, P. (2018). Echo chambers and viral misinformation: Modeling fake news as complex contagion. PLoS one, 13(9), e0203958.

Zuckerman, E. (2023). Why study media ecosystems?. In *Understanding Movement Parties Through their Communication* (pp. 169-187). Routledge