# What is the function of information in a democracy?

In a democracy, information plays a critical role in ensuring informed decision-making, facilitating deliberation, and promoting transparency and accountability. It empowers citizens, enhances government responsiveness, and contributes to social cohesion. The systematic processes and structured activities aimed at ensuring the continuous flow and integrity of information are essential for the maintenance of a healthy democratic system.

# What is an information incident?

Disruption in the information ecosystem, including both sudden and prolonged interruptions, that significantly impacts the normal flow and/or integrity of information, leading to potential or actual harm to the public, government, Canadian democracy, and/or the broader information ecosystem.

# How are incidents graded?

Information incidents can be characterized by:

## REACH AND SPEED

The rate disruption impacts a population, and the reach (size and diversity of population affected)

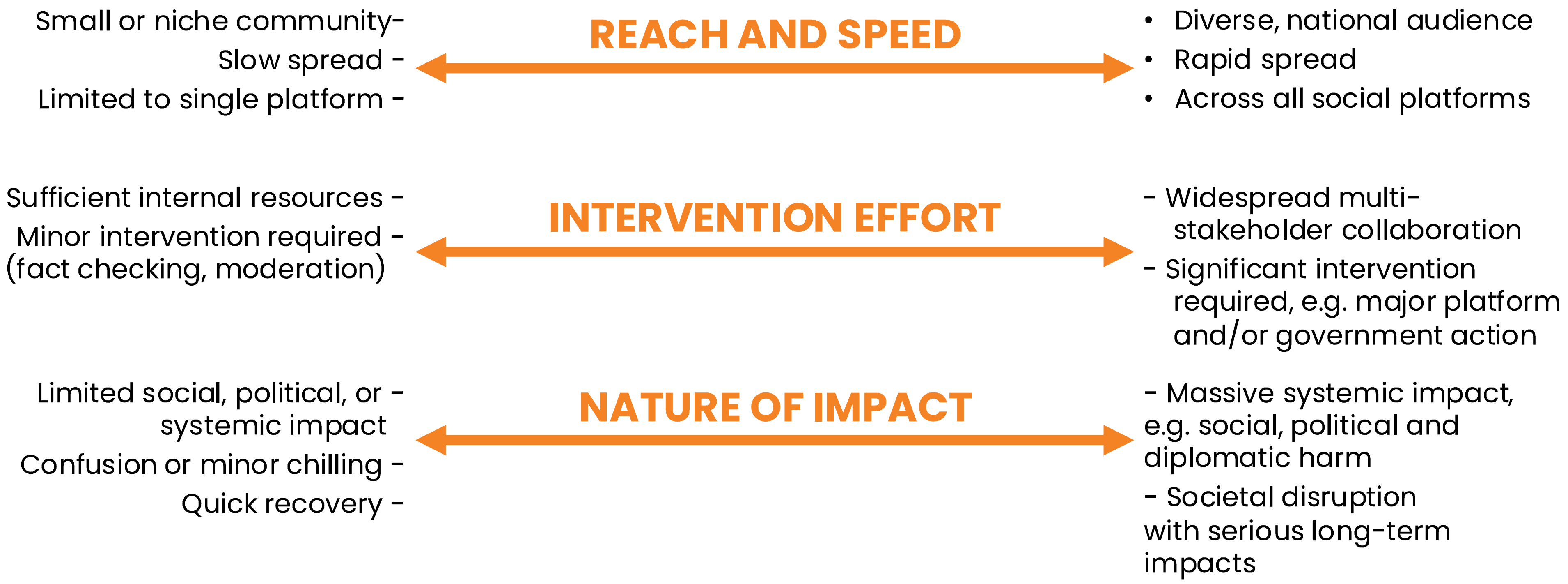
## INTERVENTION EFFORT

The scope and scale of resources (e.g. human, economic, political) required to contain and/or manage a disruption

## NATURE OF IMPACT

Impacts on the system, including social, political and/or structural shifts, combined with the length of the refractory period (short- to long-term)

# How are incidents graded?



**REACH AND SPEED**

Small or niche community-
Slow spread -
Limited to single platform -

- Diverse, national audience
- Rapid spread
- Across all social platforms

**INTERVENTION EFFORT**

Sufficient internal resources -
Minor intervention required -
(fact checking, moderation)

- Widespread multi-stakeholder collaboration
- Significant intervention required, e.g. major platform and/or government action

**NATURE OF IMPACT**

Limited social, political, or -
systemic impact
Confusion or minor chilling -
Quick recovery -

- Massive systemic impact, e.g. social, political and diplomatic harm
- Societal disruption with serious long-term impacts

# Classification of information incidents

## Minor

***Example**: coordinated harassment of a small number of Canadian parliamentarians on Twitter for a short period of time*

## Moderate

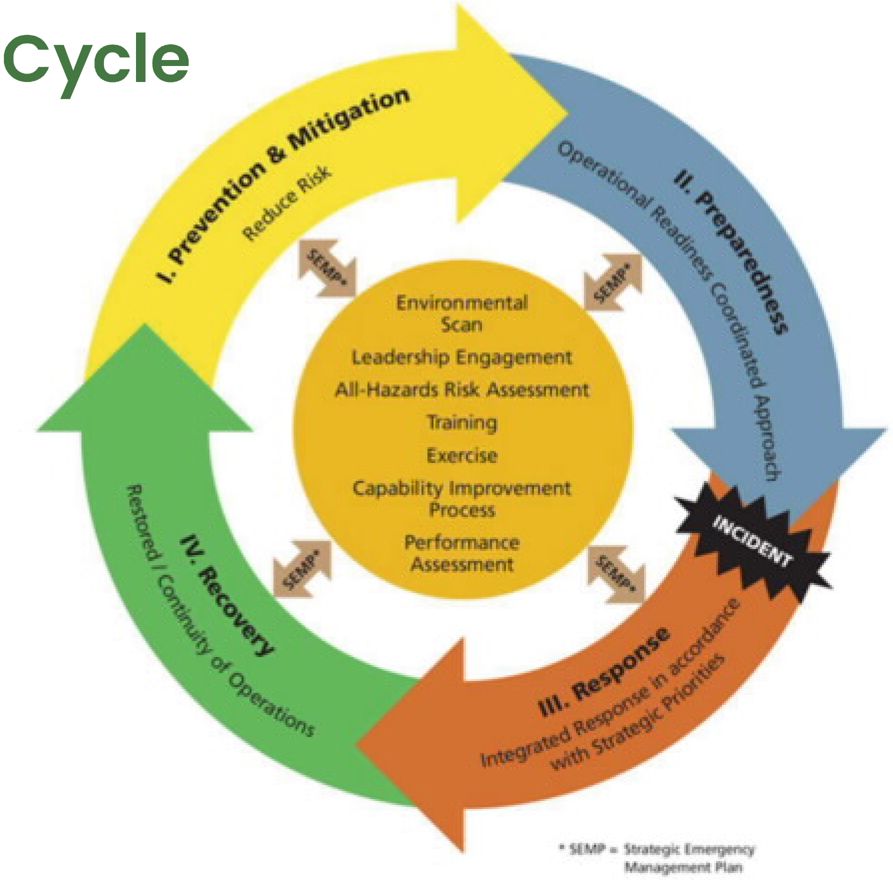
***Example**: systematic misinformation and harassment following an important geopolitical event*

## Major

***Example**: foreign interference attempt during an election, Meta blocking news across their social platforms*

# 3) Adapting an Emergency Management **Framework** for Information Incidents

# Emergency Management Cycle


I. Prevention & Mitigation
Reduce Risk
II. Preparedness
Operational Readiness Coordinated Approach
III. Response
Integrated Response in accordance with Strategic Priorities
IV. Recovery
Restored / Continuity of Operations
INCIDENT
SEMP*
SEMP*
SEMP*
SEMP*
Environmental Scan
Leadership Engagement
All-Hazards Risk Assessment
Training
Exercise
Capability Improvement Process
Performance Assessment

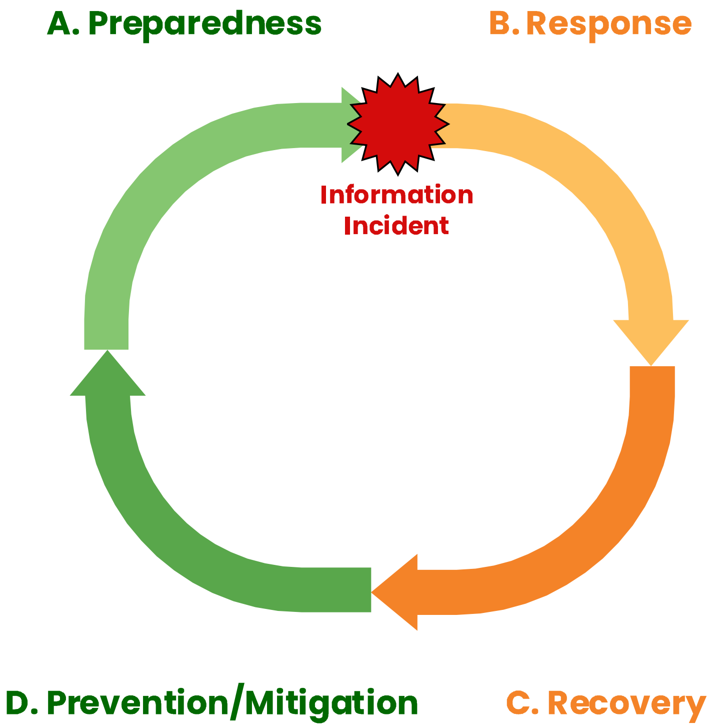
* SEMP = Strategic Emergency Management Plan

Emergencies are managed through four interdependent phases:

I. Prevention & Mitigation
II. Preparedness
III. Response
IV. Recovery

Phases are undertaken concurrently or sequentially, with core activities and outputs associated with each phase.

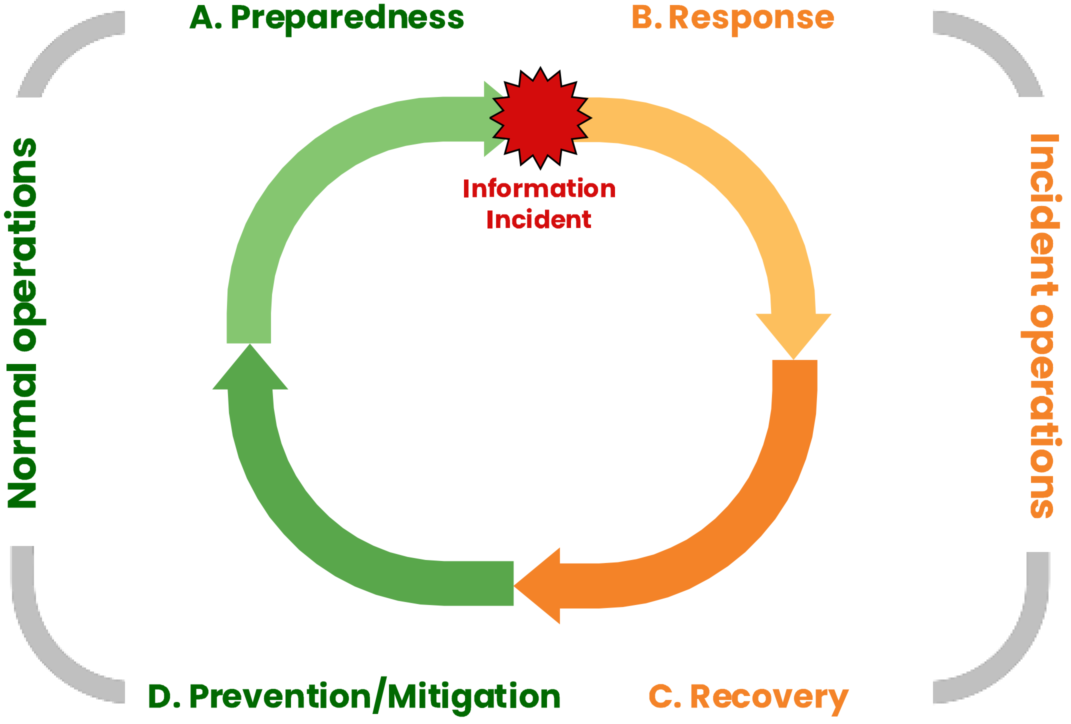
# Adapting the framework for information incidents



Information incidents can be "managed" using the same four functions.

The Research Network is already producing outputs aligned with each function.

# Research Network operations during cycle



## Normal Operations

- Continuous knowledge, capacity, and resilience building across the entire information ecosystem

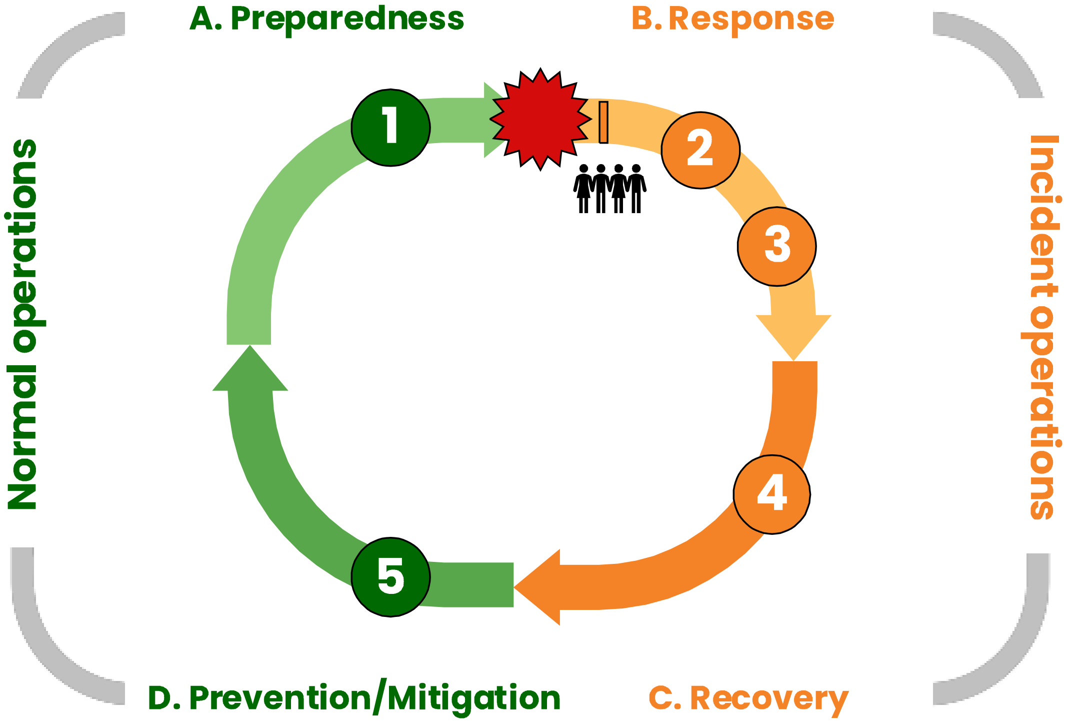
## Incident Operations

- Research and knowledge mobilization regarding the characteristics, impacts, and responses to incidents.

GOAL: **Formalization and Alignment**

# 4) Implementing an Information Incident Research **Process**

# Research Network outputs and process



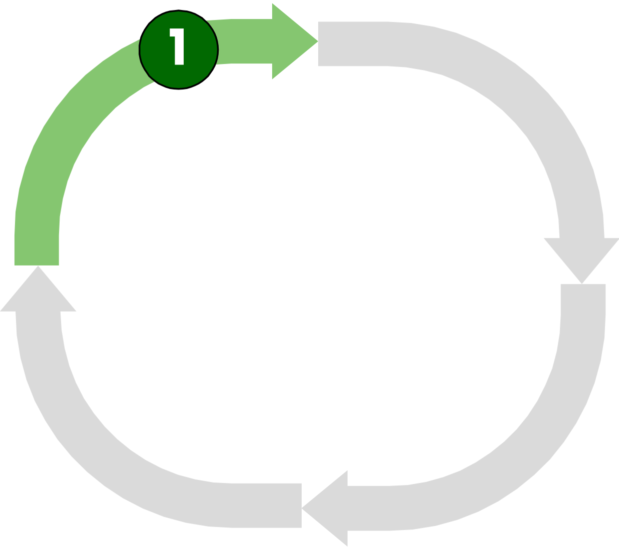
**Response team**

## Outputs

1. **Situation Reports**
2. **Incident Notifications**
3. **Incident Updates**
4. **Incident Debriefs**
5. **Resilience Initiatives**

# Preparedness operations

**A. Preparedness**

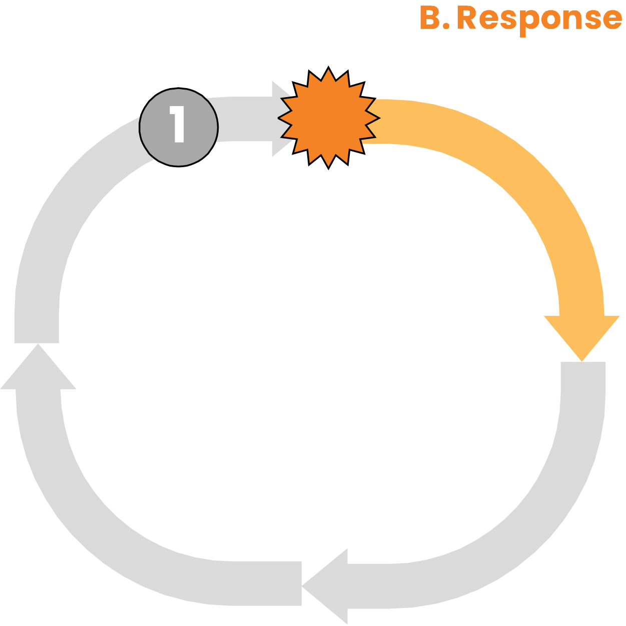


## (1) Situation Report

Monthly public-facing reports highlighting overall information ecosystem health, trends, issues, including a specific focus on mis/disinformation and foreign interference.

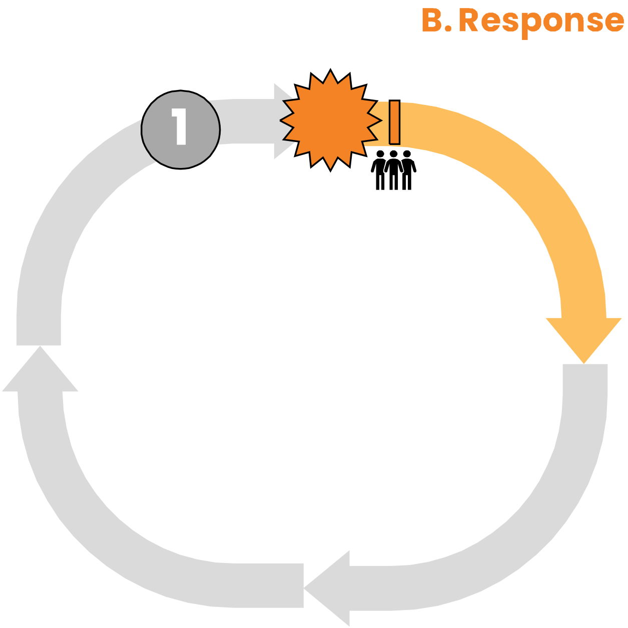
□ Information ecosystem **metrics**
□ Information **trends**
□ Evaluation of **risks**

# Response operations: An incident occurs



Disruption in the information ecosystem, including both sudden and prolonged interruptions, that significantly impacts the normal flow and/or integrity of information, leading to potential or actual harm to the public, government, Canadian democracy, and/or the broader information ecosystem.

# Response operations: evaluation of an incident

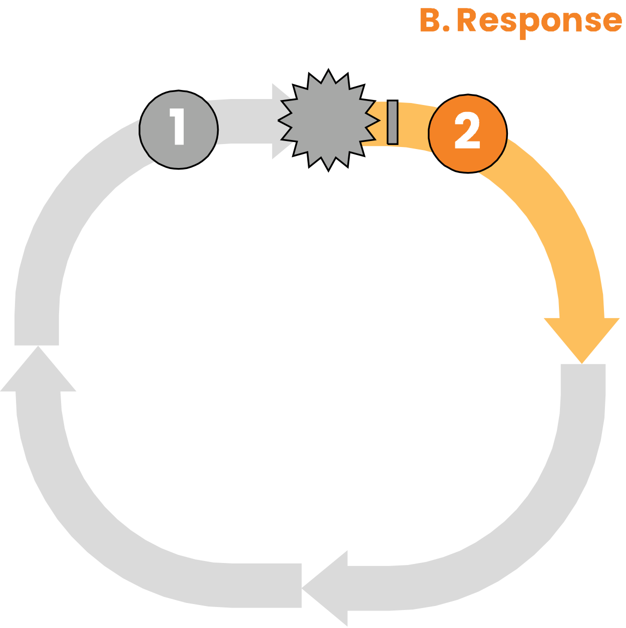


## Information Incident Response team

Activates after an incident to determine:

- ❑ Initial grade of incident
- ❑ If an incident alert is necessary
- ❑ Rapidly develop incident alert
- ❑ Initial response plan (subsequent activities, outputs, resources and timing

# Response operations: alerts to the media and public

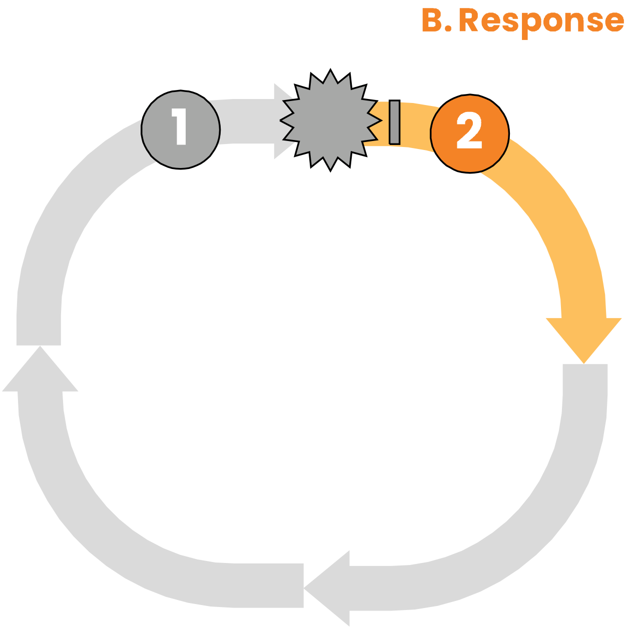


## (2) Incident Notification

Public alert acknowledging incident and helping inform the first wave of public coverage and discussion:

- ❑ Incident summary
- ❑ Background and broader context
- ❑ Key observations
- ❑ Observed and anticipated Impacts
- ❑ Emerging questions
- ❑ Expert contact information

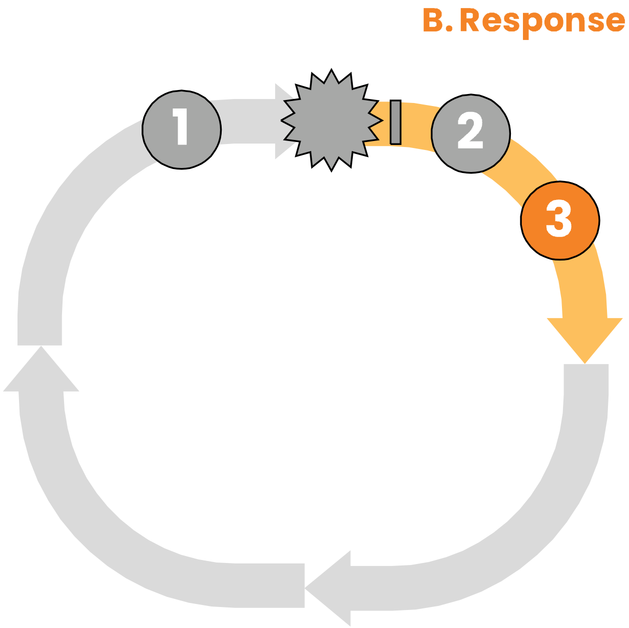
# Response operations: alerts to the media and public



## (2) Incident Notification

Public alert acknowledging incident and helping inform the first wave of public coverage and discussion.

# Response operations: briefs as needed



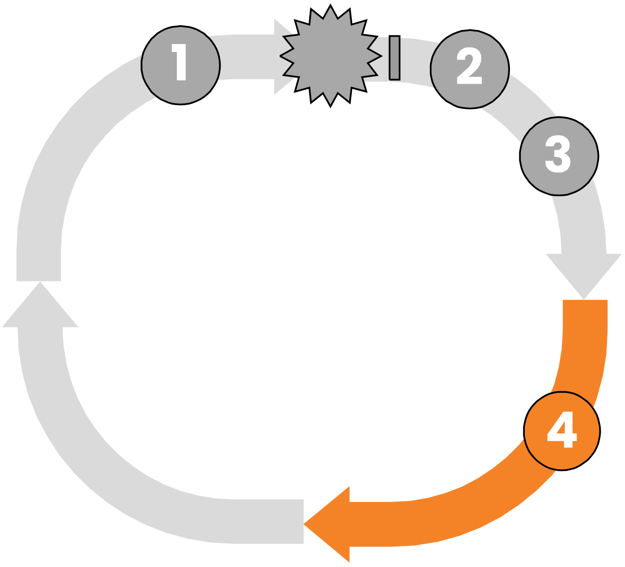
## (3) Incident Updates

Short reports or briefings for key stakeholders on evolving situation.

Briefs will focus on insights from analysis of survey and social data and could include:

- ❑ Public awareness and perception of the incident
- ❑ Social discussion of the incident
- ❑ Evaluation of media and government response
- ❑ Ongoing severity, including reach and initial impact evaluation

# Recovery operations: evaluations



C. Recovery

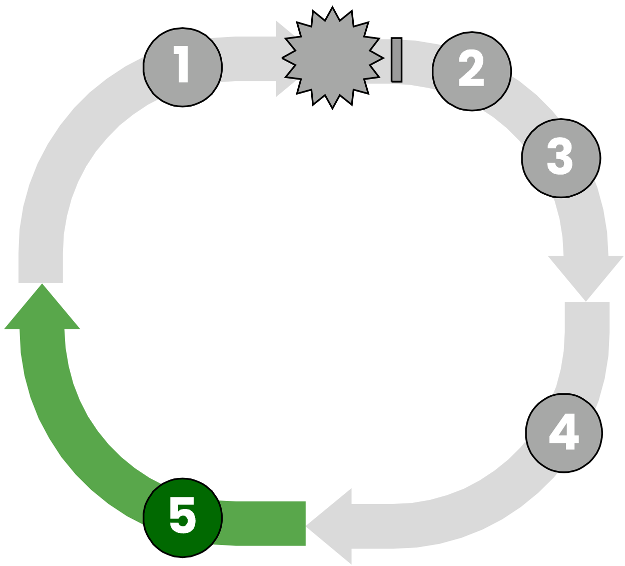
## (4) Incident Debriefs

For major incidents, we will deliver a full public-facing debrief paper that focuses on evaluating the impact of the incident on the information ecosystem.

Evaluations will include:

- ❑ Public awareness and perception of the incident
- ❑ Social discussion of the incident
- ❑ Shifts in population-level attitudes
- ❑ Shifts in online information environment

# Prevention/Mitigation operations: Resilience



D. Prevention/Mitigation

## (5) Resilience Initiatives

A broad range of research-driven activities addressing areas of:

❑ Digital literacy campaigns
❑ Policy and governance evaluations
❑ Research training
❑ Journalism training
❑ Capacity building
❑ Whole-of-society coordination