Engineering, Construction and Architectural Management

Human-centred cybersecurity for critical infrastructure: the case of the Florida water plant hack

Johan Ninan
Faculty of Civil Engineering and Geosciences, Delft University of Technology, Delft, The Netherlands
Bharadwaj R. K. Mantha
Department of Civil and Environmental Engineering, University of Sharjah, Sharjah, United Arab Emirates and
Department of Civil Engineering, Indian Institute of Technology Madras, Chennai, India, and
Balaji Kesavan
Independent Freelancer, Beaverton, Oregon, USA

Received 7 February 2025
Revised 13 July 2025
Accepted 12 August 2025

Abstract

Purpose – Cyberattacks on critical infrastructure (CI) pose serious risks to societal resilience, requiring a human-centred approach to crisis management. This study examines public responses to the Florida water plant hack by analysing social media discourse and its role in shaping cybersecurity strategies.

Design/methodology/approach – A qualitative case study approach applies the Kübler-Ross five stages of grief model to analyse Twitter posts from the first week following the attack. Abductive thematic analysis identifies patterns in public sentiment, emphasizing the role of social media as a real-time feedback mechanism. Lean principles are integrated to highlight stakeholder-driven cybersecurity improvements.

Findings – Public responses followed a structured emotional progression, from denial and humour to anger, bargaining, depression and acceptance. Social media discourse revealed concerns over systemic vulnerabilities, accountability demands and calls for cybersecurity reform. These insights emphasize the importance of transparent crisis communication, proactive risk management and public engagement in strengthening cybersecurity resilience.

Practical implications – Findings offer actionable insights for the public, media, private sector and government agencies into crisis response planning, fostering trust and resilience in digital infrastructure security by integrating public feedback into cybersecurity planning through structured social media analysis and iterative learning practices.

Originality/value – This study uniquely applies the Kübler-Ross model to cybersecurity crises, offering a novel framework for understanding public reactions. It highlights the role of social media in bridging communication between policymakers and end users and demonstrates how lean thinking can enhance adaptive cybersecurity strategies in CI management.

Keywords Cybersecurity, Lean construction, Critical infrastructure, Crisis, Stages of grief, Social media
Paper type Research article

1. Introduction

Critical infrastructure (CI), such as power grids, transportation networks, water supply systems and flood protection mechanisms, is vital to the economic stability of a country, societal well-being and security. National and international bodies recognize these systems as critical due to the essential services they provide, whose disruption could have severe consequences on public safety, health and economic prosperity. For instance, the US

Engineering, Construction and Architectural Management
Vol. 32 No. 13, 2025
pp. 547-569
Emerald Publishing Limited
e-ISSN: 1365-232X
p-ISSN: 0969-9988
DOI 10.1108/ECAM-02-2025-0213

Department of Homeland Security (DHS, 2020) defines CI as "the physical and cyber systems and assets so vital that their incapacitation or destruction would have a debilitating impact on our physical or economic security or public health or safety". Similarly, the European Programme for Critical Infrastructure Protection (EPCIP) highlights the need for uniform protection levels, minimal single points of failure and rapid recovery arrangements across the European Union (EC, 2006).

The growing interdependencies among CIs amplify their complexity, as disruptions in one sector can cascade into others, exacerbating the impact of failures (Mantha *et al*., 2024; Pescaroli and Alexander, 2016). Moreover, the increasing reliance on cyber-physical integration for real-time monitoring and control, where physical systems are interconnected with cyber systems, introduces vulnerabilities that make these infrastructures susceptible to cyberattacks. Such vulnerabilities can compromise the physical systems they govern, potentially leading to catastrophic failures (Palleti *et al*., 2021). This study critically examines these vulnerabilities of CIs to cyberattacks and explores the implications to ensure the resilience and security of such essential systems. In an era of human-centred digital transformation, social media platforms serve as a crucial medium for connecting end users with policymakers, offering a dynamic space to share concerns, disseminate information and respond to crises in real time. Understanding public responses through social media can provide actionable insights to develop lean-inspired cybersecurity strategies that incorporate public feedback, fostering a more adaptive and resilient approach to managing cyber crises.

Cyberattacks on these CI assets pose a severe threat to physical systems, potentially rendering them inoperable, delegating control to unauthorized entities or compromising sensitive data (Pacheco *et al*., 2019). The interconnected nature of CI, while essential for meeting performance and design specifications, exacerbates these risks. Interdependencies among infrastructures mean that faults or attacks on one CI can cascade into others, leading to complex and unforeseen disruptions (Rinaldi *et al*., 2001). Such escalation can disrupt operations, initiate feedback loops and amplify disturbances across interconnected systems (Palleti *et al*., 2021).

Despite significant advancements in securing networked control systems, existing technologies remain inadequate to address the fast-evolving threat landscape (Stellios *et al*., 2018). Furthermore, as technology advances, malicious actors continue to exploit vulnerabilities, using increasingly sophisticated tools to compromise systems (Tounsi and Rais, 2018). These disruptions inconvenience the public, disrupting daily life and eroding trust in essential services. Efforts to address these cybersecurity challenges vary internationally. For instance, the European Union Agency for Cybersecurity (ENISA) promotes a collaborative, multi-stakeholder approach to securing CI, with an emphasis on public–private partnerships and citizen engagement (Bossong and Wagner, 2017). In contrast, countries such as Japan and South Korea emphasize top-down regulatory frameworks with centralized response mechanisms (Aggarwal and Reddie, 2018). These diverse models of policy and engagement reflect contextual differences in governance, digital infrastructure maturity, and cultural attitudes toward public trust in technology (Krishna *et al*., 2023). However, across these diverse international approaches, it is important to understand community responses to cyberattacks necessitating the need for this research.

Social media analysis can serve as an early detection mechanism, offering valuable insights into public sentiment, concerns and evolving perceptions of cybersecurity incidents, thus playing a pivotal role in shaping adaptive cybersecurity frameworks within the AECO industry. In this context, understanding public reactions to cyberattacks can offer valuable insights for enhancing cybersecurity strategies and future infrastructure resilience. This study seeks to answer two research questions: (1) How does the public respond on social media during a cyberattack on CI assets, and what patterns emerge in their engagement? (2) How can insights from public responses inform human-centred cybersecurity management strategies for future infrastructure projects?

To address these research questions, Section 2 (literature review) critically explores existing research on cybersecurity challenges of CI, cyberattacks as a sociotechnical crisis, to

arrive at research gaps. Subsequently, Section 3 details the research methodology and case selection strategy, in which a case study approach is used focusing on the Florida water plant hack (CISA, 2021; Weber, 2021) due to it having occurred recently and having extensive social media coverage, thereby highlighting the public involvement and reaction to the incident which is critical in the context of this study. Following this, in Section 3, the findings on how people react to cyberattacks from the case study are listed. Section 5 (discussion section) then anchors the findings in existing literature and highlights multiple avenues for theorization. Finally, in Section 6, the conclusions and future work section, the contributions to theory, practice, study limitations and future research directions are discussed.

2. Literature review

The interdisciplinary nature of the topic requires a deeper understanding of multiple facets of the problem in the current context. Therefore, this section is organized into three interconnected subsections, each building upon the previous one and highlighting the continuity and relationships established by prior studies. For instance, Section 2.1 systematically explores the complexities of cybersecurity challenges and their varied implications on CI. Section 2.2 draws parallels from previous studies on how cyberattacks can be considered as socio-technical crises to better understand and analyse them. Finally, Section 2.3 identifies key research gaps and positions this study's contributions, emphasizing the human and emotional dimensions of cyber resilience through a theoretical underpinning of crisis management methodology.

2.1 Cybersecurity challenges of critical infrastructure

CI encompasses systems and functions essential for society's uninterrupted functioning, such as energy grids, transportation networks, water supply systems and smart city technologies (Lehto, 2022). In recent years, cyberattacks targeting CI and critical information infrastructures have become increasingly frequent, complex and targeted, as attackers grow more professional and sophisticated (Tounsi and Rais, 2018). These cyberattacks can disrupt or damage physical infrastructure by infiltrating digital systems controlling critical processes, leading to catastrophic consequences without requiring a physical assault. Such attacks may not only damage physical systems but also pollute environments, disrupt vital services and compromise public safety.

The evolving nature of cyber threats compounds the challenges of defending against these attacks. Identifying the source, motive and trajectory of an attack is notoriously difficult due to the global scope of cyberspace and the blurred boundaries between national, international, public and private interests (Lehto, 2013). Rapid technological advancements further complicate this landscape (Garcia de Soto *et al.*, 2022), making it difficult to anticipate and mitigate new forms of threats. While existing literature emphasizes intrusion detection and prevention methods (Baykara and Das, 2018), these measures are often inadequate to address the dynamic and pervasive nature of modern cyber threats.

Human factors play a significant role in cyberattacks, often serving as the weakest link in cybersecurity. Reports indicate that employee errors account for a majority of data breaches, frequently exploited through social engineering tactics (Romanosky, 2016). At the same time, attackers leverage sophisticated techniques to exploit cyber-physical systems in critical sectors, such as energy, water and transportation, causing disruptions with far-reaching implications for public safety, economic stability and trust in essential services (Stellios *et al.*, 2018). For instance, cyberattacks have the potential to trigger car accidents, disrupt electricity grids or contaminate water supplies, highlighting the severe societal impacts of such crises (George *et al.*, 2024).

Technical vulnerabilities in CI systems commonly stemming from the use of legacy hardware and software, insufficient authentication protocols and poor segmentation between

IT and operational technology (OT) networks provide an additional context for human responses (e.g. Sonkor and García de Soto, 2021). Systems such as programmable logic controllers (PLCs), supervisory control and data acquisition (SCADA) and human–machine interfaces (HMIs) often lack robust cybersecurity measures because they were not originally designed with digital threats in mind (Stellios *et al*., 2018). For example, remote access tools such as TeamViewer or Virtual Network Computing (VNC) are frequently used for convenience yet are rarely protected with multi-factor authentication or secure configuration (Tounsi and Rais, 2018). These technical weaknesses can be considered as an important contextual factor affecting the emotional response of the public. Thus, the growing complexity with overlap of technical and social vulnerabilities, increased frequency of attacks and severity of cyberattacks on CI necessitate framing them as crises.

2.2 Cyberattacks as socio-technical crises

Crisis, as a concept, encapsulates human reactions to significant disruptions or misfortunes, ranging from personal losses to large-scale societal events. Multiple frameworks help understand crisis such as Protective Action Decision Model (PADM) emphasizing behavioural decision-making under threat (Heath *et al*., 2018), sensemaking theory capturing how individuals and groups interpret ambiguous events (Maitlis and Christianson, 2014) and Situational Crisis Communication Theory (SCCT), examining how organizations can strategically manage reputational threats by aligning response strategies with the type and attribution of crisis responsibility (Coombs, 2007). However, in this research the Kübler-Ross five-stage model was selected because of its structured articulation of emotional trajectories during crises, which aligns closely with the research goal of understanding public sentiment as expressed on social media. The strength of the Kübler-Ross model lies in its ability to frame emotion as a dynamic and evolving process, which is particularly resonant with the nature of public discourse during cyberattacks on infrastructure projects.

Kubler-Ross (1969) five stages of grief are widely accepted as a framework thatprovides a structured understanding of emotional responses during crises. Originally developed through interviews with terminally ill patients, the stages – denial, anger, bargaining, depression and acceptance – describe the evolving emotional journey of individuals facing profound challenges. While these stages were initially associated with grief and loss, they have since been adapted to various scenarios, including organizational change (Curry, 2003), sudden misfortunes (Jacobsson and Åkerström, 2015) and disruptive events (Gerhardt and Puchkov, 2023), such as cyberattacks in this research.

The five stages are dynamic and non-linear, allowing individuals to move back and forth between them or experience multiple stages simultaneously (Castillo *et al*., 2018; Corr, 2022). Denial serves as a buffer against the initial shock, often followed by anger as individuals process feelings of betrayal or injustice (Blau, 2006). Bargaining represents attempts to regain control or reverse the situation (Gerhardt and Puchkov, 2023). Depression marks the recognition of loss, potentially leading to withdrawal or stagnation, while acceptance signals an emotional evolution, enabling individuals to explore new possibilities and adapt to a new reality (Castillo *et al*., 2018). This model has become a cornerstone for understanding crises because it offers a common language to describe shared emotional experiences. Phrases like "going through a crisis" or "coming out of a crisis" reflect its widespread cultural resonance (Jacobsson and Åkerström, 2015). Furthermore, its adaptability to various contexts, including societal disruptions and technological crises, underscores its relevance as a research framework.

The Kübler-Ross model serves as a robust framework for analysing human responses to crises, including cyberattacks on CI in this research. These events often trigger widespread emotional and behavioural reactions, making them suitable for exploration through the lens of the five stages of grief. This structured approach allows the study to explore not only the emotional evolution of affected individuals but also the broader societal implications of cyberattacks in platforms such as social media. Social media platforms play a pivotal role in

shaping and reflecting collective responses to crises. They provide a dynamic space for individuals to express emotions, share information and mobilize support. During cyberattacks, social media becomes a critical channel for crisis communication, enabling the aggregation of real-time data and the identification of emotional patterns across affected communities (Gashami *et al.*, 2020). The asynchronous and multi-platform nature of social media also aligns with the non-linear progression of grief, where individuals navigate different stages at their own pace and in diverse ways (Wong *et al.*, 2021).

2.3 Research gaps and contributions

While research on cybersecurity threats to CI is extensive, gaps remain in understanding the human and social dimensions of cyber crises. Most studies focus on technical aspects such as network security and intrusion detection (Baykara and Das, 2018; Stellios *et al.*, 2018), with limited attention to how public emotional and behavioural responses influence crisis management. Kubler-Ross's (1969) five stages of grief model, which is widely used in disaster psychology and organizational change (Curry, 2003; Gerhardt and Puchkov, 2023), has not been applied to cybersecurity contexts. In this study, the model was adapted to conceptualize public sentiment as a collective emotional trajectory, tracing how responses unfold across time through identifiable stages such as denial, anger and acceptance. This approach enables a structured analysis of social media discourse during cyber incidents, offering novel insights into public trust, fear and expectations of accountability (Jacobsson and Åkerström, 2015; Wong *et al.*, 2021).

Moreover, while social media platforms shape public discourse and policy responses (Gashami *et al.*, 2020), their role as feedback mechanisms in cybersecurity governance remains underexplored (Lehto, 2022). Cybersecurity frameworks typically neglect lean principles, such as continuous improvement and stakeholder-driven learning, which are foundational in other high-risk domains like construction and manufacturing (Koskela, 1992). Lean thinking conceptualizes system resilience not as a fixed state, but as a product of ongoing adaptation driven by stakeholder input and process diagnostics. In this study, lean principles were extended to interpret social media discourse as a real-time feedback loop, identifying emotional reactions, system critiques and public reform demands as signals for iterative learning. This lean-informed lens allows us to analyse public sentiment not just as expression, but as operational feedback, thereby highlighting inefficiencies, institutional blind spots and opportunities for adaptive response.

This study, therefore, addresses critical gaps by applying the Kübler-Ross model to map the emotional evolution of public response and by leveraging lean principles to conceptualize social media discourse as a tool for real-time, human-centred system refinement (Castillo *et al.*, 2018). Using the Florida water plant hack as a case study, it was shown how social media reveals both emotional distress and crowdsourced reform efforts – providing insights for more responsive crisis communication, trust-building and policy development. Together, these frameworks advance an interdisciplinary, adaptive approach to cybersecurity governance that treats emotional and technical feedback as interdependent elements of resilient infrastructure management (Blau, 2006).

3. Research setting and method

This section outlines the decisions made regarding research design, case selection, data collection and data analysis. The study employs a qualitative case study methodology aimed at theory elaboration – appropriate for research that seeks to deepen and refine existing theoretical frameworks in underexplored domains (Yin, 2018; Ridder, 2017). A single in-depth case of the Florida water plant hack was selected due to its capacity to provide rich, contextual insights into socio-technical crisis responses. Case studies are particularly valuable in complex settings like cybersecurity, where interrelated social, technical and institutional

factors must be examined holistically (Flyvbjerg, 2006). The research draws on the epistemological and methodological principles outlined by Ketokivi and Choi (2014), as their framework emphasizes the role of theory-building case research in generating conceptual insights, especially in under-theorized domains where empirical patterns emerge inductively or abductively. This aligns with the research goal of developing a novel interpretive framework, based on the Kübler-Ross model and lean principles, to explain public emotional and strategic responses to cybersecurity crises. Figure 1 shows the overview of the research setting and method employed in this study and is described systematically below.

3.1 Attack description

This incident occurred in February 2021, when hackers infiltrated the control systems of a water treatment plant in Oldsmar, Florida. The attackers gained unauthorized access through outdated software and weak security protocols, manipulating the plant's systems to increase the levels of sodium hydroxide, a chemical used to control water acidity to dangerous levels. The attack was thwarted before it could harm the public, but it exposed significant vulnerabilities in CI systems.

3.2 Attack significance and rationale

This case is particularly relevant for addressing the research questions in this paper for several reasons. First, it highlights the growing interdependence between physical and cyber systems in CI, emphasizing the risks posed by cyberattacks to essential services. Second, the incident received substantial social media attention, providing a rich dataset for examining public reactions. Third, it underscores systemic challenges, such as outdated technology and inadequate cybersecurity measures, that fuel public concern and discourse. By analysing this case, the study not only explores the emotional and behavioural responses of the public to such crises but also sheds light on broader implications for cybersecurity management and policy development in CI sectors.

3.3 Means of data collection

To answer the research questions on public responses to the Florida water plant hack, the study sought data that captured both the emotional and behavioural reactions of individuals, as well as broader discussions on cybersecurity policy and infrastructure vulnerabilities. Specifically, it aimed to understand how public perception evolved in response to the cyberattack and how these reactions might inform human-centred cybersecurity strategies. To achieve this, qualitative data on public narratives surrounding the incident were collected to explore their alignment with themes from Kubler-Ross's (1969) five stages of grief. Additionally, the study examined discussions on potential solutions and policy recommendations emerging from public discourse. Social media data captures this rich, real-time dataset, which could reflect public reactions and help us gain insight into the emotional trajectory of responses and the broader societal discourse on cybersecurity risks and crisis management (Reuter and Kaufhold, 2018).

While the tweets analysed in this study are publicly available, ethical considerations were taken into account to minimize the risk of re-identification. In line with established guidelines

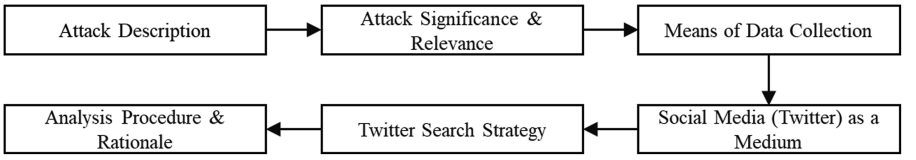

Figure 1. Overview of the research setting and method employed in this study. Source: Authors' own work

for social media research (Williams *et al*., 2017), disclosing usernames, profile information or metadata that can directly link quotes to individuals was avoided. Verbatim excerpts were selected and included only where the content was not highly specific or personal, and where the risk of traceability through search engines was minimal. The study treats public tweets as online naturally occurring data (Ninan, 2020) but follows a conservative ethical approach to protect individual privacy, such as avoiding contact with users, and accessing data through public search tools rather than using APIs or scraping (Bruckman, 2014).

3.4 Social media (Twitter) as a medium

Social media serves as a dynamic platform for real-time public discourse, enabling immediate reactions to cybersecurity incidents, shaping collective memory and influencing policymaker responses. Particularly, the affordances of Twitter, such as short text, hashtags and retweets, facilitate the rapid spread of information, allowing users to amplify concerns and critique systemic vulnerabilities (Yang *et al*., 2018). The platform also fosters participatory engagement, where expert and non-expert voices converge (Halpin *et al*., 2021) to construct shared interpretations of cyber crises. Given its potential for both information dissemination and misinformation, analysing Twitter data provides critical insights into public risk perception, crisis communication effectiveness and policy adaptation in cybersecurity management.

3.5 Twitter search strategy

Specifically, social media data from Twitter during the first week following the cyberattack, from February 8 to February 15, 2021, was compiled. Using a keyword search with the terms "Florida water plant hack," 212 tweets directly related to the event were identified and collected. These tweets provided a diverse range of public reactions, including expressions of disbelief, humour, fear, critiques of systemic vulnerabilities and calls for accountability. This dataset, as naturally occurring data without the intervention of the researchers (Ninan, 2020), offered valuable insights into how the public processes and responds to cybersecurity incidents in real-time.

While modest in size, the sample was sufficient for in-depth qualitative analysis, allowing for iterative coding and constant comparison. As recommended in qualitative research, data collection continued until thematic saturation was reached, i.e. when no new concepts or categories emerged from the dataset (Wutich *et al*., 2024; Guest *et al*., 2006). The selected tweets were rich in emotional and discursive content, enabling us to identify recurring patterns across time. The goal of the study was not statistical generalization but conceptual insight into how emotional trajectories and public feedback evolve during cyber crises. To mitigate bias, tweets were sampled over a consistent time frame, included tweets from all sources in the study period, such as individuals, journalists, experts, etc., and were manually screened for relevance and originality.

By analysing these tweets, the study aimed to capture the evolving emotional and behavioural trajectories of individuals during a cyber crisis. The data also allowed us to explore the collective discourse on social media, shedding light on societal concerns about infrastructure vulnerabilities and expectations for preventive measures.

3.6 Analysis procedure and rationale

Abductive thematic qualitative analysis was employed, a method well-suited for exploring areas where concepts are not yet well-defined and where there is a need to refine key ideas and establish a theoretical framework (Jabareen, 2009). The thematic analysis methodology was integrated into three iterative stages, i.e. open coding, axial coding and constant comparisons, to construct the theoretical model (Groat and Wang, 2013). First, open coding involved systematically breaking down, examining and categorizing data into distinct themes

(Strauss and Corbin, 1990), following a coding pattern influenced by Gioia *et al*. (2013). Efforts were made to ensure that the codes were broadly applicable, decontextualized, mutually exclusive and exhaustive (Morse, 1991), such as fear, disbelief, accountability, etc. Second, axial coding was used to group initial codes into broader categories such as emotional responses, technical critiques, policy suggestions, etc. Third, selective coding integrated these categories with theoretical constructs, producing the final themes aligned with Kübler-Ross stages and system-level concerns. For example, a tweet stating, "*That's terrifying, I've been hearing for years how vulnerable our infrastructure is*" was first coded as "fear" (open codes), then grouped under "emotional reactions to infrastructure weakness" (axial codes), and finally situated within the "Depression" stage of the grief model in the thematic structure. The whole coding process was conducted manually, and discrepancies in theme interpretation were resolved through discussions among multiple coders and constant comparison with prior codes and literature on theoretical frameworks.

The abductive process was anchored in two key theoretical frameworks: the Kübler-Ross five-stage model and lean systems thinking. The Kübler-Ross model provided a structured lens for interpreting the evolution of public emotional responses during the crisis, enabling us to map raw data onto an established emotional trajectory. This facilitated the recognition of patterns, such as denial, anger, bargaining and acceptance, in collective discourse. Complementarily, the analysis drew on lean principles of iterative learning and stakeholder-driven feedback (Koskela, 1992). Public reactions, particularly emotional expressions and reform suggestions, were interpreted not only as responses but as diagnostic feedback, highlighting systemic inefficiencies and institutional blind spots. This mirrors lean's emphasis on continuous improvement and the identification of "waste" in communication, trust and system responsiveness. By treating social media discourse as a real-time feedback loop, the analysis helped surface signals for adaptive reform, consistent with lean-informed approaches to dynamic system design. This iterative process allowed us to ground the findings in existing literature while expanding theoretical insights, thereby enhancing generalizability, improving construct clarity and elevating the theoretical contribution, as suggested by Eisenhardt (1989).

To further some of the qualitative observations, quantitative sentiment analysis was also performed using quantitative techniques. Specifically, first, a structured social media sentiment analysis methodology based on recent advances in natural language processing (NLP) and large language models (LLMs) was performed. That is, each tweet was categorized into distinct emotional dimensions (e.g. anger, denial and acceptance) based on the content of the message. The classification was performed by querying an LLM (GPT-4.1-nano-2025-04-14) with a system prompt that provided the incident context and instructed the model to assign a True/False value to each sentiment category. This binary tagging schema enabled a multi-dimensional characterization of public reaction, reflecting the psychological complexity often observed during societal reactions to cybersecurity incidents.

Second, to illustrate the temporal trends, a timeline plot was generated showing the total number of tweets for each sentiment dimension over the entire study period. Third, the daily frequency of the tweets was plotted by sentiment from the time of the cybersecurity event onward to visualize how public sentiment evolved during the incident response window. Fourth, a word cloud analysis was performed for each sentiment category, aggregating the tweets belonging to that emotion to highlight the most common terms and themes associated with each emotional response. Finally, a compare and contrast analysis was done with the qualitative observations and findings to identify the similarities and differences. Figure 2 shows the pseudo code developed to achieve these aforementioned tasks, starting from importing the data set until the aggregation and analysis of the imported tweet data. Together, these analyses help identify not only the intensity and evolution of different sentiments but also the key topics of discussion underlying each emotional response. By leveraging LLM-powered multi-sentiment tagging on a public social media dataset, this method offers a

```
BEGIN PROCEDURE
    Import data processing libraries
    Initialize sentiment analysis engine
    Load Twitter dataset containing public discourse on the incident

    FOR EACH tweet in dataset:
        Extract textual content

        Analyze tweet for presence of 20 predefined sentiment categories:
            // Categories include: Denial, Anger, Bargaining, Depression etc.
            // Sentiment classifications by querying a GPT-based NLP model with a system prompt and Top20Tags schema.
            // Uses OpenAI action model 'gpt-4.1-nano-2025-04-14'.
            // system_prompt contains context and instructions for assigning the 20 tags.
            // The provided context was:
            //   • An incident report and research goal
            // The instructions were to:
            //   • Assign each of the 20 tags a boolean value (True/False)
            //   • Return the result as a JSON object strictly adhering to the Top20Tags schema

        Generate binary classification (present/absent) for each sentiment category

        Record sentiment classifications in the dataset

        Update analysis statistics

    END FOR

    Aggregate sentiment distribution across entire dataset

    /* The resulting data enables quantitative measurement
       of public reaction patterns following the security incident */
END PROCEDURE
```

Figure 2. Pseudo code for the quantitative sentiment analysis. Source: Authors' own work

scalable, reproducible and nuanced measurement of collective public sentiment, providing unique insights into human-centred cybersecurity challenges.

Although social media data are commonly analysed using automated techniques such as NLP, a qualitative, abductive approach was adopted to capture the nuanced emotional trajectories and context-specific meanings embedded in public responses (Pink *et al*., 2010). The research aim was not to quantify sentiment polarity or detect linguistic patterns at scale, but to map temporally evolving emotional states and interpret tweets as expressions of collective grief, critique or reform advocacy. This interpretive depth, particularly in aligning raw discourse with the Kübler-Ross emotional framework and lean-informed feedback signals, requires contextual sensitivity that current NLP models may not provide with sufficient granularity or theoretical alignment. In addition, manual thematic analysis enabled tracing the shifting meanings over time, detecting figurative expressions such as metaphor, sarcasm or humour, that are often misclassified by NLP models (Weitzel *et al*., 2016), and aligning social discourse with structured theoretical stages. While NLP may offer scalability, the current method better supports the exploratory, theory-building objectives of this study, allowing for a richer understanding of how public emotion, sentiment and critique inform human-centred cybersecurity strategies.

4. Findings

The cyberattack on the Florida water treatment plant provoked a diverse and evolving array of public reactions on social media. These responses, ranging from initial disbelief and humour to fear, critique and calls for action, reveal significant insights into societal attitudes toward cybersecurity risks, the perceived vulnerabilities of CI and expectations for future preventive measures. This can be preliminarily observed in the summarized quantitative analysis results in Section 4.1 (Quantitative Sentiment Analysis). For instance, the findings from this analysis provide a broad overview regarding the emotional dimensions, temporal trends, tweet frequency and common themes through word clouds. However, given the nature of these complex emotional public reactions, several inconsistencies and challenges still persist, and hence, a human in the loop or human oversight is still warranted. Therefore, as mentioned earlier in Section 3.6 as well, the latter part of this section synthesizes these responses into three overarching themes based on the qualitative analysis performed, namely evolving emotional reactions (Section 4.2), critiques of systemic vulnerabilities (Section 4.3), and calls for

accountability and reform (Section 4.4). Figure 3 shows the summarized pictorial overview of the responses systematically described as per the aforementioned categories and described in detail below.

4.1 Quantitative analysis

Figure 4 shows the total number of tweets based on each of the five categories. It can be seen that anger (42%) and acceptance (45%) constitute a significant portion, which can be pursued as the typical alignment with sometimes the extreme and immediate nature of the public reaction to such events. This was further scrutinized with the help of a temporal response and shown in Figure 5. Corroborating the observation made above, a greater number of tweets overall (34% of the tweets on the first day) can be seen immediately after the event occurred, compared to those of the instances at a later stage (12% on the eighth day). To further understand the specifics of how people reach within each of these categories, word clouds were generated for each of the five categories. Figure 6 shows the word cloud generated for the denial category.

While there are relevant phrases that can shed immediate light on the way people express their reaction, there are still several inconsistencies that need to be addressed, which is one of the inherent limitations of the quantitative approach. For example, words like "lol" and "why" clearly depict the respective reaction categories of denial. However, some general terms like "Hunter," "well," and "like" might not truly represent that category or present a partial picture or sometimes even mislead in some instances. This is precisely the reason for human-in-the-

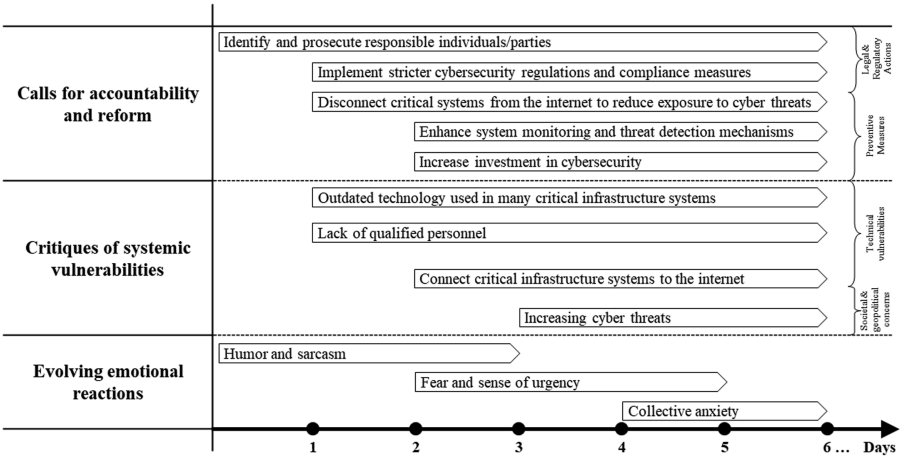

Figure 3. Timeline-based categorization of Twitter responses. Source: Authors' own work

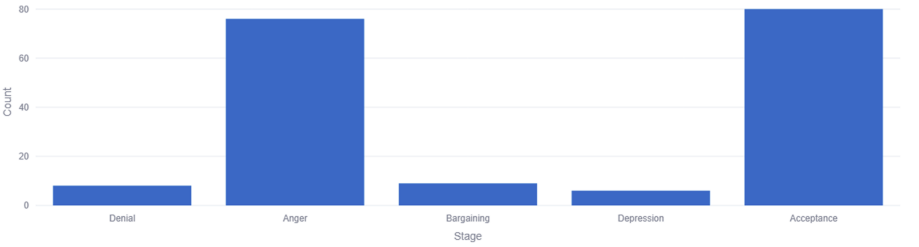

Figure 4. Total number of tweets based on each respective category. Source: Authors' own work

Figure 5. Timeline-based respective categorization of the number of tweets. Source: Authors' own work

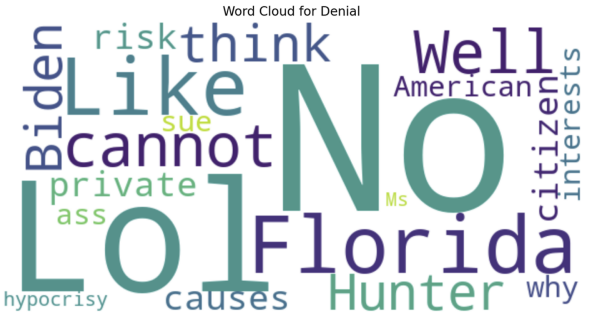

Figure 6. Word Cloud of the most frequently used words within the denial category. Source: Authors' own work

loop and human oversight-based approaches, particularly when LLMs or NLP-based approaches are used for categorization (Xu *et al.*, 2025; Pangakis and Wolken, 2025). This is beyond the purpose and goal of this study and hence not investigated further, but rather a thorough, systematic and comprehensive qualitative investigation was performed, which is described below.

4.2 Evolving emotional reactions

In the immediate aftermath of the attack, many social media users reacted with disbelief, often employing humour or sarcasm to process the event. Posts likened the incident to scenes from science fiction and while these comments were often light-hearted, they underscored an initial struggle to grasp the gravity of the situation. One user sarcastically remarked, "Was it a pHishing attack?" referring to pH as the scale that measures the acidity or basicity of a substance while another quipped, "Skynet is coming!" referring to the Terminator movie franchise. Another user sarcastically highlighted that the government is not doing enough to prevent such kind of attacks, citing previous attacks as below:

> They've only had twenty years since 9/11 to tighten up their stuff. Give it time (Quoted from a tweet dated 9 Feb 2021)

As details of the incident emerged, humour gave way to fear and a sense of urgency. Users began to articulate concerns about the potential consequences of such an attack, particularly the dangers posed by tampering with essential services like water treatment. Many expressed alarm at the ease with which the hackers gained access, with one post stating, "*Why isn't this national news? This is terrifying.*" Others highlighted the critical role of water in daily life, with one user emphasizing, "*Water is life, electricity is convenience.*" Another user remarked:

> That's terrifying, I've been hearing for years now how vulnerable our infrastructure is to attacks like this (Quoted from a tweet dated 9 Feb 2021)

The shift from humour to fear reflects a growing public awareness of the risks posed by cyberattacks on essential infrastructure. The emotional weight of the incident deepened as users contextualized the attack within broader societal and technological vulnerabilities. Some posts speculated about the hackers' intentions, suggesting the attack could be a test for more significant disruptions in the future. *"Someone was just 'testing the fence,'"* one user wrote, alluding to a deliberate probing of systemic defences. Another expressed a broader unease, stating, *"This is the downside of technology . . . It's scary that someone could do this."* Such comments reveal a collective anxiety about the increasing reliance on digital systems and the potential for malicious actors to exploit them.

4.3 Critiques of systemic vulnerabilities

As fear and awareness grew, discussions on social media shifted toward identifying the systemic weaknesses that allowed the attack to occur. A recurring critique was the decision to connect CI systems, such as Programmable Logic Controllers (PLCs), to the internet. One user questioned:

> Why on earth is their PLC network online? Who wants to operate a water treatment plant from home? (Quoted from a tweet dated 9 Feb 2021)

This sentiment was echoed in numerous posts, highlighting a widespread perception that prioritizing convenience over security had left essential systems exposed to cyber threats. Another significant point of criticism focused on the outdated technology used in many CI systems. The Florida water treatment plant reportedly operated on older software, including Windows XP, which is no longer supported with security updates. Users cited this as emblematic of broader underinvestment in cybersecurity for public utilities. One post observed:

> In America, water treatment facilities are widely municipal, underfunded, low-resourced in IT, and don't get anywhere near the cybersecurity attention and support that electricity does. (Quoted from a tweet dated 8 Feb 2021)

This critique reflects public frustration with what is perceived as systemic neglect of cybersecurity in critical sectors. In addition to technical vulnerabilities, users also pointed to a lack of qualified personnel as a contributing factor. Posts highlighted the challenges faced by smaller municipalities in attracting and retaining skilled cybersecurity professionals. This issue was framed as a structural problem that extends beyond individual incidents, reflecting broader concerns about the allocation of resources and expertise in public sector cybersecurity.

The critiques were not limited to the technical domain. Some users linked the incident to broader societal and geopolitical concerns. For example, one post suggested that the attack could be part of a larger trend of increasing cyber threats facilitated by international collaborations, stating, *"They'll want to increase it a lot more now, since *** [name of country A] has deals with both *** [name of country B] and *** [name of country C] to improve their cyber capability."* Such comments illustrate the interplay between local incidents and global cybersecurity narratives in shaping public discourse.

4.4 Calls for accountability and reform

The cyberattack also catalysed calls for accountability and systemic reform. Many social media users demanded swift action to identify and prosecute those responsible. *"Find out who did it and prosecute them to the fullest extent of the law,"* one user urged, reflecting a widespread desire for justice and deterrence. Others emphasized the need for preventive measures to ensure such incidents do not recur. One post asked:

> What is being done to make sure this doesn't happen again? Anywhere else need to be monitored for hacking into such systems? (Quoted from a tweet dated 9 Feb 2021)

Suggestions for reform ranged from technical solutions, such as disconnecting critical systems from the internet to broader policy changes. Users called for increased investment in cybersecurity, both in terms of technology and personnel. There is a need for layered security measures that can mitigate the impact of breaches even when initial defences are compromised. Public discourse also highlighted the importance of communication and transparency during such incidents. Many users expressed frustration with the perceived lack of timely information from authorities, suggesting that clearer and more proactive communication could help mitigate public fear and confusion. This sentiment was encapsulated in one post: *"People need to know what's happening and what's being done to protect them. Silence only makes it worse."* However, responding to a press conference on the cyberattack, one user responded,

> Everything else aside, that was one of the best press conferences about a computer attack I've seen in a while. Explained the scope, what happened, etc in a technically comprehensible way. (Quoted from a tweet dated 8 Feb 2021)

The tweet highlights that transparent communication can help manage people who are scared with a lack of adequate information on the scale of the crisis.

5. Discussion

The findings from the Florida water plant hack highlight the different reactions of people. These reactions are anchored in the five stages of grief model by Kubler-Ross (1969) for a systematic understanding, followed by a discussion of the implications for cybersecurity management, as described below.

5.1 Understanding how people react to cyberattacks

The findings are situated within Kubler-Ross's (1969) five stages of grief framework, emphasizing its adaptability for understanding emotional and behavioural responses to large-scale disruptions.

(1) *Denial:* Denial emerged as the dominant initial response, characterized by disbelief and minimization of the event's severity. Social media posts often trivialized the attack, using humour and sarcasm to deflect its seriousness. For instance, users joked about the attack as if it were a plot from a science fiction movie or a video game. These reactions align with Kübler-Ross's assertion that denial acts as a psychological buffer, allowing individuals to process shocking events incrementally (Blau, 2006). This stage also reflected a broader societal challenge: the public's limited understanding of cybersecurity risks. Denial in this context was not merely a refusal to acknowledge the event but also a lack of awareness about the potential implications of cyberattacks on CI. Humour served as a coping mechanism, temporarily alleviating the fear of systemic vulnerability. However, such responses also underscore the need for improved public education on cybersecurity threats. From a policy perspective, denial highlights the importance of pre-crisis communication strategies. Public awareness campaigns that demystify cyber risks and explain their potential consequences can mitigate the initial disbelief and enable faster transitions to constructive responses. Such efforts should focus on making technical information accessible and relatable, fostering a baseline understanding of cybersecurity among the general population.

(2) *Anger:* As the reality of the attack set in, public reactions shifted to anger. This stage was marked by frustration directed at systemic vulnerabilities, such as the use of outdated technologies like Windows XP in critical systems. These technical

oversights – particularly the continued use of unsupported operating systems and unsecured remote access – were widely discussed on social media, reinforcing the perception of institutional negligence. The anger from the public thus stemmed not only from the fact of the attack, but from a sense that basic technical precautions had been ignored. Anger in this context was not merely an emotional outburst but a demand for accountability and systemic reform. The anger stage aligns with previous research on crises, where individuals often seek to identify and blame responsible parties (Gerhardt and Puchkov, 2023). This response reflects a broader societal expectation that institutions should prioritize security and reliability, particularly for critical services. The public's frustration with outdated systems and insufficient investments in cybersecurity underscores a disconnect between institutional priorities and societal expectations. Anger also revealed the public's distrust of authorities, exacerbated by a lack of timely and transparent communication during the crisis. This finding supports existing literature emphasizing the critical role of trust in crisis management (Jacobsson and Åkerström, 2015). When authorities fail to provide clear and accurate information, they risk fuelling public anger and eroding trust, complicating recovery efforts. In the case of the Florida water plant hack, it was seen that anger was directed at the region (Florida), authorities (municipalities) and organizations (water plant and windows) affected by the attack, and it influenced the trust of the public in these entities (Williams *et al*., 2024). For cybersecurity management, the anger stage underscores the importance of proactive measures to address systemic vulnerabilities. Regular audits, timely upgrades to critical systems, and transparent communication about ongoing efforts can help build public confidence. Additionally, involving citizens in discussions about cybersecurity priorities can foster a sense of shared responsibility and reduce feelings of helplessness during crises.

(3) *Bargaining:* Bargaining emerged as a proactive stage where social media users proposed practical solutions to mitigate future risks. Suggestions included disconnecting critical systems from the internet, increasing investments in cybersecurity and enhancing crisis communication protocols. Many of these suggestions were responses to specific technical flaws identified by users, such as the lack of firewalls, outdated SCADA configurations, and insufficient network segmentation. These public critiques show that emotional responses were often coupled with technically informed proposals for reform, underscoring the value of public discourse as a diagnostic feedback mechanism. This stage represents an attempt to regain control and influence the outcome of similar events in the future. The bargaining stage reflects the public's capacity for problem-solving and their willingness to engage in constructive discourse during crises. Unlike the anger stage, which focuses on assigning blame, bargaining emphasizes solutions, highlighting the public's potential as a resource for crisis management. This finding aligns with Gerhardt and Puchkov's (2023) observation that bargaining often involves collaborative efforts to reverse or alleviate the impact of crises. However, the public's suggestions also revealed gaps in institutional preparedness and communication. For instance, the emphasis on disconnecting critical systems from the internet suggests a lack of awareness about existing security protocols and their limitations. This highlights the need for organizations to communicate not only the risks but also the measures they have in place to address them. From a policy perspective, the bargaining stage underscores the importance of engaging the public in cybersecurity strategies. Citizen feedback can provide valuable insights into societal expectations and priorities, enabling organizations to align their efforts with public concerns. This stage also highlights the potential of social media as a platform for crowdsourced problem-solving, where diverse perspectives can contribute to innovative solutions.

(4) *Depression:* The depression stage was characterized by widespread anxiety and a sense of helplessness as individuals recognized the systemic vulnerabilities exposed by the attack. Social media posts expressed fear about the potential consequences, such as water contamination or broader cyber threats. This stage reflects the public's acknowledgment of the risks and their perceived inability to influence outcomes. Depression in this context aligns with Kübler-Ross's description of withdrawal and stagnation during crises (Jacobsson and Åkerström, 2015). Unlike the proactive engagement seen in the bargaining stage, depression marks a period of emotional exhaustion, where individuals focus on the inevitability of risks rather than potential solutions. This stage highlights the psychological toll of cyberattacks on public morale, emphasizing the need for mental health considerations in crisis management. Authorities should recognize that prolonged exposure to crises can lead to emotional fatigue, affecting public resilience and engagement. Providing reassurance through clear and consistent communication can help alleviate anxiety and foster a sense of stability.

(5) *Acceptance:* Acceptance emerged as the final stage, where individuals began to advocate for systemic reforms and long-term solutions. Social media users emphasized the need for increased investments in cybersecurity, improved crisis communication, and proactive measures to safeguard CI. This stage reflects an emotional evolution, where individuals move beyond reactive emotions to explore new possibilities and adapt to a changed reality (Corr, 2022). Acceptance in this context was not passive resignation but an active acknowledgment of the need for change. The public's advocacy for systemic reforms highlights their readiness to engage in long-term efforts to enhance cybersecurity resilience. This finding supports the observation by Castillo *et al*. (2018) that acceptance often involves a shift from emotional responses to constructive action. For cybersecurity management, the acceptance stage underscores the importance of fostering public trust and engagement in long-term strategies. By involving citizens in the design and implementation of cybersecurity measures, organizations can build a sense of shared responsibility and resilience. This stage also highlights the potential for social media to serve as a platform for mobilizing public support and advocacy, enabling collective action toward systemic change.

The findings demonstrate that public responses to a cybersecurity crisis follow a discernible emotional trajectory that aligns with, but also adapts, the Kübler-Ross five-stage grief model. The application of this model in the cybersecurity domain helps capture the collective emotional evolution, from denial and humour to anger, bargaining, depression and eventual calls for systemic reform, visible in social media discourse after the Florida water plant hack. Thus, cybersecurity incidents were conceptualized as emotional, temporal crises rather than purely technical or organizational disruptions. The contribution lies in reconceptualizing public reactions not as isolated attitudes but as staged, temporally ordered emotional responses, which can be anticipated and managed as part of cybersecurity crisis planning. A new affective lean-informed framework is conceptualized for cyber crisis response, offering a complementary framework to existing models focusing on technical and organizational aspects of disruption.

Lean principles such as iterative improvement, stakeholder engagement and feedback integration can be adapted from their roots in construction management to cybersecurity governance. Rather than focus on technical efficiency alone, lean principles enable a conceptualization of public social media discourse as a real-time feedback loop – a mechanism through which emotional reactions, critiques and suggestions are continuously generated and circulated. The findings highlight that community tweets contained crowdsourced solutions, critiques of system design and recommendations for reform, which could help iterate

cybersecurity strategies, mirroring lean feedback loops in design and construction, where end-user feedback is used to incrementally improve systems. This lean perspective helps cybersecurity interventions move beyond static security models and positions cybersecurity resilience as a socio-technical, adaptive process, emphasizing responsiveness over control. While prior work on lean construction emphasizes efficiency and waste reduction, the contribution of this research is in adapting lean as a human-centred, reflexive mechanism to improve adaptive capacity in cyber crisis, which could be extended to other contexts as well. Thus, by systematically exploring the emotional trajectory of public responses, the study links these to actionable strategies, bridging the gap between emotional responses and practical cybersecurity management.

5.2 Implications for cybersecurity management for future projects

The application of Kübler-Ross's five stages of grief to public reactions during cyberattacks offers valuable insights for improving crisis communication and cybersecurity strategies. These implications address the research questions by linking emotional responses to actionable measures:

(1) *Enhancing crisis communication:* The denial and anger stages highlight the critical role of timely and transparent communication during crises. Authorities should prioritize proactive strategies that provide accurate updates, address public concerns and counter misinformation. Effective communication can mitigate initial disbelief, reduce public anger and foster trust, enabling faster transitions to constructive responses. During crises, communication should not only provide factual updates but also address the emotional needs of scared or anxious stakeholders. This involves empathetic messaging, reassuring the public about ongoing efforts and clearly outlining steps being taken to mitigate the threat. Tailored communication can help reduce panic and foster a sense of control.

(2) *Humour as a coping mechanism:* Humour emerged as a significant response to cyberattacks on social media, serving as both a coping mechanism and a way for individuals to stand out in the crowded digital landscape. While humour can diffuse tension and foster a sense of solidarity, it also presents challenges for organizations. They must balance engaging with light-hearted content to humanize their responses without trivializing the severity of the attack. Recognizing humour as a cultural and psychological response allows organizations to approach crisis communication with greater empathy and creativity, fostering a sense of connection with their audience (Sergeeva and Ninan, 2023). This insight is particularly relevant in a social media age, where standing out and maintaining public trust are paramount.

(3) *Building awareness:* The denial stage underscores the need for pre-crisis education and awareness campaigns. Public awareness initiatives can demystify cybersecurity risks and explain the potential consequences of cyberattacks on CI. Increasing awareness not only mitigates denial but also empowers individuals to respond more constructively during crises. These efforts should emphasize practical tips for identifying and reporting suspicious activities, fostering a culture of vigilance.

(4) *Addressing systemic vulnerabilities:* The anger and bargaining stages underscore the public's demand for accountability and systemic reform. Investments in modernizing CI, disconnecting sensitive systems from the internet and employing robust security protocols are essential. Policymakers must also address structural challenges, such as resource constraints and a lack of cybersecurity expertise, particularly in smaller municipalities.

(5) *Brainstorming ideas through crowdsourcing information:* Social media platforms emerged as spaces for brainstorming ideas and proposing solutions during the

bargaining stage. Crowdsourcing information from diverse perspectives can generate innovative mitigation strategies. However, authorities must implement mechanisms to verify the accuracy and credibility of crowdsourced data before incorporating it into decision-making processes. Engaging the public in this way can foster a collaborative approach to crisis management, encouraging individuals to contribute constructively rather than merely reacting emotionally.

(6) *Fostering public trust and resilience:* The depression and acceptance stages reveal the importance of fostering public trust and engagement. By involving citizens in discussions about cybersecurity priorities and demonstrating a commitment to long-term solutions, organizations can build a resilient societal response to cyber threats. Public education campaigns that emphasize the shared responsibility of cybersecurity can further empower individuals and communities. Crises often leave individuals feeling isolated and helpless, particularly during the depression stage. Effective communication strategies should emphasize collective efforts, reinforcing the idea that individuals are not alone in facing these challenges. Highlighting community solidarity and shared responsibility can foster resilience and a sense of belonging, enabling more constructive engagement.

(7) *Leveraging social media for crisis management:* The role of social media as a barometer of public sentiment and a platform for crowdsourced problem-solving highlights its potential for crisis management. Authorities can monitor social media to gauge public reactions, identify emerging concerns and disseminate accurate information. However, they must also address challenges such as misinformation and fearmongering to ensure constructive discourse.

(8) *AI in cybersecurity management:* Artificial intelligence (AI) technologies play a dual role in this landscape. On the one hand, AI-based tools can support cybersecurity through anomaly detection, real-time monitoring and predictive threat modelling (Ali *et al*., 2025). On the other hand, attackers are also leveraging AI for automated phishing, adaptive malware and deepfake social engineering, increasing the sophistication and speed of attacks (Tounsi and Rais, 2018). The integration of AI into CI introduces both opportunities for proactive defence and new dimensions of vulnerability, particularly where algorithmic opacity or data poisoning may compromise decision-making.

(9) *Integrating emotional and technical strategies:* The emotional trajectory mapped through the Kübler-Ross model underscores the importance of integrating technical and human-centred strategies in cybersecurity management. The research findings highlight that public emotional responses, particularly anger and fear, were often triggered by awareness of specific technical vulnerabilities, such as outdated operating systems and unsecured remote access. These technical flaws became visible symbols of institutional failure, intensifying emotional reactions and eroding trust. Framing technical weaknesses as contextual triggers of public sentiment highlights the need for proactive collaboration between technical and communication teams. Addressing high-visibility vulnerabilities not only strengthens cyber defences but also mitigates emotional fallout. An integrated approach that considers both system integrity and public perception can improve crisis responsiveness and foster long-term resilience.

By framing public reactions to the Florida water plant hack within the Kübler-Ross model and lean principles, this study provides a structured understanding of the emotional and behavioural dynamics during cybersecurity crises. As the digital transformation of CI continues, fostering public trust, resilience and proactive engagement will be essential for mitigating the societal impacts of future cyber threats. This discussion underscores the need for

interdisciplinary approaches that bridge the technical and social dimensions of cybersecurity, paving the way for more resilient and inclusive strategies in the digital age. Figure 7 summarizes these findings in the form of a recommended time-sensitive action plans, each corresponding to a specific stakeholder directly and indirectly associated with the process, including government agencies, public, media and private sector.

6. Conclusions and future work

The increasing frequency and sophistication of cyberattacks on CI underscore the urgent need for research into the societal impacts of these events. In the context of human-centred cybersecurity transformation, social media provides a valuable platform for engaging end users and policymakers. This study focused on the Florida water plant hack, exploring public reactions through the lens of Kübler-Ross's five stages of grief and offering a lean-inspired approach. By examining social media discourse, the study highlighted how individuals process such crises emotionally and behaviourally, from initial disbelief to eventual calls for systemic reform. The findings underscore the importance of continuous stakeholder engagement, iterative feedback and transparency, which are at the core principles of lean thinking, as key components of effective cybersecurity resilience. Much like lean construction enhances efficiency by integrating end-user feedback into project workflows, frameworks on cybersecurity management of CI can adopt lean methodologies to improve adaptability and response strategies through end-user involvement.

This research makes significant theoretical contributions. First, it adapts the Kübler-Ross model to the context of cyber crises, demonstrating its applicability beyond personal grief to large-scale societal disruptions. By framing public reactions to cyberattacks within this model, the study provides a structured understanding of emotional trajectories during crises, offering a novel lens for analysing and acting upon societal responses to technological vulnerabilities. Second, by positioning public engagement as a key driver of cybersecurity response, the study bridges the gap between crisis management and cybersecurity literature by incorporating emotional and behavioural dimensions into traditionally technical discussions. This interdisciplinary approach highlights the interconnectedness of human factors and systemic vulnerabilities in shaping public resilience. Third, the research introduces the concept of collective grief in the digital age, showing how social media amplifies and reflects emotional stages during crises. This aligns with lean principles by emphasizing the role of social feedback loops in improving response strategies and fostering systemic change. The research also extends existing crisis communication theories by emphasizing the dynamic and participatory nature of online discourse. Fourth, the study enriches the understanding of public

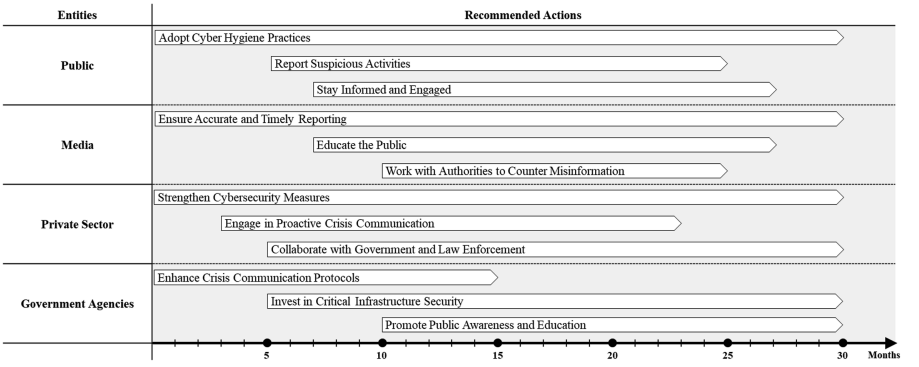

Figure 7. Overview of recommended action plan for different stakeholders in the event of potential cyber incidents. Source: Authors' own work

engagement in cybersecurity, proposing that emotional responses, such as anger and bargaining, can serve as precursors to collective problem-solving and advocacy for systemic reform. Fifth, this study advances crisis management theory by complementing existing cognitive and interpretive frameworks with a sequential, emotionally grounded perspective. By showing how public emotions evolve through recognizable stages during a cybersecurity crisis, the research introduces a temporally structured model that helps anticipate and manage emotional responses over time. Sixth, by extending lean principles into the domain of cybersecurity governance, the study reframes resilience not simply as a matter of technical preparedness, but as an adaptive process driven by continuous, emotionally informed public feedback. This affective lean-informed framework opens new directions for research on iterative, human-centred approaches to managing digital disruptions in CI.

From a practical perspective, the study provides actionable insights for integrating lean-based strategies into cybersecurity management, focusing on continuous improvement, proactive stakeholder engagement and transparent communication during crises. Organizations can leverage social media analysis to improve their response mechanisms, build public trust and ensure resilience through timely interventions. This human-centred approach fosters collaboration across sectors and enhances the capacity to respond effectively to evolving cyber threats. To operationalize these insights, policymakers and infrastructure managers can implement structured social media monitoring during and after cyber incidents using publicly available tools or dedicated sentiment analysis platforms. Real-time analysis of emotional trajectories, such as spikes in fear, anger or calls for reform, can help authorities tailor crisis communication, correct misinformation and prioritize system-level responses. Moreover, public feedback collected from platforms like Twitter can be incorporated into cybersecurity planning cycles through regular review sessions, digital town halls or stakeholder advisory panels. Applying lean principles, such as iterative improvement and stakeholder co-design, these feedback loops can become embedded in organizational learning processes, enabling cybersecurity strategies to evolve in step with public concerns. In practice, this means developing internal protocols for classifying public sentiment, integrating it into post-incident reviews and assigning responsibility for acting on public input within cybersecurity teams. These steps can help move from reactive communication to proactive, trust-building engagement – ultimately increasing the legitimacy, transparency and responsiveness of cyber crisis management. Thus, the findings emphasize the need to modernize CI with a focus on stakeholder-driven solutions, fostering collaboration between policymakers, industry leaders and end users to achieve more adaptive and resilient cyber defence frameworks.

Despite its contributions, the study has limitations. It focuses on a single case, which may constrain the generalizability of findings. Future research could explore diverse cyberattacks across varied contexts to validate and refine the proposed framework. Additionally, while social media offers rich data, it may not capture the perspectives of all affected stakeholders. Future research through interviews, focus groups and surveys could complement social media insights, ensuring a more comprehensive understanding. Moreover, integrating complementary theoretical lenses, such as the Kübler-Ross model with PADM, SCCT or sensemaking theory, could provide a more holistic understanding of both emotional and cognitive dimensions of public response and therefore could enhance the explanatory depth of future work. Finally, longitudinal studies could examine how public attitudes toward cybersecurity evolve over time, offering deeper insights into building long-term resilience.

References

Aggarwal, V.K. and Reddie, A.W. (2018), "Comparative industrial policy and cybersecurity: a framework for analysis", *Journal of Cyber Policy*, Vol. 3 No. 3, pp. 291-305, doi: 10.1080/23738871.2018.1553989.

Ali, S., Wang, J. and Leung, V.C.M. (2025), "AI-driven fusion with cybersecurity: exploring current trends, advanced techniques, future directions, and policy implications for evolving paradigms–A comprehensive review", *Information Fusion*, Vol. 118, 102922, doi: 10.1016/j.inffus.2024.102922.

Baykara, M. and Das, R. (2018), "A novel honeypot based security approach for real-time intrusion detection and prevention systems", *Journal of Information Security and Applications*, Vol. 41, pp. 103-116, doi: 10.1016/j.jisa.2018.06.004.

Blau, G. (2006), "A process model for understanding victim responses to worksite/function closure", *Human Resource Management Review*, Vol. 16 No. 1, pp. 12-28, doi: 10.1016/j.hrmr.2006.02.003.

Bossong, R. and Wagner, B. (2017), "A typology of cybersecurity and public-private partnerships in the context of the EU", *Crime, Law and Social Change*, Vol. 67 No. 3, pp. 265-288, doi: 10.1007/s10611-016-9653-3.

Bruckman, A. (2014), "Research ethics and HCI", in *Ways of Knowing in HCI*, pp. 449-468.

Castillo, C., Fernandez, V. and Sallan, J.M. (2018), "The six emotional stages of organizational change", *Journal of Organizational Change Management*, Vol. 31 No. 3, pp. 468-493, doi: 10.1108/jocm-05-2016-0084.

CISA (Cybersecurity and Infrastructure Security Agency) (2021), "Compromise of U.S. water treatment facility", available at: https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-042a (accessed January 4 2025).

Coombs, W.T. (2007), "Protecting organization reputations during a crisis: the development and application of situational crisis communication theory", *Corporate Reputation Review*, Vol. 10 No. 3, pp. 163-176, doi: 10.1057/palgrave.crr.1550049.

Corr, C.A. (2022), "Elisabeth Kübler-Ross and the five stages model in selected social work textbooks", *Illness, Crisis, and Loss*, Vol. 30 No. 2, pp. 320-332, doi: 10.1177/1054137320932302.

Curry, B.K. (2003), "Organizational flux and its destabilizing influence on employee identity", *Management Decision*, Vol. 41 No. 6, pp. 558-569, doi: 10.1108/00251740310484894.

DHS (2020), *Critical Infrastructure Security*, U.S. Department of Homeland Security, available at: https://www.dhs.gov/topic/critical-infrastructure-security.

EC (2006), "On a European programme for critical infrastructure protection", in *Communication from the Commission, COM(2006) 786 Final*, European Commission.

Eisenhardt, K.M. (1989), "Building theories from case study research", *Academy of Management Review*, Vol. 14 No. 4, pp. 532-550, doi: 10.2307/258557.

Flyvbjerg, B. (2006), "Five misunderstandings about case-study research", *Qualitative Inquiry*, Vol. 12 No. 2, pp. 219-245, doi: 10.1177/1077800405284363.

Garcia de Soto, B., Georgescu, A., Mantha, B., Turk, Z., Maciel, A. and Sonkor, M.S. (2022), "Construction cybersecurity and critical infrastructure protection: new horizons for construction 4.0", *Journal of Information Technology in Construction*, Vol. 27, pp. 571-594, doi: 10.36680/j.itcon.2022.028.

Gashami, J.P.G., Libaque-Saenz, C.F. and Chang, Y. (2020), "Social-media-based risk communication for data co-security on the cloud", *Industrial Management and Data Systems*, Vol. 120 No. 3, pp. 442-463, doi: 10.1108/imds-03-2019-0131.

George, A.S., Baskar, T. and Srikaanth, P.B. (2024), "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors", *Partners Universal International Innovation Journal*, Vol. 2 No. 1, pp. 51-75, doi: 10.5281/zenodo.10639463.

Gerhardt, T. and Puchkov, R. (2023), "Preparing for the future: understanding collective grief through the lens of the Kubler-Ross crisis cycle", *Higher Education, Skills and Work-based Learning*, Vol. 13 No. 5, pp. 983-1008, doi: 10.1108/heswbl-12-2022-0289.

Gioia, D.A., Corley, K.G. and Hamilton, A.L. (2013), "Seeking qualitative rigor in inductive research: notes on the Gioia methodology", *Organizational Research Methods*, Vol. 16 No. 1, pp. 15-31, doi: 10.1177/1094428112452151.

Groat, L.N. and Wang, D. (2013), *Architectural Research Methods*, John Wiley and Sons, New York, NY.

Guest, G., Bunce, A. and Johnson, L. (2006), "How many interviews are enough? An experiment with data saturation and variability", *Field Methods*, Vol. 18 No. 1, pp. 59-82, doi: 10.1177/1525822x05279903.

Halpin, D.R., Fraussen, B. and Ackland, R. (2021), "Which audiences engage with advocacy groups on Twitter? Explaining the online engagement of elite, peer, and mass audiences with advocacy groups", *Nonprofit and Voluntary Sector Quarterly*, Vol. 50 No. 4, pp. 842-865, doi: 10.1177/0899764020979818.

Heath, R.L., Lee, J., Palenchar, M.J. and Lemon, L.L. (2018), "Risk communication emergency response preparedness: contextual assessment of the protective action decision model", *Risk Analysis*, Vol. 38 No. 2, pp. 333-344, doi: 10.1111/risa.12845.

Jabareen, Y. (2009), "Building a conceptual framework: philosophy, definitions, and procedure", *International Journal of Qualitative Methods*, Vol. 8 No. 4, pp. 49-62, doi: 10.1177/160940690900800406.

Jacobsson, K. and Åkerström, M. (2015), "The crisis model: a socially useful psychologism", *Qualitative Sociology Review*, Vol. 11 No. 2, pp. 232-245, doi: 10.18778/1733-8077.11.2.15.

Ketokivi, M. and Choi, T. (2014), "Renaissance of case research as a scientific method", *Journal of Operations Management*, Vol. 32 No. 5, pp. 232-240, doi: 10.1016/j.jom.2014.03.004.

Koskela, L. (1992), *Application of the New Production Philosophy to Construction*, Stanford university, Stanford.

Krishna, B., Krishnan, S. and Sebastian, M.P. (2023), "Examining the relationship between national cybersecurity commitment, culture, and digital payment usage: an institutional trust theory perspective", *Information Systems Frontiers*, Vol. 25 No. 5, pp. 1713-1741, doi: 10.1007/s10796-022-10280-7.

Kubler-Ross, E. (1969), *On Death and Dying*, Routledge, London.

Lehto, M. (2013), "The cyberspace threats and cyber security objectives in the cyber security strategies", *International Journal of Cyber Warfare and Terrorism*, Vol. 3 No. 3, pp. 1-18, doi: 10.4018/ijcwt.2013070101.

Lehto, M. (2022), "Cyber-attacks against critical infrastructure", in *Cyber Security: Critical Infrastructure Protection*, Springer International Publishing, Cham, pp. 3-42.

Maitlis, S. and Christianson, M. (2014), "Sensemaking in organizations: taking stock and moving forward", *The Academy of Management Annals*, Vol. 8 No. 1, pp. 57-125, doi: 10.1080/19416520.2014.873177.

Mantha, B.R., Sonkor, M.S. and Garcia de Soto, B. (2024), "Investigation of the cyber vulnerabilities of construction networks using an agent-based model", *Developments in the Built Environment*, Vol. 18, 100452, doi: 10.1016/j.dibe.2024.100452.

Morse, J.M. (1991), "Strategies for sampling", in Morse, J.M. (Ed.), *Qualitative Nursing Research, A Commentary Dialogue*, Sage Publications, London, pp. 127-145.

Ninan, J. (2020), "Online naturalistic inquiry in project management research: directions for research", *Project Leadership and Society*, Vol. 1, 100002, doi: 10.1016/j.plas.2020.100002.

Pacheco, J., Benitez, V.H. and Pan, Z. (2019), "Security framework for IoT end nodes with neural networks", *International Journal of Machine Learning and Computing*, Vol. 9 No. 4, pp. 381-386, doi: 10.18178/ijmlc.2019.9.4.814.

Palleti, V.R., Adepu, S., Mishra, V.K. and Mathur, A. (2021), "Cascading effects of cyber-attacks on interconnected critical infrastructure", *Cybersecurity*, Vol. 4, pp. 1-19, doi: 10.1186/s42400-021-00071-z.

Pangakis, N. and Wolken, S. (2025), "Keeping humans in the loop: human-centered automated annotation with generative AI", *Proceedings of the International AAAI Conference on Web and Social Media*, Vol. 19, pp. 1471-1492, doi: 10.1609/icwsm.v19i1.35883.

Pescaroli, G. and Alexander, D. (2016), "Critical infrastructure, panarchies and the vulnerability paths of cascading disasters", *Natural Hazards*, Vol. 82 No. 1, pp. 175-192, doi: 10.1007/s11069-016-2186-3.

Pink, S., Tutt, D., Dainty, A. and Gibb, A. (2010), "Ethnographic methodologies for construction research: knowing, practice and interventions", *Building Research and Information*, Vol. 38 No. 6, pp. 647-659, doi: 10.1080/09613218.2010.512193.

Reuter, C. and Kaufhold, M.A. (2018), "Fifteen years of social media in emergencies: a retrospective review and future directions for crisis informatics", *Journal of Contingencies and Crisis Management*, Vol. 26 No. 1, pp. 41-57, doi: 10.1111/1468-5973.12196.

Ridder, H.G. (2017), "The theory contribution of case study research designs", *Business Research*, Vol. 10 No. 2, pp. 281-305, doi: 10.1007/s40685-017-0045-z.

Rinaldi, S.M., Peerenboom, J.P. and Kelly, T.K. (2001), "Identifying, understanding, and analyzing critical infrastructure interdependencies", *IEEE Control Systems Magazine*, Vol. 21 No. 6, pp. 11-25.

Romanosky, S. (2016), "Examining the costs and causes of cyber incidents", *Journal of Cybersecurity*, Vol. 2 No. 2, pp. 121-135.

Sergeeva, N. and Ninan, J. (2023), *Narratives in Megaprojects*, Routledge – Taylor and Francis Group, London.

Sonkor, M.S. and García de Soto, B. (2021), "Operational technology on construction sites: a review from the cybersecurity perspective", *Journal of Construction Engineering and Management*, Vol. 147 No. 12, 04021172, doi: 10.1061/(asce)co.1943-7862.0002193.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C. and Lopez, J. (2018), "A survey of iot-enabled cyberattacks: assessing attack paths to critical infrastructures and services", *IEEE Communications Surveys and Tutorials*, Vol. 20 No. 4, pp. 3453-3495, doi: 10.1109/comst.2018.2855563.

Strauss, A. and Corbin, J. (1990), *Basics of Qualitative Research*, Sage publications, London.

Tounsi, W. and Rais, H. (2018), "A survey on technical threat intelligence in the age of sophisticated cyber attacks", *Computers and Security*, Vol. 72, pp. 212-233, doi: 10.1016/j.cose.2017.09.001.

Weber, D. (2021), "ICS hot take: Oldsmar, FL water facility event", available at: https://www.sans.org/blog/ics-hot-take-oldsmar-fl-water-facility-event/ (accessed 4 January 2025).

Weitzel, L., Prati, R.C. and Aguiar, R.F. (2016), "The comprehension of figurative language: what is the influence of irony and sarcasm on NLP techniques?", *Sentiment Analysis and Ontology Engineering: An Environment of Computational Intelligence*, pp. 49-74, doi: 10.1007/978-3-319-30319-2_3.

Williams, M.L., Burnap, P. and Sloan, L. (2017), "Towards an ethical framework for publishing Twitter data in social research: taking into account users' views, online context and algorithmic estimation", *Sociology*, Vol. 51 No. 6, pp. 1149-1168, doi: 10.1177/0038038517708140.

Williams, N., Ninan, J. and Kwak, Y.H. (2024), "Online firestorms in Twitter: exploring risks to large infrastructure projects from digital communities", *IEEE Transactions on Engineering Management*, Vol. 71, pp. 13963-13974, doi: 10.1109/tem.2024.3432712.

Wong, I.A., Lin, S., Lin, L. and Liao, R. (2021), "Triple grief cycle of cancelled events: the emotional crisis aftermath", *International Journal of Contemporary Hospitality Management*, Vol. 33 No. 7, pp. 2314-2336, doi: 10.1108/ijchm-09-2020-0953.

Wutich, A., Beresford, M. and Bernard, H.R. (2024), "Sample sizes for 10 types of qualitative data analysis: an integrative review, empirical guidance, and next steps", *International Journal of Qualitative Methods*, Vol. 23, 16094069241296206, doi: 10.1177/16094069241296206.effortsto.

Xu, Y., Chakraborty, T., Kıcıman, E., Aryal, B., Rodrigues, E., Sharma, S., Estevao, R., Angels de Luis Balaguer, M., Wolk, J., Padilha, R., Nunes, L., Balakrishnan, S., Lu, S. and Chandra, R. (2025), "RLTHF: targeted human feedback for LLM alignment", *arXiv preprint*, doi: 10.48550/arXiv.2502.13417.

Yang, Q., Tufts, C., Ungar, L., Guntuku, S. and Merchant, R. (2018), "To retweet or not to retweet: understanding what features of cardiovascular tweets influence their retransmission", *Journal of Health Communication*, Vol. 23 No. 12, pp. 1026-1035, doi: 10.1080/10810730.2018.1540671.

Yin, R.K. (2018), *Case Study Research and Applications: Design and Methods*, 6th ed., Sage Publications.

Corresponding author
Johan Ninan can be contacted at: johan.ninan@gmail.com