Crisis Events Taxonomy for Fact-Checking Organizations

This taxonomy has been developed within the framework of the "Facteur" project, led by the EFCSN. The EDMO Taskforce on Elections and Crisis-Related Disinformation decided to adopt it in recognition of the quality of the document, the close relationship between the organizations involved in Facteur and those participating in EDMO, and the need to avoid duplication and inconsistencies within the disinformation-countering community.

Introduction

The rapid spread of disinformation during crises requires a shift from reactive monitoring to a structured, proactive operational framework. While the Digital Services Act and the Code of Practice provide a legal basis for intervention, a significant gap remains between high-level mandates and the technical realities of managing information disruptions. Establishing a definition of information crisis and a crisis events taxonomy followed by a preparedness toolkit allows fact-checking organizations to align their human and technical resources with the specific scale and velocity of an unfolding crisis.

Background

Article 36 of the Digital Services Act (DSA) defines that a crisis shall be deemed to have occurred where extraordinary circumstances lead to a serious threat to public security or public health in the Union or in significant parts of it. Where a crisis occurs, the Commission can deploy its Crisis response mechanism.

Furthermore, the Code of Practice on Disinformation establishes clear obligations for its signatories to bolster European resilience through formalized cooperation. Specifically, under Commitment 37.2, signatories pledge to develop a rapid response system designed for deployment during extraordinary circumstances, such as elections or crises. This is further reinforced by Commitment 42, which mandates that, upon request from the European Commission, relevant signatories must provide proportionate and appropriate information and data. This includes the delivery of ad-hoc specific reports and dedicated chapters within regular monitoring cycles, all functioning in accordance with the rapid response framework established by the Task Force to ensure a swift and coordinated defense of the information ecosystem.
Experience from the fact-checking community suggests that crises impacting information integrity in the Union are significantly more frequent, diverse, and broader in scope than the DSA definition suggests.

The necessity for a definition of information crisis and a comprehensive taxonomy of crisis events stems from the need to move beyond reactive measures toward a structured, proactive framework for information integrity.

By establishing a definition of information crisis and a clear classification of events that are likely to cause such a crisis, ranging from predictable electoral cycles to sudden natural disasters and international conflicts, fact-checking organizations can develop the situational awareness required to anticipate harmful narrative surges before they reach peak velocity. A standardized taxonomy of crisis events provides a first step in setting up an action tool for organizational capacity building, allowing teams to assess their technical, human, and financial readiness and to formulate strategic plans for foreseeable crises.

Acknowledging that while not every identified situation (crisis event) will inevitably escalate into a full-scale information crisis, it is highly

recommended to monitor the information ecosystem closely and prepare for potential escalation whenever such events occur. Furthermore, we recognize that an information crisis may emerge in one country without necessarily manifesting in another, as the potential for a situation to escalate into a full-scale information crisis often depends on specific national contexts and societal resilience. However, national-level crises are frequently exploited by disinformation actors to establish or reinforce specific disinformation-based narratives that then become cross-European. In this context, coordinated Foreign Information Manipulation and Interference (FIMI) operations, as long-lasting structured activities with dedicated infrastructure, can act as a powerful amplifier, strategically weaponizing crisis events, to boost their impact and scale narratives across borders. At the same time, FIMI operations possess the capacity to generate crises at both national and international levels. Therefore, in this Taxonomy, we consider FIMI operations a cross-cutting horizontal issue that must be accounted for in every information crisis, requiring fact-checking activities to be adapted based on the assessment of whether FIMI operations are involved.

Information crises are characterized by the emergence of an "information vacuum", a critical window where the demand for reliable news far outpaces the supply of verified facts. It is within this vacuum of high uncertainty that disinformation thrives, often overwhelming the regular response capacities of media and fact-checking organizations. While sudden information crises leave little room for maneuver, predictable events allow organizations to utilize the available lead time to pre-emptively build resilience and prepare their response strategies.

Establishing a definition of information crisis and a crisis events taxonomy, coupled with an actionable toolkit featuring preparedness recommendations and assessment frameworks for the escalation of predictable and semi-predictable crises, empowers the community to scale its response mechanisms effectively. This approach ensures that the sudden surge in the volume and velocity of disinformation does not outrun the technical and human resources necessary to maintain a resilient and truthful information ecosystem.

Definition

For the purposes of this taxonomy,

*We define an **information crisis** as the disruption of the information system characterized by a surge in the volume and intensity of disinformation within public and digital spaces.*

This involves the deliberate spread of false or misleading content intended to deceive the public, cause harm, or achieve political, economic, or security gains, and triggering further social and political escalations in information space including hate speech, inciting public panic, increased societal polarization and institutional mistrust, threats to collective safety, and both online and physical attacks against specific social groups.

An information crisis is often, even if not always, determined by a **crisis event**. We can divide these crisis events into three main categories: predictable, semi-predictable and unpredictable.

Predictable crisis events

A. Political events:

I. Periodic elections (European, national, regional, local)
II. Referendum
III. Recurrent demonstrations - such as regularly held protest marches and events, which can be assessed as crises due to the general socio-political situation

B. Regularly held events for which we know from previous experience can escalate the disinformation ecosystem:

I. International events (e.g., COP, G8, Olympics, etc.)
II. Conflict-Prone anniversaries - commemorations of historical events with the potential to amplify existing internal social and/or international conflicts (e.g., Srebrenica Commemoration, Stonewall, conflict-related anniversaries, etc.)

Semi-predictable crisis events

A. Political events:

I. Snap elections (European, national, regional, local)
II. Social unrest arising from long-smoldering social conflict
III. Announced protests
IV. Contested changes in legislation or public policies that touch upon internal social or political conflict
V. Institutional deadlocks (e.g. minority governments, government shutdowns, constitutional crises)
VI. Institutional integrity scandals (e.g.high profile corruption affairs, large scale data leaks or releases)
VII. Internationally relevant political events (e.g. NATO crisis, EU enlargement, diplomacy conflicts, migration crisis, etc.)

B. Long-term military and international conflicts

C. Socio-economic disruptions

I. Economic events (e.g. stock market collapse, inflation surge, supply chains disruptions)
II. Highly impactful technological advancements (e.g. AI development, innovation in communication, energy and other strategically important technology)
III. Discovery and/or announced exploitation of material wealth (e.g. fossil fuels, rare earths) with the potential for environmental and/or economic disruption

D. Recurring events for which we know from previous experience can escalate the disinformation ecosystem:

I. Climate events that occur seasonally (e.g., heat waves, wildfires, etc.)
II. Public health related events (e.g., changes in the mandatory vaccination plan, regular national mammography campaigns, etc.)

Unpredictable crisis events

A. Emergent wars, hybrid attacks, ethnic conflicts and forced migration

B. Terrorist attacks and/or targeted political violence; including state-sponsored violence against political opponents

C. Spontaneous or short-term organized social unrest and protests

D. High-level political statements and actions that escalate disinformation surge

E. Violent incidents able to escalate existing social tensions

    I. Individual acts of violence (that are either identity based or are publicly perceived as interethnical, interracial, interreligious, gender-based, due to victims or perpetrators ethnic or national background.)
    II. Collective or group violence (football ultras fan conflicts and attacks, discriminatory-based group attacks on other individuals and groups - migrants, LGBTIQ persons, religious minorities, etc.)

F. Extreme weather conditions and natural disasters (e.g. wildfires, earthquakes, floods, tornadoes, etc.)

G. Environmental crisis situations (e.g. pollution of water, air, soil due to an unpredictable situation such as explosion of a waste landfill)

H. Collapses of energy, transport, border or other key national systems or infrastructure

I. High-casualty events and industrial disasters (e.g. transport crashes with mass casualties, industrial disasters)

J. Cyber-attacks on state/economic digital infrastructure

K. Public health crises (e.g. unknown infectious diseases, escalation of known infectious diseases, etc.)

L. Any other relevant crisis event that leads to an information crisis consistent with the adopted definition