D5.4 Social Awareness and message generation

Work Package:	WP5 - Post-Crisis management for response and mitigation of physical and cyber threats
Lead partner:	Sheffield Hallam University (CENTRIC)
Author(s):	Helen Gibson, Sam Heyes, Abigail McAlpine, Rowan Dennis, Alice Raven (CENTRIC)
Due date:	M22 – 30 June 2022
Version number:	1.0 **Status:** Final
Dissemination level:	Public

Project Number:	883284	**Project Acronym:**	7SHIELD
Project Title:	Safety and Security Standards of Space Systems, ground Segments and Satellite data assets, via prevention, detection, response and mitigation of physical and cyber threats		
Start date:	September 1st, 2020		
Duration:	30 months		
Call identifier:	H2020-SU-INFRA-2019		
Topic:	SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe		
Instrument:	IA		

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284

Revision History

Revision	Date	Who	Description
0.1	30/07/2021	CENTRIC	Table of Contents
0.2	03/11/2021	CENTRIC	Literature, background and initial case studies
0.3	21/06/2022	CENTRIC	Completion of main content
0.4	27/06/2022	CENTRIC	Feedback from first review (SERCO)
0.5	28/06/2022	CENTRIC	Feedback from second review (INOV)
0.6	29/06/2022	CENTRIC	Exec summary, final formatting and update
1.0	30/06/2022	CENTRIC	Final version for submission

Quality Control

Role	Date	Who	Approved/Comment
Internal review	27/06/2022	SERCO	Document accepted; only minor changes suggested
Internal review	28/06/2022	INOV	Document acceptable if changes are made

Disclaimer

This document has been produced in the context of the 7SHIELD Project. The 7SHIELD project is part of the European Community's Horizon 2020 Program for research and development and is as such funded by the European Commission. All information in this document is provided 'as is' and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability. For the avoidance of all doubts, the European Commission has no liability with respect to this document, which is merely representing the authors' view.

Executive Summary

In a crisis, threat or incident it is essential to be able to communicate rapidly and effectively with those directly impacted by the effects of the incident to mitigate against the consequences and to enhance their safety and security. When providing a service that is impacted by such an incident, good communication also supports the reputation of the operator. In the event of a failure or disruption of critical infrastructure, by definition, it can have a significant impact on of society or services dependent upon that infrastructure; therefore, strategies to optimise and improve this communication to maximise its impact are essential. The space sector is one such segment of critical infrastructure operations that may need to communicate about an incident.

To effectively communicate, a number of strategies for crisis communications, public warning and other messaging have been developed for authorities to use. Utilising best practices in communication strategies ensures that the maximal amount of information can be shared in the more efficient way. The advent of social media has provided new opportunities for rapid communication of information and enhanced two-way communication between authorities and citizens, and each other, where both parties can leverage the information shared to better improve their own understanding of the incident and plug gaps in their own communications efforts by utilising citizen information as a form of soft intelligence.

Numerous approaches to crisis communications and public warning strategies exist; however, most suggest that there are several bits of key information that should be included in alert messages to maximise the information shared with citizens and achieve the desired impact. Typically, organisations should include event information, location, timing and guidance for citizen or service users' action in their message. Beyond that, more extensive messages can also relay what actions are being carried out by the responder or operating organisation, when updates can be expected, where to go for further information and a more detail description of ongoing events.

The preparation for such messaging should be included in the crisis communications plan, developed during the preparedness phase of a crisis. Such messaging can anticipate common events and strategies on how the organisation should react accordingly. Furthermore, it is essential during a crisis that communications are clear, consistent and provided regularly so as to keep those affected updated. To support the delivery of such information, which can often be more difficult to provide when efforts are focused on resolving the situation at hand, several authors and best practices have suggested the use of templated messaging whereby short alerts can be rapidly constructed according to a pre-existing template to get the information out. And, while natural and bi-directional communication should not be neglected in this time to provide specific responses to queries and requests for information such preparation can ease the burden on communications teams in what can be a difficult and stressful time.

To support this effort, several standards and approaches exists to support the transition from information categorisation to natural language descriptions of incidents. The Common Alerting Protocol (CAP) is one of the standards that provides a basis for our warning message generation approach.

To fully develop the CAP approach to developing templated messages, we combined this firstly with two sets of research into social awareness and social communication in the event of crisis situations. The first approach considered the current social media strategies and information sharing online of 7SHIELD end users to understand how compatible a templated messaging approach would be with their current social media communications and to what extent they are (or not) communicating about a broad range of crisis events that would be relevant to their followers. In this case, we identified accounts on Facebook, Twitter and Instagram and reviewed the type of information shared as well as the level engagement with that content. Overall, while all end users had accounts and regularly posted information, news and events to these accounts there were very few instances of crisis or incident communications. Nonetheless, it was encouraging to see that when a service disruption did happen (in the case of the ONDA DIAS platform) that many of the features utilised in effective warning messages were present in their online communications.

At least in the case of space operators, the levels of bi-directional communication from citizens or service users and back from operators was relatively limited. While space services are still perhaps a niche area in terms of public awareness, it is possible that such organisations could potentially leverage more from social awareness by increasing their engagement with citizens/service users through their online communication channels as well as investigating the possibility of employing social media monitoring during a crisis event to ensure that they have full situational awareness of all developing conversations and incidents in the online sphere.

To contrast the end user analysis, we also analysed five case studies from the wider critical infrastructure area with incidents that could be analogous with potential threats faced by 7SHIELD end users and the space sector in general. Therefore, we consider a cyber-incident leading to mass disruption of services in the healthcare sector, a power grid failure due to an extreme weather event, a cyber-incident in relation to the provision of gas/oil for transportation, a drone incursion, and a data breach. For each case study, the scope of the incident, the organisational response and their online communication strategy were analysed. It was clear that organisations that got ahead of the story and communicated clearly about the incident, their reaction and the action that citizens, employees or service users could take were able to better control the narrative and prevent long lasting reputational damage. On the other hand, for example in the Gatwick drone incident, while the airport's own communication strategy worked well, the lack of coordination with other stakeholders, such as the police, led to mixed messaging and overall negatively impacted the public's view of the incident.

Based on these lessons, the best practices and knowledge from current research and the orientation of the 7SHIELD use cases and end user partners, it was developed an approach to construct templated messages from a series of pre-defined categories that can be combined to build simple and extended incident warnings and communications in the scope of 7SHIELD. The core of these messages takes the following format:

[severity] [type] for [category] active from [time/date] {until [time/date]} {at [location]}. {[event description]}. [audience] should [instructions]. {[organisation] is [response].} {Update is expected at [date/time]}. Visit [url] for more information {or contact us using [contact info]} [additional media]

This could lead to the following extended warning messages that could be disseminated through various social channels.

Red warning for system unavailability active from 10/06/2021 14:49 until 11/06/2021 at Sheffield. Communication systems are down and log on servers are unavailable. Users should log out of all systems. CENTRIC is updating services. Update is expected at 16:00. Visit www.example.com for more information or contact @organisation

Finally, approaches for message translation are presented to ensure that message generator is able to be used in a multilingual environment and a prototype for the implementation of the warning message generator within the 7SHIELD system is presented that allows users to rapidly create messages and post them to their preferred social sites.

Table of Contents

List of Figures

List of Tables

Definitions and acronyms

A2A	Authorities to Authorities
A2C	Authorities to Citizen
BA	British Airways
CAP	Common Alerting Protocol
CCV	Card Code Verification
CDC	Centres for Disease Control and Prevention
CERC	Crisis and Emergency Risk Communication
CERT	Computer Emergency Response Teams
CFA	County Fire Authority
CI	Critical Infrastructure
CIP	Critical Infrastructure Protection
CISA	Cybersecurity and Infrastructure Security Agency
COVID-19	SARS-CoV-2
C/P	….Cyber/Physical
C2A	Citizens to Authorities
C2C	Citizens to Citizen
DDoS	Distributed Denial of Service Attack
DIAS	Data Information Access Service
DoA	Description of Action
DoH	Department of Health
DoSP	Department of Social Protection
EC	European Commission
EENA	European Emergency Number Association
EO	Earth Observation
EU	European Union
EECC	European Electronic Communications Code
EMSI	Emergency Management Shared Information
EUCI	European Union Confidential Information
ERCOT	Electric Reliability Council of Texas
ESA	European Space Agency
ET	Eastern-Time
ETSI	European Telecommunications Standards Institute
FEMA	Federal Emergency Management Agency
FBI	Federal Bureau of Investigation
FMI	Finish Metrological Institute
FT	Financial Times
GA	Grant Agreement
GNSS	Global Navigation Satellite Systems
HSE	Health Service Executive
ICO	Information Commissioner's Office
ISO	International Organization for Standardization
JC3IEDM	Joint Consultation, Command and Control Information Exchange Data Model
MFA	Multi-Factor Authentication

MS	Member State
NATO	North Atlantic Treaty Organization
NCSC	National Cyber Security Centre
NHS	National Health Service
NOA	National Observatory of Athens
NOAA	National Oceanic and Atmospheric Administration
NSA	National Security Agency
NSTC	National Science and Technology Council
OASIS	Organization for the Advancement of Structured Information Standards
PDT	Pacific Daylight Time
SATCOM	Satellite Communications
SGS	Satellite Ground Station
SMS	Short Message Service
TTC	Telemetry, Tracking, & Commanding
UAV	Unmanned Ariel Vehicle
VP	Vice President
WP	Work Package
WMG	Warning Message Generator
UNESCO	United Nations Educational, Scientific and Cultural Organization
2FA	Two-Factor Authentication

1. Introduction

In the event of a crisis, major incident or other cyber-physical threat it is essential to be able to communicate rapidly and effectively with those that may be immediately affected by the incident itself or the impacts of the incident. In the case of critical infrastructure this may be especially important as people and organisations may be affected by the threat itself in the sense that it may endanger their safety or require them to take evasive action. However, it can also be that other people and organisations are dependent on the services provided and therefore they must also be aware of the impact of the incident to allow them to mitigate against the downstream effects on their own provision.

The methods through which this information is communicated over time has changed. While traditionally broadcast media may have been used to communicate information over a longer time horizon and rapid communication could mainly be achieved through the use of television or radio broadcast; now, social media and other mobile communication technologies enable people to be alerted and contacted almost instantly. Furthermore, the same people can also share warnings or information online about threats or incidents they themselves are experiencing resulting in an additional intelligence source and an opportunity for bi-directional communication.

While there has been extensive research into the topic of crisis communications in the events of incidents such as natural disasters, terrorist attacks and the like, communications around critical infrastructure services are significantly more limited and are often focused on problems related to utility supply (e.g., water, gas, electricity). The space sector is perhaps more niche in this respect. The services provided by the space sector: satellite imagery, navigation systems and satellite communications are important to the everyday activities of many organisations and people but the overall public awareness of what would happen if an interruption to these services was to occur and the impacts upon society are perhaps underestimated, the need for clear and consistent communication in the event of an incident is even more critical.

Given these concerns, it is important that organisations that run or offer these services are able to get the message out in the event of an incident. However, how to manage that communication and to be able to achieve it through a mechanism that is both rapid and standardised whilst also providing the necessary depth of information that enables the receiver to understand and take actions required to mitigate against the threat or impacts of the incident is imperative. It is also recognised within this process that social media is and should be a vehicle for bi-directional communication and that information provided to the organisation can be valuable to understand the overall impact of the event more comprehensively and, even more importantly, if there are elements to the threat/ incident they have not understood or still need to initiate a response towards.

Therefore, this deliverable aimed to look at two particular aspects of communication during threat incidents: firstly understanding the type of threat faced, what are the best strategies of communication, and secondly, how can communication messages be optimally constructed to provide this information to broader sections of society where necessary – whilst also considering that the scope of 7SHIELD – this may need to also include focused communication to those directly in the shadow of an incident. The motivation for this task was to address elements of the initial call document that made the following three requests[1]:

- "Innovative methods should be proposed for sharing information with the public in the vicinity of the installations - including through social media and with the involvement of civil society organisations -, for the protection of first responders such as rescue teams, security teams and monitoring teams, and for ensuring service continuity."
- "Innovative approaches to monitoring the environment, to protecting and communicating with the inhabitants in the vicinity of the critical infrastructure."
- "Establishment and dissemination throughout the relevant user communities of specific models for information sharing on incidents, threats and vulnerabilities with respect to both physical and cyber threats."

Therefore, this task takes the following approach – the first sections are focused on reviewing and understanding how social awareness and public warning message communications are structured and prepared for general crisis communications, for critical infrastructure and where possible the space sector itself. In particular, we also drill down into different frameworks or best practices for the construction of warning messages and ultimately look to leverage aspects of the Common Alerting Protocol (CAP) to form the basis of a warning message generation framework. Secondly, we perform an analysis of how existing organisations within 7SHIELD who are involved in the piloting activities are utilising social media from external perspective to communicate more broadly with the public and how this communication changes when there is a need to communicate about a particular incident. Thirdly, we review some recent communication strategies in the wider critical infrastructure sector to understand the success or not of how these strategies were realised during an actual crisis event. While these are not specific to the space sector, they mirror some of the potential use cases that would also affect 7SHIELD end users (cyber-attacks, data breach, drone incursion, and service interruptions). We also look at to what extent both the 7SHIELD end users and the organisations in the case studies take on board incoming information from people outside the organisation and engage in bi-directional communication to support their goals.

[1] H2020 SU-INFRA01-2018-2019-2020 Prevention, detection, response and mitigation of combined physical and cyber threats to critical infrastructure in Europe https://cordis.europa.eu/programme/id/H2020_SU-INFRA01-2018-2019-2020

Finally, bringing all this work together we propose a warning message generation (WMG) framework for 7SHIELD that will enable end users to rapidly construct warning messages for a variety of situations and can be used to target the broader public, service users/customers and where necessary also employees. This will then be able to be used as a baseline to be able to instantiate a warning message generation system that would enable space service and ground segment operators to quickly construct messages and disseminate them through social media and other services as required in the event of a threat.

As a small caveat to the scope of the deliverable, there is a need to ensure that information from the remainder of the project, that has a limited dissemination level (either Confidential or contains European Union Classified Information (EUCI)) is not included in this deliverable; therefore, discussions around use cases and example threats are considered at a high-level and are integrated into the framework in such a manner. Nonetheless, due to the proposed structure and implementation of the WMG it is easily extensible include more specific information and thus can be adapted for future needs and piloting needs as required.

2. State-of-the-art in social awareness and public warning for critical infrastructure incidents

2.1. Scope and definitions

2.1.1. Critical infrastructure

Critical infrastructure (CI) is defined in the EU as "an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions." [1] Therefore, the security and protection of CI in European Union Member States (EU MS) is essential for the safe functioning of Europe and the security of European citizens. The original 2008 Council Directive focused on the energy and transportation sectors; however, a proposed updated directive assures a wider definition of CI to include energy, transport, banking, financial market infrastructure, health, drinking water, wastewater, digital infrastructure, public administration, and space[2] and is therefore directly in the scope of 7SHIELD.

This proposed directive takes the position that individual critical entities must be able to 'prevent, resist, absorb and recover from disruptive incidents' and both the Security Union Strategy for 2020-2025 and the Counter-Terrorism Agenda recognise the importance of the resistance of critical entities to physical and digital threats [3]. Furthermore, the European Programme for Critical Infrastructure Protection (EPCIP) notes that threats caused by natural disasters and accidents should also be within scope of their crisis management planning [4].

In the event of a disaster that directly or indirectly affects CI, it is important for authorities to communicate with citizens and those in the vicinity, the recent EU Electronic Communications Code [5] provides for the case where EU MS may transmit official public warnings through additional means (to cell-based broadcasts) which could include social media. In fact, recent research by Petersen et al. [6] found that citizens expect CI operators to communicate information during and after a disaster event through both traditional channels and via social media.

2.1.2. The space sector and CI

The space sector will be considered as part of critical infrastructure under COM/2020/829. The Annex to this proposal formalises these entities as 'operators of ground-based infrastructure, owned, managed and operated by Member States or by private parties, that support the provision of space-based services, excluding providers of public electronic communications networks within the meaning of point (8) of Article 2 of Directive (EU)

2018/1972.' A space system (as depicted in Figure 2-1[2]) is generally composed of three main components: the ground segment, the space segment and the user segment [7] with the ground segment itself typically consisting of three elements: a telemetry, tracking, and commanding (TT&C) system whose primary function is to monitor and command the satellite to ensure it remains in the correct orbit; the ground/control centres which manage space mission operations and payload while the terrestrial communication network connect the ground systems together and distribute and enable access to data. Therefore, incidents which could affect or disrupt the ground segment could have a significant impact on the services that utilise its data.

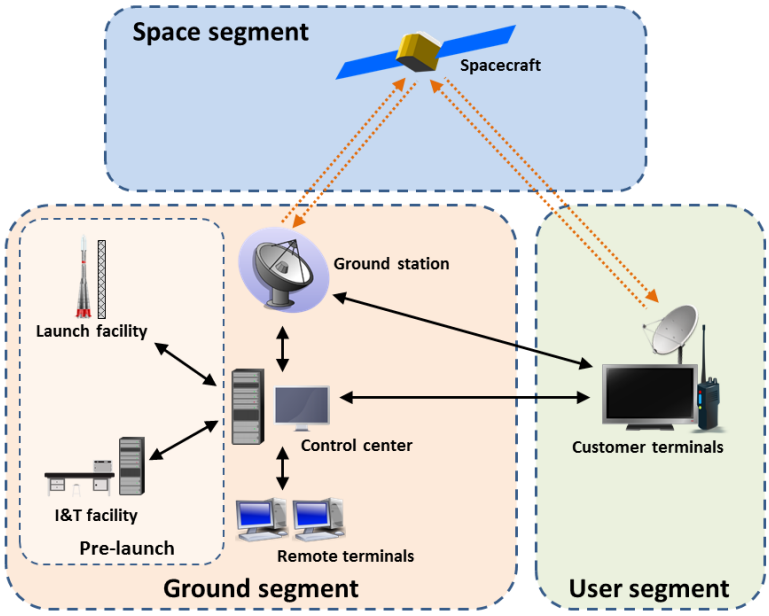


Figure 2-1 - Organisation of a space system and ground segment

A space system usually has one of three purposes: Satellite Communications (SATCOM); Earth Observation (EO); or Global Navigation Satellite Systems (GNSS). The ensuing dependencies on these services may also be crucial to other critical infrastructures, first responders and other frontline services such as the defence sector. Therefore, the protection of these assets from both cyber and physical threats is essential and the consequences for their disruption may be severe. To further add to the complexity of protecting such systems, especially from physical attacks or threats, the ground segment is often located in a relatively remote area that may be more vulnerable to an incident or have longer response times from first responder services.

2.1.3. Common threats to CI, space systems and ground segments

Critical infrastructure can be subject to a wide range of natural and man-made threats that occur in both the physical and digital sphere. As a project, 7SHIELD has already defined

[2] Simplified diagram of segments of a satellite system https://commons.wikimedia.org/wiki/File:Ground_segment.png (CC BY-SA 4.0)

throughout the project several threats that underpin the pilot use cases. These will form the basis of the threats we will consider in this deliverable; however, to allow for an approach that extends beyond the project, some additional relevant threats will be identified where appropriate.

The main physical threats to a ground segment, as considered within the 7SHIELD project, are unauthorised access to the outer area around the segment by a single person, multiple people or a remotely piloted vehicle such as a UAV (unmanned aerial vehicle). Separately unauthorised access into the datacentre or the ground segment operations room would be another threat. Other threats could be caused by the results of natural disasters or meteorological events (earthquakes, floods, wildfires, thunderstorms), attacks from people such as theft, vandalism, use of explosives or similar terrorist threats while infrastructure problems such as overheating of the datacentre, interruption to power or communications lines could also cause significant problems.

Similarly, cyber-related threats have significant potential to cause major incidents for ground segment operators: this can include unauthorised remote access to a sever or machine or access to log-in details. While specific cyber-attacks may include issues relating to the firewall, jamming, spoofing, (distributed) denial of service (DDoS) attacks, or the deployment of ransomware or other computer viruses into the system.

In the worst-case scenario, cyber-physical threats to the space system and particularly the ground segment multiply the potential impact of the incident. For example, unauthorised access to the datacentre itself would also cause a significant threat but following this access if the intruder is also able to access systems leading to a cyber incident this would cause untold levels of further damage. Early work by Graczyk et al. [8] has also investigated several potential opportunities for cyber physical threats on space systems directly, particularly noting that the ground segment itself can be considered a critical point for the instigation of threats. They note a scenario where potential attackers may conduct reconnaissance (both online and offline) and then investigate the use and ultimately exploitation of open-source solutions/software. Otherwise, access to the segment itself or noting the timing of communication windows between the segment and the satellite can also support the identification of opportune moments to attack or intercept communications.

It is also important to consider not only the threat itself but what the consequence of the threat could or would be if it were to be left unchecked. For example, this could include the corruption, deletion, exfiltration or breach of the data within the system – which would be even more problematic if personal data was within the information compromised. The service (EO, SATCOM, GNSS) could also be taken offline causing significant problems for consumers of that data especially if it is used for other critical systems or first responders. Similarly, damage to the ground segment itself could also cause a service interruption meaning the operator cannot fulfil their client contracts as well as incurring significant costs for repair that would have to be borne by the operator. Both physically trespassing on a

site or entering a system remotely via cyber means could be considered a form of industrial, or for highly secure assets state-sponsored, espionage as well as the possibility to obtain satellite imagery of potentially secure or classified sites. Finally, the long-term reputational harm caused by the incident, or the results of the incident, could also pose significant impacts on the operator.

As this deliverable is focused on warning messages to citizens, not all of the above listed impacts are necessarily relevant for their awareness, in general citizens/service users/employees would need to know if (1) the attack causes some physical threat to them; (2) that the service is unavailable/compromised; or (3) their own personal data/account is compromised.

2.1.4. Crisis definitions, progression and communication

When considering a crisis in the context of incident management and subsequent need for communication we can rely on some existing definitions to understand what constitutes a crisis. As show in Table 2-1, Herman [9] proposes three specific criteria that can be used to define the onset of a crisis and what that means for the organisation that is affected.

Definition	Links to 7SHIELD
Threatens the **highest priority values** of an organisation	The ground segment operator is unable to provide its services or protect its users
Presents a **restricted amount of time** in which a response can be made	Services can only be offline or interrupted for a short amount of time for operational (and in some cases, commercial) viability.
Is **unexpected or unanticipated** by the organisation	While 7SHIELD may anticipate certain types of crisis may happen, the timing actual occurrence and impacts cannot be known ahead of time.

Table 2-1 - Herman's working definition of a crisis and links to 7SHIELD

Critical infrastructure is both susceptible to the impacts of natural phenomena whilst also being an attractive target for malicious actors for a number of reasons. Natural disasters, cyber and/or physical attacks on installations and communication networks can cause debilitating impacts on public safety, and security of citizens and could potentially affect other critical infrastructure. Attacks on space ground segments, whilst currently rare, may result in the loss of or access to data.

For the organisations involved there are also several other effects emanating from a crisis or other incident that can have significant long-term impacts on an organisation if not handled well from the outset. Therefore, communication surrounding a crisis or incident must be handled carefully to ensure that such impacts are minimised. Olsson [10] has focused on crisis communications in relation to public organisations and the specific needs

and requirements for operating in such a sphere. While not all end users in 7SHIELD are public bodies, the nature of critical infrastructure is such that it provides a service for the public good and effective functioning of society. Therefore, these considerations are specifically relevant to the 7SHIELD context. Olsen has set out two dimensions of crisis communications as a typology that can be used to effectively support their communication activities: these are (1) **reputation versus resilience**-oriented communication and (2) **strategic versus operational** communication. The features of these are described in Table 2-2 and Table 2-3. Understanding the goal of the communication can also support the messaging by identifying what the user sender aims to achieve by disseminating the message as well as allowing them to perceive how the receiver may interpret the message.

Reputation	Resilience
Sender-oriented	Receiver-oriented
Organisation-centred	Providing information that is critical to survive and revive the current crisis/incident
Protecting the reputation of the organisation	Facilitating coordination
Increases credibility and legitimacy	Information sharing and collective sense-making
Stakeholder perceptions and perceived quality	Initiating the rebuilding and recovery process
Raising awareness and recognition	

Table 2-2 - Reputational and resilience-oriented communications

Strategic	Operational
Planned and structured content	Providing information to people/citizens
Focused on achieving long-term goals	Information focused on managing the incident at hand
Managerial function	Enabling informed decision-making
Promotes positive perceptions amongst stakeholders	Comprehensive information, availability and emotional reactions

Table 2-3 - Strategic and operational communication goals and outcomes

Together the two-dimensions can be organised into four types of crisis communication: operational-resilience, operational reputation, strategic reputation and strategic resilience. Within this task in 7SHIELD, the focus for the warning messages will fall into the **operational strand** of communication for the most part with communications taking on both **resilience and reputational** aspects. Nonetheless, organisational communication will likely need to cover all aspects to building a conscious presence online that is both heard and acted upon where necessary.

The style of crisis communication can also be affected by the rhythm of the crisis. Depending on the type of crisis different timescales are in play. These can also impact on how messages are received and acted upon as it not unusual for extreme circumstances to feel like the norm if urgent communication and actions are extended over a longer period – a form of message fatigue that has become more prominent over the COVID19 crisis [11]. The four main time horizons of a crisis are fast-burning (rapid development and rapid dissipation); long-shadow (rapid development but slow termination), cathartic (gradual development and rapid dissipation) and slow-burning (slow development and slow dissipation) [12]. These can also affect the type of communication required, for example a rapidly developing crisis leaves little time to prepare, and communication should have a form of urgency while more slowly developing crises (if recognised by the authorities) allow for plenty of pre-crisis communication to prepare citizens and other parties that may be impacted and enable better mitigation measures. The crisis and incidents faced within 7SHIELD may touch on all of the above crisis time horizons, in particular, natural disasters or unauthorised access can happen quickly while the effects can often be felt for a long period afterwards, leaving an emphasis towards long-shadow crisis.

2.2. Social media communication and intelligence

2.2.1. Use of social media for crisis communication

Social media is now ubiquitous and the extent it is used as a communication medium by public and private organisations and groups is now a protocol that is expected rather than an add-on to an existing communication strategy. In fact, given the speed and available reach of social media posts, it is often social media that is first used to 'get the message out' while other forms of media – radio, television, websites, press conferences and newspapers (online and in print) is where more in depth coverage and commentary can be provided. One of the most interesting aspects of social media compared to more traditional means of communication is the ease through which communication can happen in a bi-directional manner. Reuter et al. [13] classified these forms of communication into four different relationships:

(1) **Crisis Communication:** Authorities to Citizens (A2C);

(2) **Interorganisational Crisis Management:** Authorities to Authorities (A2A);

(3) **Self-help Communities:** Citizens to Citizens (C2C);

(4) **Integration of Citizen Generated Content:** Citizens to Authorities (C2A).

Within this deliverable, we are primarily focused on the **crisis communication** aspect with some input from the **integration of citizen generated content** aspect as a means of identifying soft intelligence for the early warning of threats (to a certain extent this is also covered through other research within the project focused on threat intelligence including from open sources).

Due to the scope of 7SHIELD, providing information to the public in the event of an incident on a publicly accessible site or to customers who may be reliant on the service is particularly important to ensure that they can both deal with any threats that they face and potentially react themselves to any critical outages of services they may rely upon from the space system.

When considering crisis communication, we can also pay attention to the phase of the crisis or incident we are currently in. Each phase may require different communications strategies and approaches as well as the need for different information to be shared. The crisis management cycle generally follows five-steps: *preparedness → detection → response → recovery → mitigation* which would then feed back to the preparedness phase. For the purposes of crisis communications these five phases can be slimmed down to three core communication phases: ***pre-crisis, crisis*** *(i.e., during a crisis) and* ***post-crisis*** *(after a crisis)* based on the CERC (Crisis and Emergency Risk Communication) Model and best practices from Coombs [14]. It is during the pre-crisis phase, where the focus can be on risk messages, warnings and preparations for a potential incident ahead of time, Reynolds and Seeger [15] also note that is the time where messages can potentially be pre-prepared in an advance of an incident to know what information can be published ahead of time or how to react in certain situations. Discussions on the structure and content of such warning messages is covered more extensively in Section 5. Then during the actual crisis, the focus should be about getting the message out as consistently and regularly as possible to ensure that citizens are provided with the information, they need to take action accordingly [16].

One of the first considerations when setting up a social media strategy is to understand the audience for the information. The CERC model [17] from the CDC provides a strategy for identifying who may be the audiences affected by the incident and therefore who may be assisted by information received through social media. In the case for 7SHIELD, we consider the following communities or receivers of information:

- Directly affected community – in 7SHIELD this could be the general public, service users, employees of the ground segment;
- Community immediately outside the affected area – in 7SHIELD this could be users dependent on downstream services or near to the ground segment operations;
- Emergency responders – incident responders or CERT (Computer Emergency Response Teams) or blue-light services in the event of a physical manifestation of an incident;
- Civic leaders – less likely to be involved directly in 7SHIELD activities but could be particularly influential in dealing with cascading effects if key services are unavailable and directly affect specific communities;
- Partner organisations – organisations that consume or rely on the services of the ground segment;

- **Community leaders including government organisations** – government services that rely on the ground segment or directly if it is a publicly operated site;
- **Media** – can support in spreading the message and mitigating the impact – especially if the incident results in a personal data breach for example;
- **Business, trade and industry** – private organisations dependent on the ground segment data to offer their services;
- **International community** – space operations are, by definition, global and thus potential impacts on satellites could affect a much wider community.

In a major incident it is also important to recognise that these audiences may be receiving information from multiple sources if the crisis is significant enough or they may be identifying other information posted online by other users mentioning the incident. Therefore, failure to get ahead of this communication can also be catastrophic and lead to a spiralling of the crisis incident or breakdowns in communication that have a longer-term impact as well as the spread of misinformation, for example.

One of the key elements of communicating about an incident is to ensure that there is reduced uncertainty about what is happening and what actions should be taken. Research by Serafinelli et al. [18] was focused particularly on communication strategies for critical infrastructure operators and came up with a list of recommendations that can be utilised prior to an incident taking place and during an incident to inform the public about the current incident and its impacts:

(1) Engage key stakeholders in order to ensure message consistency across traditional and social media platforms;

(2) Social media should be used to provide real-time updates to citizens about ongoing efforts to restore services;

(3) Observe and adhere to context-specific regulatory frameworks for emergency management and resilience;

(4) Post-disaster learning should be employed in order to enhance and develop future communication strategies *[outside the scope of this specific deliverable]*.

This therefore emphasises the fact that crisis communications should be an ongoing effort and if an organisation only begins communicating at the moment of onset of a crisis it will reduce the impact of their messaging, even if their actual messages are highly effective.

2.2.2. Social media intelligence for crisis and CI

Social media has long been considered as a possible source of valuable information for public authorities, first responders and other agencies in the midst of a crisis situation. The field of crisis informatics is built upon this premise of the potential utility to use social media as a further signal (amidst the noise) that can be leveraged to improve situational awareness

and response ahead of official channels. Similarly, over the last 10 years the field of open-source intelligence has expanded rapidly and beyond just the usage by the police or military domains to organisations themselves realising they can be on top of the public conversation about their services.

In an effective crisis communications strategy, it is important to consider that those in authority may not be fully aware of how the experience of the crisis is being felt on-the-ground or, in the case of a much larger or fast-moving incident, that it is impossible to know what is happening in multiple locations at one time. Therefore, utilising a backchannel of communications information that is already in the public domain is one way to further support the incident response.

Extensive studies have been conducted looking into the types of information shared via social media in the midst of a crisis – especially by those who are witnesses, observers or even victims or the event. Reuter et al. [13] have reviewed the current state-of-the-art of crisis informatics noting that this is a field that has exploded since the growth of social media from 2006; however, they have commented that there is often a bias towards English language data. The use of crisis informatics data usually falls into the citizens-to-authorities (C2A) element of communication and has considered the use of crowdsourcing, citizens as social sensors as well as social listening tools that try to extract signal from noise in the general social media conversation. A limitation in this area is that much of the research is done on data collected after the incident and thus the effectiveness of how well this content truly informs authorities in near real-time is not fully evaluated.

Tying social media intelligence/monitoring to crisis communications, Eriksson [19] notes that understanding the public conversation in the midst of crisis also enables communication mangers to tailor their messages to the needs of the public. For example, if the public are missing elements of information or are unsure what actions to take, this will be prevalent in the social media discussion. Therefore, monitoring of social media should also form part of the crisis or incident communication strategy as well as informing the activities of first responders.

Key takeaways:

- Warning messages in 7SHIELD fall into the authorities to citizens domain; however, other communication targets should not be discounted;
- Warning messages are primarily focused on the actual crisis phase; nonetheless, building a following and strategy for crisis communications must begin in the pre-crisis phase;
- Target communities should be defined in advance of a crisis. The recipients of messages in 7SHIELD may be local citizens, service users or customers and potentially onsite employees;

- ❖ Messages can be prepared ahead of time through templates and in the midst of a crisis should be disseminated with consistency and regularity;
- ❖ Social media monitoring and intelligence can benefit crisis communication strategies by identifying gaps and engagement opportunities as well as highlighting the situation on-the-ground.

2.3. Approaches to warning message generation

2.3.1. Public warning messages

As discussed above the ability to harness social media for crisis communications and public warnings is vast and has been taken on by almost all organisations from public to private sector to provide information to local citizens, customers, service users, victims or at-risk people, amongst others. As can be seen by the extensive literature base in this area, such as that by Reuter et al. [13], the reach and applicability of the field is extensive and has been demonstrated to provide opportunities not only for crisis communications but also for sharing of information between first responders and citizens through crowdsourcing and to provide overall better situational awareness and potentially intelligence (as discussed in Section 2.2.2). In the case of 7SHIELD, the core use case is perhaps adjacent to that of a typical social media crisis management application whereby the goal of the task is to ensure that information is effectively communicated to citizens, in this case it is also essential to include people in the ground segment area who are potentially under threat as well as service users whose use of the data provided by the satellite system may be affected by an issue with the ground segment or users/employees whose data or information could be compromised in the event of a cyber incident or other unauthorised access to the system.

In the scope of 7SHIELD the range of potential incidents is particularly broad and the categorisation of such incidents and how they align with the warning message generation framework will be discussed in detail in Section 5; however, many of the lessons learned from the management of crisis related incidents apply also to this situation whilst this can be further complemented by the *other* meaning of crisis communications that often applies in the case of *brand management* to ensure the reputation of the organisation is maintained in the face of an incident.

Given the goal is to create a *warning message* we begin with definitions from existing standards on the difference between a Public Warning and Public Warning System [20]:

- **Public warning:** notification and alert messages disseminated as an incident response measure to enable responders and people at risk to take safety measures;
- **Public warning system:** set of protocols, processes, and technologies based on the public warning policy to deliver notification and alert messages in a developing emergency situation to people at risk and to first responders.

Therefore, although we focus this deliverable specifically on the public warning aspect it is important to note that the warning message generation (WMG) should ultimately fit into a larger scope that encompasses the entire system (both technological and organisational) for public (or customer/user) warning.

As has already been discussed the scope of public warning and crisis communication is particularly large and as well as communication about incident it can also encompass public relations activity and other aspects as well. Other major organisations have also put forward relevant definitions about public warning messages and a particularly comprehensive one comes from the United States' Federal Emergency Management Agency (FEMA) [21] who state that public information and warning should realise the following: *'Deliver* ***coordinated, prompt, reliable, and actionable*** *information to the whole community through the use of* ***clear, consistent, accessible, and culturally and linguistically appropriate*** *methods to effectively relay information regarding any threat or hazard, as well as the* ***actions being taken*** *and the* ***assistance being made available****, as appropriate.'*

This definition emphasises therefore the need to have single voice that provides consistent information, that is delivered in a timely manner whilst maintaining accuracy; and that such information provides concrete actions for the user to take (if necessary) and what actions the organisation (the sender) is taking to mitigate or respond to the crisis. Furthermore, that the style and type of language used should be appropriate for a wide audience and able to be understood by those who need to be aware of the information directly.

Warning messages themselves should be delivered by the medium that is most appropriate in terms of how they can reach the receivers who need to consume the information. While traditionally this may have been through broadcast media or even print journalism, now the emphasis is on rapid communication and use of newer technologies such as social media platforms, cell broadcast approaches, SMS or even mobile applications. In the broad public warning space in Europe, EENA (the European Emergency Number Association) [22] have set out official guidelines on the different communication media through which warning information could be shared including the above listed approaches but also other cell-based solutions. Of even greater relevance they note the possibility for social media to be 'force multipliers' for the sharing of specific content. This is particularly true if other users go on to further share content and extend its reach beyond the initial circle.

It is also important that the timeliness, tone and approach to crisis communications is well managed. Poor attempts at communication or limited information can damage an organisation's reputation and trust from its users. This is another reason for considering the use of template-based messages; it has been found that while communication should be authentic and demonstrate transparency, there is also a need to refrain from being drawn into emotional discussions that can detract from the important messages that should be shared.

The work of Roshan et al. [23] also divides organisational response types into 10 different categories, in the context of 7SHIELD and public warning messaging the categories instructing information (*informing stakeholders)* and adjusting information *(expresses sympathy or explains the crisis)*, are the most relevant for constructing warning messages while others such as ingratiation *(praise),* apology and reminding information are more appropriate for free-text style messages or posts.

2.3.2. Public warning messages in CI incidents

There has been limited research into how the public expect critical infrastructure operators to use social media for communication during the immediate impact and aftermath of a crisis. Research by Petersen et al. [24] noted that often too much focus was placed on how emergency managers used social media to communicate about crisis events and there was considerably less focus on how CI operators use and may use such services optimally. In particular, they added to a relatively small base of empirical research by consulting citizens on what European citizens expect of CI operators in this circumstance. They specifically looked at water networks, a port and a transportation network and the communities nearby finding that the local community expected such organisations to use traditional broadcast media as well as 74% expecting them to utilise social media in some format, with particularly high prevalence amongst the younger age groups. Since the research was published in 2017, and due to the growth in social media it can be reasonably expected that such a figure now may be even higher. There was less clarity on whether citizens expected such companies to respond to queries directly about the incident; however, still, over 55% of respondents expected some form of two-way communication where possible. This is interesting for our research on message generation as whilst it is possible to communicate initial public warnings or information over social media (or any kind of media) based on a formulaic approach, two-way communication demands that there is a more conversational element available to take over where appropriate.

Most other research that touches critical infrastructure focuses on individual CI elements such as transportation/mass transit, the energy and utilities sector, and the health sector. As will be discussed in some of the case studies in Section 4 there can be different approaches taken by these organisations during their response to a crisis. For example, in the transportation sector, and especially public transportation such as rail or air travel that is particularly vulnerable due to disruption and can leave many thousands of people in the wrong place, effective communication with those passengers is critical. In 2016, Southwest Airlines experienced a power outage, grounding several flights and separating travellers from their luggage, passengers became increasingly frustrated due to the lack of information; despite this, the airline was praised for how it handled the crisis both from a communications perspective through the way in which they framed their crisis response and for the refunds/compensation paid to passengers [25]. In particular, this was a good example of where bi-directional communication was used to respond quickly to concerned

passengers, apologise and provide updated information where possible. A full apology was also posted to Facebook and while customers initially experienced extreme frustration as Boamah summarises, *"these communication strategies and tactics were satisfactory enough to help the company regain its reputation and credibility through positive posts from travelers [sic]'*. This response was in complete contrast the that of United Airlines who, following the removal of a passenger from their airline, tried to downplay the incident exacerbating the ensuing social media storm and ultimately affecting United's reputation for years to come [26].

In 2021, Liverpool Women's Hospital was the site of a terrorist attack whereby an improvised explosive device was detonated in a taxi outside the hospital entrance. Shortly after the incident it was first confirmed on social media by Merseyside Police[3] while the hospital itself followed up with information to patients about how they could still attend the hospital [27]; although the messages themselves contained very little information. Social media communication (even in response to the original tweet by the Merseyside Police) immediately included speculation with rumours circulating about a suicide bomber to a simple electrical fault in the car while the police were subsequently active in dispelling rumours and reassuring citizens. Overall, it was the police services that took over the main communications in managing this incident, while after the first few hours of the incident the majority of communications were focused on the investigation, the initial statement as shown in Figure 2-2, and disseminated through social media, addressed many of the key elements of an effective crisis communications message.[4] Some online posters did note the lack of information for pregnant people during the early hours of the crisis (tweet edited to protect poster identity):

Checking posts about Liverpool Women's Hospital incident...NO POSTS about issues for pregnant women and other women who may be trying to get into hospital nor what support or direction is being provided.

This uncertainty could have caused significant problems with people arriving to the hospital if it was not accessible causing additional stress or worry.

[3] https://twitter.com/MerseyPolice/status/1459881144204337154
[4] https://twitter.com/MerseyPolice/status/1459913781405007876

Figure 2-2 - Merseyside Police statement after terrorist attack at Liverpool Women's Hospital

Key takeaways:

- CI operators must communicate with citizens directly and not leave managing the crisis to emergency managers;
- Warning message generation in 7SHIELD must have a broader scope that includes crisis communications, service continuity and reputation management;
- Regularity, timeliness and tone of communications is particularly important;
- Social media is considered an acceptable vehicle for rapid communication provided it is supplemented by other broadcast media to ensure the widest possible reach for messaging;
- Operators engaging in social media communications should expect include of bi-directional communication should be incorporated where possible;
- There are few existing examples of official communications or advice from space CI operators.

2.3.3. Effective warning message content and construction

The need to not only communicate but to do it effectively whilst maximising the information content of the message is also essential. The paper by Petersen et al. [28] also recommended what content should be included in messages by critical infrastructure operators. They noted that the following three elements should be included as standard in the message content: what has happened; what is expected to happen; and what citizens should do to mitigate the effect of the incident. The following statement was particularly impactful and resonates with the case study discussions in Section 4 below.

"…it is vital that CI operators publicly acknowledge the disruption to their service(s), even if no further information on their cause and likely resolution is known. It is also important to

inform members of the public that they are working to restore these services even if no new information is available at that time."

With the above said, giving citizens an estimate of when they expect services to be restored is especially important to prevent them becoming frustrated with the lack of service. This can also lead to long-term reputational damage far beyond the original incident and is therefore especially important to tackle. Similarly, ensure they have access to recommended actions they can take – either in the form of a disaster management plan or specific advice current and relevant to the incident at hand is also important. For when the public is onsite, this may also form part of the safety briefing.

Finally, Petersen et al. also emphasise that information could and should be provided in multiple languages where possible, especially where English may not be the first language of many of the affected users. There is also an expectation of not needing to overcomplicate the language – providing information in a clear and concise manner can also be particularly helpful – a benefit of using a standardised message structure. This is also recognised by Temnikova et al. [29] who have researched the need for readability in social media messages during crisis events and highlights those sentences should be concise but fully formed with a maximum of 1-2 main points per tweet keeping the wording simple and limiting the use of acronyms or abbreviations with hashtags placed towards the end of the tweet.

The components of a *'good'* message have been thoroughly researched and considered across multiple studies and crisis situations: from terrorist incidents to natural disasters to health warning and CI applications. Ensuring that the messages shared are clear, concise, accessible and informative is paramount to ensuring that the messaging is effective and understood [30]. Sutton et al. [31] add to these recommendations by also stating the importance of consistency (which can be helped by templated or pre-prepared messages) as well as ensuring that the information provided is actually useful or actionable by the receiver. Sutton et al. described both five main characteristics of message content and of message style as described in Table 2-4 below.

Effective Warning Message Content		Effective Warning Message Factors	
Guidance	Tell people exactly what to do to maximize their health and safety and tell them how to do it	**Clear**	Messages should be simply worded, free of jargon, and in words that people can understand
Time	Tell people by when they should begin their protective action and by when they should have it completed	**Specific**	Provide messages that are precise and non-ambiguous about the area at risk, what people should do, the character of the hazard, how much time people have to engage in protective action

			before impact, and the source of the message
Location	Say exactly who should and who should not do it in terms that the public can readily understand, e.g. the physical geographical boundaries for the location where people who need to take action are located	**Accurate**	Messages should provide timely, accurate, and complete information that is free from errors to the extent possible
Hazard and Consequences	Tell about the impending hazard by describing the event, the consequence of the hazard's impact, the threat posed, and how what they are being asked to do reduce consequences	**Certain**	Messages should be stated authoritatively, confidently, and with certainty even in circumstances in which there is ambiguity about message content factors and especially about the protective actions the public is being asked to take
Source	Say who is giving the message based on what constitutes the most credible/believable source for the population as a whole	**Consistent**	Messages should be externally consistent, for example, by explaining changes from past messages and also consistent internally, for example, by never saying things that conflict with each other such as 'radiation is in the air, but do not worry'

Table 2-4 - Effective warning message content and factors

While certain aspects of the above communication specifically related to place-based crisis or incidents that provide a threat to the health or safety of citizens or the public the themes of these messages are also appliable to other forms of warning messages including those in 7SHIELD. Further guidance on the above warning message content also notes that for messages where more than 280 characters are available (i.e., a message longer than a tweet) ordering the information in the form: **source, hazard, location, time and guidance** is most beneficial to understanding, belief and decision-making by the receiver (although source can be skipped over if it is clear the author of the tweet is also the source) [32]. The Australian Disaster Resilience Handbook also provides a chapter on public information and warnings [33], that also suggested the key content of a warning message (in all forms) to include:

- The title of the warning;
- The issuer of the warning and date/time of issue;

- A clear call-to-action;
- The type of threat and how likely it is to occur, with a short description;
- An explanation of the expected impacts and consequences, including detail on the specific communities at risk and expected time of impact;
- Where to get more information;
- When to expect the next update (as appropriate);
- Further advice on action people should take, described as specifically and succinctly as possible;
- General information if relevant, including how emergency services are responding.

The above is of course dependent on the available character limits to share a message and the available format. They also highlight the advantages of the use of templated messages to support with a consistent approach to messaging but also temper that with advice ensure that messages still appear tailored and specific to the event/community they targeted at.

The work of Neußner [34] also looked a common 'wordings' using in crisis communications messages specifically focused on early warning systems and natural hazards (although the research has much broader applicability) noting the extent of the different phraseology used in communications – although highlighting words such as advisory, watch and warning were particularly common as is the use of alert; however, one concern is that the hierarchy of how such terms are used and what they mean specifically is perhaps not well understood by the receiver. Furthermore, they note the use of terminology to convey a specific event, level of danger or recommended actions. They also note a suggestion that words such as severe or imminent could be used to convey the urgency of a situation, which is not always well recognised by the receiver. Interesting they even analysed the use of colour schemes – which despite their inclusion in a specific crisis management standard (see Section 5.1.1) still vary across situations. Meanwhile, Kelman and Fearnley [35] suggest that while standardisation is useful there may also be a need to integrate some flexibility to manage local contexts and processes.

In previous work, Pannocchia et al. [36] suggested a Gold Standard for public alerting and warning content (as described in Table 2-5) that provided three elements of alerting and warning message content. This included: essential content that should be contained in every message, extended information where available and useful and *magnet media* which can be used to bring attention to content in what can be a cluttered social media space.

Essential alert content	• Crisis severity (e.g., green, yellow, red). • Crisis type (e.g., cyber-attack, natural disaster, trespass). • Timeframe (e.g., hours, days, months, years). • Location (e.g., local, regional, national).

Extended warning information	• Impacts. • Recommended actions. • Countermeasures deployed by authorities. • Emergency contact details and further information.
Magnet media	• Unique hashtags • Infographics • Emoji • Videos • Images

Table 2-5 - Gold Standard for social media public alert and warning content

Based on the idea that specific content should be included in warning or crisis information messages, Coombs [37] emphasises the idea that templates can be used for all forms of crisis-related content including that which can be published on social media allowing for fields to then be filled quickly and speeding up the dissemination process. Further examples of content have also been analysed by Sutton and Kuligowski [38] for different types of alerts: 90 characters; 280 characters and 360 characters. They raised concerns that much of the content they reviewed may have presented difficulties for people to understand due to abbreviations and lack of specificity while including ALL CAPS for certain elements to increase urgency, being specific about the threat and location, use of imperative language to encourage people to take action and visual imagery can all support the effectiveness of message content – especially for Twitter.

Key takeaways:

- ❖ Templated messages are a valuable part of any incident response toolkit;
- ❖ Operators should publicly acknowledge the incident and be honest about expectations for the return to service;
- ❖ State what has happened, what actions the CI operator is taking and what citizens can do to mitigate the impact;
- ❖ Use clear and concise language and adopt a multilingual approach where possible;
- ❖ Messages should include incident information, location, time and guidance/instructions as standard. The severity and urgency of a need for action should be conveyed within the text;
- ❖ Additional information on operator actions, return to service or next update, where to obtain further information and additional media as extended content.

2.3.4. Policies and existing standards

As described in the above section, standardisation of warning messages is an attractive approach as it can speed up crisis communications in the face of an incident, enable

messages to be consistent and the structured format can help with ensuring that all relevant content that needs to be in each message is included. This is especially important as sometimes during the pressure of a situation key elements can be forgotten or put aside accidentally.

In this case, specific policies and standards can also help in forming message structure and taking into account best practices of certain types of communication. In considering standards and policies in this area there are a few key streams of activities to incorporate. Firstly, the European Commission's EPCIP (European Programme for Critical Infrastructure Protection) that seeks to harmonise some of the management of critical infrastructure within Europe as well as making operators of CI more accountable in terms of their processes and communication in the face of an incident. Secondly, further European guidelines from the European Electronic Communications Code also provides some standards on how to communicate with the public in the midst of an incident through the EU-ALERT protocol and there are also several European and ISO standards that relate to communications during a crisis that also provide valuable structure for the creation and content of public warning messages. Finally, we also dedicate the next section wholly to the Common Alerting Protocol as the framework that will provide the basis for the warning message generation (WMG) within 7SHIELD.

European Legislation – the European Programme for Critical Infrastructure Protection (EPCIP)

In 2006, the European Council published a programme for Critical Infrastructure Protection [4]. The goal of this programme was to provide a vehicle for the European Commission to manage the protection of critical infrastructure across the EU that could support cooperation between different EU MS and external countries where appropriate. Out of this legislation arose the Directive on European Critical Infrastructure in 2008 [1]. This directive, whilst only applicable to the transport and energy sectors, required operators to start thinking more strategically about their CI operations and the processes that should be in place in the case of an incident.

In 2018, a review of the directive was launched and the decision to designate further CI sectors including space was recommended to further develop standards in the operation of CI across Europe. Ultimately, in late 2020 a proposal for new Directive for critical entities was launched [3]. The relevance of these activities is the inclusion within them on the need to communicate in the event of an incident affecting the CI's operation. This recent legislation puts the onus on CI operators to not only communicate with the competent authority in the event of an incident but also to potentially inform the wider public or services users as necessary (depending on the type of incident).

European Electronic Communications Code (EECC)

Complementing other European guidance is the alerting protocols that have been put forward in a recent EU Directive known as the European Electronic Communications Code (EECC) [39]. While, this is focused on a much broader system of public warning and alerting through standardised messaging approaches that is able to transmit emergency messages to European citizens as efficiently as possible. In 2018, the EECC Directive set out to understand *'whether it is possible in accordance with Union law, and feasible to set up a single Union-wide public warning system in order to alert the public in the event of an imminent or developing disaster or major state of emergency across different Member States'* [40]. In particular, through Article 110 of the Directive, EU MS that have public warning systems must also adopt this provision to be routed through mobile networks to support further informing of citizens in the event of an incident. While this is not yet applicable to the use cases within 7SHIELD, it is also feasible to see how in future aspects of the CIP programme and the EECC could converge with regard to the need to alert citizens of incidents through the EECC protocols.

European and International Standards in Crisis Management

There are several applicable ISO standards to the crisis communication area many of which include the obligation, mechanism and approaches for warning and alerting the public. The most prominent ISO standard is ISO 22322 - Guidelines for public warning.[5] This standard includes many relevant features that align with the warning message approach of 7SHIELD. For example, it explicitly suggests seven elements to be addressed when developing a public warning message in relation to an incident:

1. who should issue the public warning (the sender);
2. who should receive the information (the receiver);
3. when is the public warning to be issued (the timing);
4. who is expected to take action and why is action required (audience and actions);
5. what action is expected and when (authority response and timescales);
6. what to expect as the situation develops (next steps);
7. how the people at risk can access additional information (further information).

As will be seen in the next section these concur with the best practices developed through other theoretical and empirical research as well as related standards. ISO 22322 goes on to propose the inclusion of very specific information within the public alerts and that it is possible to divide the overall information package into an alert and a notification. The 'alert' segment should somehow provide a mechanism to reach the target group while the notification provides the actual essential information those at risk. Based on the above

[5] SO 22322:2015 Societal security — Emergency management — Guidelines for public warning

seven key elements the standard then provides the following specifics in terms of the content:

- the type and purpose of the alert that will be issued (alert type);
- the hazard, threat, or emergency situation prompting the notification (category);
- when the emergency situation is expected to occur (timescales);
- the people at risk to whom the notification applies (audience);
- the appropriate safety actions to be taken (audience instructions);
- when additional information will be available and how to get it (further information).

Further information on the dissemination channels is also discussed as well as the potential influence of human factors elements and accessibility requirements.

Due to the growth in the use of social media in the public alerting and crisis communications space, ISO under TC 292 have proposed a new standard that addresses the use and integration of social media in public alerting situations. The standard recognises that emergency managers and the public use social media to communicate in this situation and that both may need to also monitor social media to understand what actions to take. In relation to 7SHIELD, it does not provide specifics for message templates but covers information about alerting for specific incidents, impact of writing/communication styles, roles, actions, navigation and no-go zones, requirements for first responders and other organisations as well as recognising the limitations of social media in terms of reach and reliance on communications networks, i.e., it should be a tool in the emergency managers' arsenal but not the whole toolbox.

Emergency management is an active area in the standardisation domain with relevant aspects to crisis communications being included in several other standards. However, for the most part they are beyond the scope of this deliverable, for example, in PD ISO/TR 22351 the EMSI (Emergency Management Shared Information) codes are significantly more detailed and broader in scope is needed for the activities and potential events within 7SHIELD. Additionally, this, like many of the more technical standards emphasise information exchange between systems rather than for human consumption as natural language. Other examples include:

- ISO 22328 1:2020 General guidelines for the implementation of a community-based disaster early warning system;
- PD ISO/TR 22351 Security and resilience -- Emergency management -- Message structure for exchange of information;
- BSI (BS 11200) Crisis management – Guidance and good practice.

The recently developed and implemented EU-Alert system is also relevant here, especially for when larger public warning is required. The EU-Alert protocol (as defined by ETSI

(European Telecommunications Standards Institute)) supports the idea and specification of a European Public Warning System.[6] As the system is oriented towards cell broadcast solutions, there are some aspects such as the four levels of alert that would be relevant to the pre-set fields of a warning message template:

- Alert – to warn citizens of an imminent emergency situation, divided into four sub-levels:
  - EU-Alert level 1 – the highest level of alert which citizens cannot opt out of;
  - EU-Alert level 2 – extreme alert;
  - EU-Alert level 3 – severe alert;
  - EU-Alert level 4 – public safety alert.
- Advisory (EU-Info) – messages of less urgency than alert;
- Amber – for child abduction incidents;
- Test – for various testing activities or when conducting exercises.

Other relevant approaches include the Joint Consultation, Command and Control Information Exchange Data Model (JC3IEDM) that may support communication to citizens[7] but the model is more complex than is required with a military emphasis [42].

Other relevant standards include ISO/IEC 27031:2011[8] which includes the obligation to communicate with stakeholders in the event of an incident under the scope of business continuity while ISO 22301:2019[9] also notes the following on communication: *"The organization shall determine the internal and external communications relevant to the BCMS [business continuity management systems] including (a) what it will communicate; (b) when to communicate; (c) with whom to communicate; (d) how to communicate and (e) who will communicate."* Therefore, the development of messages for warnings in the event of an incident can also support the implementation of standards in relation to BCMS.

Key takeaways:

- ❖ There is strong crossover between the outcomes of research in public warning message and content and that described in modern standards;
- ❖ Standards for use of social media for disseminating warning message content still provide relatively generic information.

[6] ETSI TS 102 900 v1.3.1 (2019-02) Emergency Communications (EMTEL) and European Public Warning System (EU-Alert) using the Cell Broadcast System. Available at: https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.03.01_60/ts_102900v010301p.pdf

[7] NATO - STANAG 5525 Joint C3 Information Exchange Data Model - JC3IEDM

[8] ISO/IEC 27031:2011 "Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity"

[9] ISO 22301:2019 Security and resilience. Business continuity management systems. Requirements

Overall, we note that there are several available standards that contribute to public alerting and warning, in the next section we will focus specifically on one further standard – the Common Alerting Protocol (CAP) as perhaps the currently and most widely implemented framework in the alerting space.

2.3.5. Common Alerting Protocol

The Common Alerting Protocol (CAP) [43] was developed following a report from the United States' National Science and Technology Council (NSTC) Committee on Environment and Natural Resources and the Working Group on Natural Disaster Information Systems Subcommittee on Natural Disaster Reduction in 2000 on 'Effective Disaster Warnings' [44]. The topics discussed in the report led to several recommendations being made, those with an emphasis on crisis communication included the requirement:

"A standard method should be developed to collect and relay instantaneously and automatically all types of hazard warnings and reports locally, regionally, and nationally for input into a wide variety of dissemination systems."

And while this report had both an orientation towards natural disasters, as well a US focus, many of the outcomes are applicable in a much broader setting. In particular, the emphasis on disseminating warning messages through as many available channels as possible is especially pertinent to public warning and alerting as well as the use cases within 7SHIELD. Given this report underpinned the ensuring CAP proposal, it perhaps comes as no surprise that they proposed the need for a ***single, consistent, easily-understood terminology*** *[…] alongside a* ***single, consistent suite of variables to be included in a general digital message.***

As with the types of alerts noted in Section 2.3.4 above, the report also highlighted the different types of alerts that could be delivered. Specifically, they noted that the National Weather System [45] (in the US) already employed multiple message types:

- **Warning:** The hazardous event is occurring or is imminent. The public should take immediate protective action;
- **Advisory**: An event, which is occurring or is imminent, is less severe than for a warning. It may cause inconvenience but is not expected to be life- or property-threatening, if normal precautions are taken;
- **Watch**: Conditions are favourable for occurrence (development or movement) of the hazard. The public should stay alert;
- **Outlook**: The potential for a hazard exists, though the exact timing and severity is uncertain;
- **Statement**: Detailed follow-up information to warnings, advisories, watches, and outlooks is provided;
- **Forecast**: This is a prediction of what events are expected to occur.

As we can see there is already a range of terminology on offer for different elements of the system, often suggested by similar agencies, depending on the type of hazard. Therefore, this further motivated them to introduce standardisation across the emergency alerting community. Furthermore, an additional 22 different fields to be included in a universal warning message, were also introduced with the idea that these features could cater from basic to complete warning types of message.

Based on this analysis, the Common Alerting Protocol (CAP) was defined in order to provide a framework for message structure, format and content whilst maintaining compatibility with multiple information exchange networks. The standard is managed by the OASIS (Organization for the Advancement of Structured Information Standards) under the Emergency Management Technical Committee. The management of the standard is active with annual workshops; most recently, this included a call to action on emergency alerting *'to scale up efforts to ensure that by 2025 all countries have the capability for effective, authoritative emergency alerting that leverages the Common Alerting Protocol (CAP), suitable for all media and all hazards.'*[10] One of the benefits of utilising CAP is the existing high levels of adoption (see Figure 2-3[11]), and efforts to improve and promote the uptake provides further advantages if it is aligned with the message generation approach in 7SHIELD.

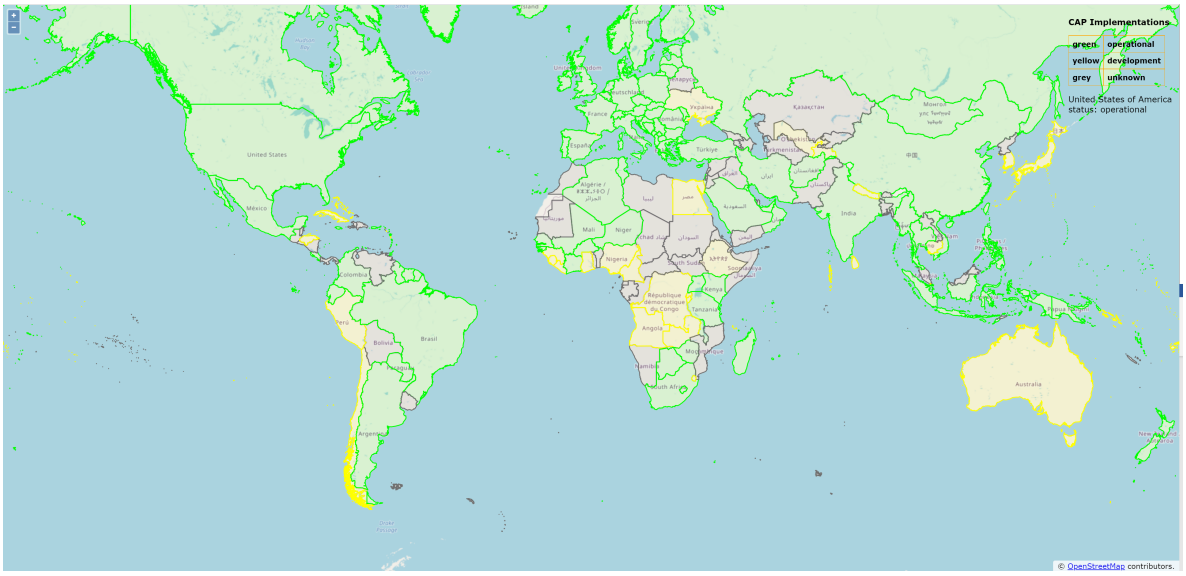


Figure 2-3 - Map of the scale of CAP uptake

The most recent version of CAP (v1.2) was released in July 2010; however, as described above and with further examples below it is still maintaining traction within the emergency alerting community. CAP itself is independent of any technology or communication protocol but instead aims for a wide range of compatibility with existing communication

[10] Call to Action on Emergency Alerting - https://cap-uptake.s3.amazonaws.com/call-to-action.html
[11] Image from https://cap-uptake.s3.amazonaws.com/map.html

services whilst also maintaining backwards compatibility with existing frameworks. In particular, CAP states that it supports the following enhanced capabilities:

- Flexible geographic targeting using latitude/longitude shapes and other geospatial representations in three dimensions;
- Multilingual and multi-audience messaging;
- Phased and delayed effective times and expirations;
- Enhanced message update and cancellation features;
- Template support for framing complete and effective warning messages;
- Compatible with digital signature capability; and,
- Facility for digital images and audio.

The features related to language and audience and template support are particularly relevant for the potential adaptation and implementation in 7SHIELD. The next sections discuss the main features of CAP relevant to 7SHIELD.

CAP defined using XML (eXtensible Markup Language) and each message is divided into four top-level components: **Alert; Info; Resource;** and **Area.** Each segments contains specific elements of information. The **alert** segment provides details about the message (purpose, source, status), a unique id and links to related messages. Each alert segment will usually then contain at least one **info** segment. The info segment contains the most pertinent information: urgency (time), severity, and certainty (i.e., confidence level). The info segment may also contain free text and categories to better describe the incident as well as other response parameters as needed. **Resource** segments are contained inside info segments and provide optional additional information such as digital assets (images, video, audio). Finally, the **area** segment provides the relevant location, while postcodes or other textual location descriptions are permitted for CAP the preferred option is to provide geospatial shapes, nonetheless, due to the eventual need to natural language alerts we will utilise a location description rather than a polygon.

CAP emphasises simplicity and interoperability, especially between different emergency systems and their ability to communicate or share information. In the case of 7SHIELD we are looking towards templated messages, however, this structured approach to message definition means that many elements are relevant to all types of communication and alerting to various stakeholders. The complete model for CAP (including all features) is shown in Figure 2-4.

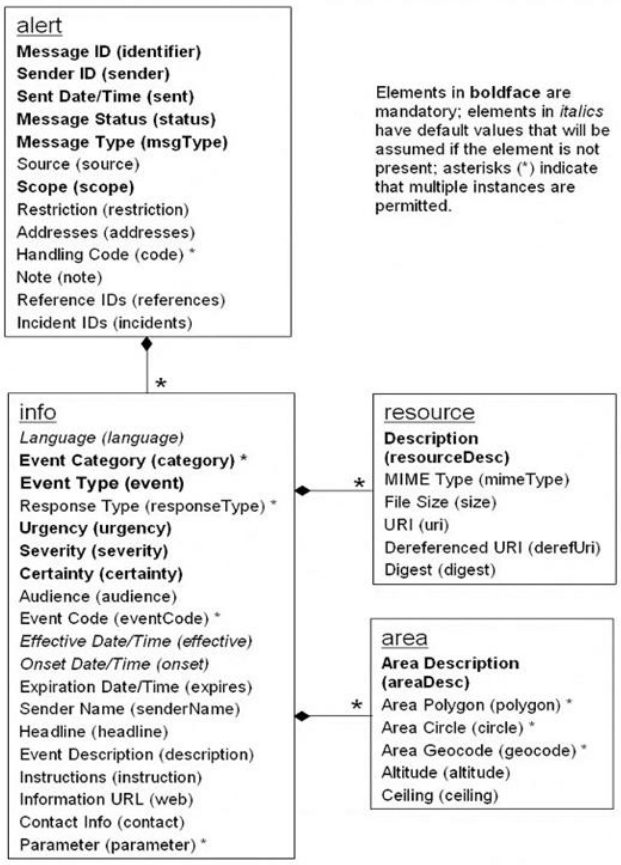


Figure 2-4 - Document Object Model of a CAP alert

Based on these fields and our previous research above, it is clear that several CAP elements overlap with the recommended fields within existing state-of-the-art research for crisis communications and public alerting. Below (in Table 2-6) we highlight the main CAP elements and their mapping to other public warning research.

Segment	Definition
Alert	
msgType	Nature of the alert message (alert, update, etc.)
Info	
Category	Main descriptive category of the event
Event	Text about the event
ResponseType	Action recommended for the target audiences (instructions)
Severity	Severity of the event
Audience	Intended target of the message
Effective	Time from when the communicated information is effective
Onset	Time from when the event began
Expires	Time until the communicated information is valid
SenderName	Organisation that is communicating the information (source)
Description	Description of the hazard (combined with Event)

Instruction	Description of the recommended action for the target audience (combined with Response Type)
Web	URL for more information
Contact	Contact details for more information
Resource	
Resource	Additional media to be included
Area	
Area Description	Location of the incident

Table 2-6 - CAP elements relevant to 7SHIELD WMG framework

Some of the sub-features within a CAP message have pre-defined values for different fields that we can use to inform the construction of the warning messages for 7SHIELD, these can also be customised for the specific alerting content required for 7SHIELD – as will be demonstrated in Section 5.2. In the alert segment, the message type (msgType) is the key element for our framework as this provides information on the 'type' of alert being sent (alert, warning advisory, etc.). The CAP info segment is where the key information for the message content is contained – in terms of the human readable format. Due to its wide applicability, the categories of messages are quite broad to cover all crisis types, however, the response and severity types are relevant to any crisis situation.

The CAP standard sets out several examples of complete CAP messages for different types of scenarios while other approaches have also used CAP as a baseline to develop their own message templating approach. And while some organisations such as EENA [46] have noted that CAP is generally a US-centric protocol, it has been successfully adapted by other countries, for example, Canada and Australian have developed their own profiles while noting that the Italian Fire brigade have provided an adaptation for their purposes [47]. Other adaptations of CAP include Be-Alert in Belgium, an example for both earthquake and COVID-19 alerts in South Korea [48], and even the Google Public Alerts system is an adapted version of CAP.[12] The use of CAP in European Public Warnings on natural disasters is also recommended by Rossi et al. [49] in a report for the EC Joint Research Centre. Table 2-7 shows a mock-up of an SMS message that could be based on CAP.

As mentioned above, Australian has also developed a message protocol based on the CAP standard [50] (a full version with all standardised values can be found here[13]). In this case, over 170 different event types have been defined. The Victoria State Government have also developed a warning protocol that utilises CAP and demonstrates how a standard, human-readable warning message can be developed from the CAP standard. The example

[12] Google Public Alerts: Get started. Available at: https://developers.google.com/public-alerts/guides/get-started
[13] http://www.bom.gov.au/schema/cap-au/v3_0/capauv3-0_schema-v1-1.xsd

presents the following template (Table 2-7) where the 'voice message' could be easily also used for longer-format messages.

Message Type	Severity	Voice Message	Text Message
Bushfire	Warning	Emergency. Emergency. This is a Bush Fire Emergency Warning message issued by the CFA. Resadents in the //LOCATION// and surrounding areas should seek shelter now. Further information is available via the media, or go to www.cfa.vic.gov.au	Bushfire Emergency Warning from CFA. //LOCATION// and surrounding areas. Seek shelter now. Check local radio or www.cfa.vic.gov.au

Table 2-7 - Victoria Warning Protocol – CAP implementation

Further examples of CAP messages and customisation for 5 different languages/countries for 20 different alert types can also be found here.[14]

Similarly, although the CAP standard presents messages in a xml format transposing them into a human-readable format we also see the following examples in Table 2-8.

Segment	Homeland Security Alert	Severe Thunderstorm Advisory	Earthquake Update
Alert: msgType	Alert	Alert	Update
Info: Category	Security	Met	Geo
Info: Event	Homeland Security Advisory System Update	SEVERE THUNDERSTORM	Earthquake
Info: ResponseType		Shelter	
Info: Urgency	Immediate	Immediate	Past
Info: Severity	Severe	Severe	Minor
Info: Certainty	Likely	Observed	Observered
Info: Expires		2003-06-17T16:00:00-07:00	
Info: SenderName	U. S. Government, Dept. Of Homeland Security	National Weather Service Sacremento	Southern California Seismic Network (TriNet) operated by Caltech and USGS
Info: Description	The Department of Homeland Security has elevated the Homeland Security Advisory System threat level to ORANGE / High in response to intelligence which may indicate a heightened threat of terrorism	At 254 pm PDT...national weather service doppler radar indicated a severe thunderstorm over south central alpine county...or about 18 miles southeast of kirkwood...moving southwest at 5 mph. Hail...intense rain and strong damaging winds are likely with this storm.	A minor earthquake measuring 3.4 on the Richter scale occurred near Brawley, California at 8:30 PM Pacific Daylight Time on Wednesday, June 11, 2003. (This event has now been reviewed by a seismologist)
Info: Instruction	A High Condition is declared when there is a high risk of terrorist attacks. In addition to the Protective Measures taken in the	Take cover in a substantial shelter until the storm passes	

[14] https://docs.google.com/file/d/0B5FiAsl5yGbZUHZkWnE1Y2I5aTg/edit?resourcekey=0-ZolnoJdQl4O35KG4JvUzgQ

	previous Threat Conditions, Federal departments and agencies should consider agency-specific Protective Measures in accordance with their existing plans.		
Info: Contact		Baruffaldi/Juskie	
Info: Web	(url)		(url)
Resource: URI	(url)		
Area: AreaDesc	U.S. nationwide and interests worldwide	Extreme north central Tuolumne County in California, extreme Northeastern Calaveras County in California, southwestern Alpine County in California	1 mi. WSW of Brawley, CA; 11 mi. N of El Centro, CA; 30 mi. E of OCOTILLO (quarry); 1 mi. N of the Imperial Fault

Table 2-8 - Examples of three CAP messages from the official standard

Based on the above, we see significant potential to utilise CAP as a basis for a warning message generation framework which can be customised to create natural language messages whilst employing a templating approach that allows for rapid message construction.

3. End User Communication Analysis

3.1. Approach and Methodology

To better understand how existing organisations within 7SHIELD are using social media services to communicate and whether the approach with the scope of this deliverable aligns with their current communication strategies, we undertook an analysis of their recent online communications. Given the changes to the way society has operated during the COVID19 pandemic there is a potential limitation to the approach especially when considering warnings for those onsite as many events were instead held online. Nonetheless, the review serves as a useful view into how engagement currently happens and the extent to which the organisations have already developed an audience for their service.

The main approach was as follows, firstly we undertook to identity the main social media accounts of each of the five end user organisations within 7SHIELD. We focused on the platforms Twitter, Facebook and to a lesser extent Instagram as these generally are the main social platforms and are also those which data can be relatively easily obtained from. For account information from Twitter, we relied on a simple online tool from Vicinitas (https://www.vicinitas.io/) to obtain all or the last 3200 tweets for each account (whichever came sooner). For Facebook and Instagram we relied on the academic access to the online platform CrowdTangle (https://www.crowdtangle.com/) that is a service provided by the parent company Meta. We focused only on organisational accounts so as to not collect personal data and focus solely on organisational communication. For Facebook, CrowdTangle supports the access of posts made to Facebook Pages and also public groups; however, given the scope of our research we focused only on the Pages aspect as this is how organisations use Facebook to disseminate information. Where possible, CrowdTangle provides the full history of the posts to the page (provided they are still published) and therefore our analysis for each page begins from the Pages' inception, similarly for Instagram.

We did not conduct a full coding or content analysis of all pages but specifically sought out warning messages, service interruptions, incidents or disruptions and looked at the level of engagement of these posts. For Facebook, CrowdTangle provides an 'overperforming' metric that compares how well a particular post performs on engagement compared to other posts on the page. Using this score we could also make high-level assessments about how well 'warning' or information type posts performed compared to regular posts such as news or events. Finally, where available (and mainly through Twitter) we analysed any instances of bi-directional communication to see where organisations were communicating more widely with a specific page or account. Where page posts were not in English, Google Translate was used to translate each post individually using the functionality available through Google Sheets.

The following accounts (Table 3-1) were identified as being related to the 7SHIELD end users and pilot use cases.

Social Platform	National Observatory of Athens (NOA)	Finnish Meteorological Institute	ONDA DIAS	Ice Cubes Service	Elecnor Deimos
Twitter		@meteorologit @IlmaTiede @FMISpace	ondadias	@ icecubesservice	@ElecnorDeimos
Facebook	athensobservatory visitorscenters	fmibeta	ondadias	ICE-Cubes-Service-113135143451535	
Instagram	observatoryathens	ilmatieteenlaitos	ondadias		@elecnor_deimos

Table 3-1 - Social accounts of 7SHIELD end users

3.2. Overview of existing communication strategies

Following the identification of the relevant social accounts for each pilot site, the next step was to analyse the information shared by these accounts both in terms of the type of content shared and how, if in any way, information about incidents and service disruptions is provided to followers. Overall size of the accounts and frequency of posting differed significantly between the different services and so direct comparisons between the different sites and end users are not necessarily fair and instead should be considered within the context of the specific account.

3.2.1. National Observatory of Athens

The National Observatory of Athens runs three main social media sites: (1) A Facebook page dedicated to the observatory itself (Figure 3-1); (2) a Facebook page specifically for the visitors centre and; (3) an Instagram page for the Observatory.

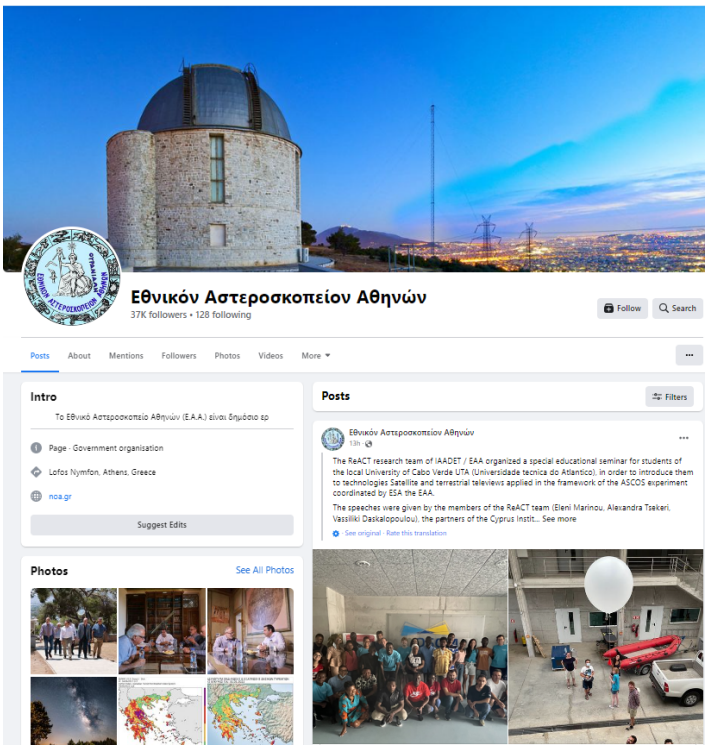


Figure 3-1 - NOA Main Facebook Page (https://www.facebook.com/athensobservatory/)

The main observatory page is the mostly highly followed; however, content is often shared between the two pages to raise awareness.

Using CrowdTangle the posting history of each page was extracted – as far as available within the service, this includes posted content, shared content, videos, albums, events, etc. The pages had varying amounts of content posted:

- AthensObservatory: 1973 posts since August 2013 with 37,000 followers to date;
- VisitorsCenters: 1267 posts since June 2017 with 21,700 followers to date;
- ObservatoryAthens: 21 posts since July 2020.

From the above, it is clear that both AthensObservatory and Visitors Centers pages are both used extensively to share content.

The AthensObservatory page shares a variety of content that generally has high engagement from its followers. Overall, most content has some form of interaction, with an average of 32 likes but much lower numbers for comments and shares. Photos, statuses, links, native and YouTube embedded videos all have significant likes; however, it is mainly photos that result in comments and high rates of sharing as show in Table 3-2.

Type of Content	Average Total Interactions	Average of Likes	Average of Comments	Average of Shares
Link	45.51	35.52	0.52	5.62

Live Video Scheduled	21.33	20.00	0.33	0.00
Native Video	43.16	32.55	0.39	6.08
Photo	64.54	44.33	1.39	10.88
Status	50.17	36.83	1.17	6.79
Video	27.80	22.30	1.30	2.70
YouTube	43.17	32.84	0.88	5.14

Table 3-2 - AthensObservatory per post metrics

CrowdTangle uses a metric known as the 'overperforming' metric that compares each post to all other posts on the page to understand which type of content is most successful. In terms of the AthensObservatory page, the posts are often used to communicate about incidents that have been detected through the Earth Observation (EO) and satellite imagery of the centre. For example, the most highly performing post is the following relating to air quality in August 2021 (translated from Greek and emphasis ours):

*August 4 05:00: The situation now in many areas of **Athens is bad for harmful particles** PM2.5 (minutes inhaled particles, with a diameter of about 2.5 microns and smaller ones). We draw attention to the residents of the Basin, in the areas with high PM2.5 prices, **staying inside their houses** with hermetically closed windows and doors. If you need to release **outside use N95, KN95 or FFP2 mask**, which provide protection against PM2.5 particles. From the European PurpleAir Air Quality Metrics Platform: Real-Time Air Quality Monitoring based on the new generation of "Internet of Things" sensors. The units are in micrograms per cubic meter. The values that appear are unsubstantiated and must be divided by a factor of about 1.8. You can watch PM2.5 prices in real time at:*

https://www.purpleair.com/map?opt=1/mpm25/A10/CC0#10.21/38.021/23.7292:=HTTPS://map .purpleair.com/? opt = 1%2FMPM25%2FA10%2FCC0

According to the CrowdTangle's metrics this post performed three times as highly as any other post on their page and garnered a total of 7,800 interactions (likes, comments and shares). Other posts from around the same period also had high performance metrics; while content such as the history or news about the centre also performed well.

Particularly interestingly, and not seen in any of the other posts, was a directed post dispelling some misinformation in 2018. The following was shared:

*In recent hours, it has been circulating on the internet or "news" that a magnetic storm of the first level of the corresponding scale is expected to hit Earth on July 23. The Athens National Observatory officially informs that **such long -term forecasts are scientifically impossible** and their unnecessary **promotion creates panic and is therefore extremely dangerous**. Possible predictions are possible, based on real -time analysis of observations and have a few hours horizon (with a maximum prognosis window of about 24 hours). Such forecasts are provided on a daily basis by NCA research groups, which have developed relevant services in the context of European Space Agency (ESA) programs or programs*

and other international organizations. Also note that a "violent" event in the sun, such as a strong flare on its surface often accompanied by ejections.

Such as post also generated over 500 interactions and overperformed compared to the posts on the page in general.

Relevant to 7SHIELD is the number of posts made about incidents relating to onsite, these were often linked also to the visitors centre (the page shared over 100 posts from the Visitors Centres account) and other activities as well as providing specific guidance due to the COVID19 pandemic and the need for limited visitor numbers or application of social distancing.

For example, the following are announcements are about the closure of the visitors centre in advance due to a variety of reasons. Such posts received on average 25 different interactions (mainly likes) from the page's followers (translated from Greek). When cross checking against the same posts on the actual visitors centre's pages the interaction was on average almost twice as high for the original post.

ANNOUNCEMENT FOR THISSIO VISITAL CENTER *- On Wednesday 08/07 the Thissio Visitors Centre will* ***remain closed to the public (for technical reasons****) and the scheduled night will not take place.* *- On Thursday 09/07, the musical night of the Opera Chaotique will take place, which will follow the observation of the sky as part of this event.* *For the public who wishes to visit only the Observatory, the Doridis telescope will be available from 21:00 to 22:30. The museum will not be visited on this night.* *- The nights at the Thissio Visitor Centre will continue on the basis of the following program: http://www.noa.gr/index.php?id=628&lang=en:pwws://www.noa.gr/?id=628&lang=en*
EXTRAORDINARY ANNOUNCEMENT *For the Pentelis Visit Center* *The Pentelis Visitor Centre will remain closed for the next 3 days - from Thursday 02/07 until Saturday 04/07, for maintenance of its telescopes, due to emergency technical problems that arose.* *Next week, on Thursday 09/07, evening visits will be held normally. You can make your bookings from next Tuesday at 210 - 3490022.* *Those of you who have already reserved for the next few days inform you that they are not valid and will need to refresh them. We are very sorry for the inconvenience. Alternatively we recommend a visit to the Thissio Visitor Center if it serves you. Thank you very much.*
Due to bad weather, today's night will not take place for the public at the Thissio Visitors Centre. We continue tomorrow Saturday 29/09 (weather permitting) like every Wednesday, Friday and Saturday.
Announcement: As part of the measures to prevent the propagation of Coronavirus, the morning and evening visits - guided tours will not take place at the Thissio and Penteli Visitors to 31 March 2020. Already scheduled visits from schools and other groups will be transferred to later dates after consultation with the centers. Pentelis Visitor Centre: 210 3490022. Thision Visitor Centre: 210 3490160/120 3490036 and Visitorcenter@noa.gr Thank you very much for your understanding and help. Announcement

Due to the measures to be taken in order to resume the likelihood of spreading coronavirus, The Scheduled Evening Tours at the Visitor Centres (Thissio & Penteli) WILL NOT TAKE PART FOR THE NEXT 3 Weeks (Until 31/03/2020). Thank you.
For more Information Please Contact Us AT: 201 3490022/3490160/3490036 and visitorcenter@noa.gr

The visitor centres' page focus exclusively on the information relating to the activities of the visitors center. Given the closures as described above, information was shared also via the AthensObservatory page there is no need to repeat that information directly here. Nonetheless, it is interesting to note that despite lower numbers of followers (21,000) the interaction metrics are higher across all content types, as shown in Table 3-3, thus highlighting in the event of an incident the message is likely to spread faster if shared through the visitorscenter page first followed up by the Observatory page.

Post Type	Average of Total Interactions	Average of Likes	Average of Comments	Average of Shares
Link	85.09	63.73	0.67	11.83
Live Video Complete	206.80	108.60	29.00	16.60
Live Video Scheduled	187.00	167.44	0.84	0.00
Native Video	70.71	49.41	0.47	11.14
Photo	124.34	87.86	1.31	16.35
Status	38.36	31.71	0.43	1.29
Video	24.42	20.00	0.50	2.33
YouTube	78.41	53.19	1.19	13.78

Table 3-3 - Interaction metrics for the visitorscenters page (Facebook)

Similarly, additional content is also shared through the visitorscenters page about closures and that they include much of the messaging required for an effective message.

"Due to high risk of manifestation and fire spreads [hazard], given the air pollution [consequence/impact] in the Attica Basin [location] and for security reasons, the Pentelis visit center will remain closed to visitors [organisation actions] and the public on Friday 6/8 and tomorrow Saturday 7/8 [date]. Scheduled performances are cancelled [instructions] and there will be a new announcement on its reopening."

"Unfortunately, the conditions prevailing in Attica do not allow us tonight the public at the hills of the Observatory in Thissio. We will soon announce the program of visits as they will continue to be held at the Thissio and Pentelis Visitors' Centers after August 15th. We hope to improve the very difficult situation in our country soon, to cleanse the atmosphere of the pollutants and particles that are burdened by it and to be able to observe the night sky again."

"EXTRAORDINARY ANNOUNCEMENT [severity] FOR PENTELIS CENTER [location] The Penteli Visitor Center will remain closed for the next 3 days [event details] - from Thursday 02/07 until Saturday 04/07 [timescale], for the sake of maintenance [organisation response] of its telescopes due to emergency technical problems [category]. Next week, on Thursday 09/07, evening visits will be held normally [update]. You can make your reservations from next Tuesday at 210 - 3490022. Those who have already made reservations for the next few days inform you that they do not apply and will need to renew them [instructions]. We are very sorry for the inconvenience [apology]. Alternatively we recommend a visit to the Thissio Visitor Center if it serves you [alternative solution]. Thank you very much."

As a different type of platform (focused on the sharing of media content and significant limitations on the sharing or reposting of others' content or links), we expect the Instagram page – ObservatoryAthens – to have a different focus and indeed this is borne out of the analysis.

The interaction metrics for the ObservatoryAthens page (Table 3-4) have a more similar profile to the VisitorsCenters pages with high levels of engagement across all content types (video, photo, album (multiple photos/videos shared in one post) although most of the engagement was a 'like' rather than a comment, note that views are only available for videos.

Type	Average of Likes	Average of Comments	Average of Views	Average of Total Interactions
Album	111.00	1.33	0.00	112.33
Photo	85.60	0.87	0.00	86.47
Video	117.00	1.50	448.00	118.50

Table 3-4 - Interaction metrics for the ObservatoryAthens page (Instagram)

The types of content posted on Instagram ranged from advice or praise for citizen actions, e.g.,

November 5th has been established by UNESCO as the World Tsunami Awareness Day (https://www.un.org/en/observances/tsunami-awareness-day). On this day, international organisations, national and local bodies, are invited to include tsunami awareness actions and the dissemination of innovative approaches to reduce the risk of tsunamis. Greece, as a seaside and seismic country, has a rich history of tsunamis that have been created in its recorded history (reference to our article in the magazine kosmos of NCA: http://magazine.noa.gr/archives/3868). During the recent earthquake and tsunami on October 30th (image from a video of Manolis Pyrgiotis in Vathi, Samos), we saw a ***positive response from the state and residents. Many citizens reacted correctly, either by making the right gestures of self-protection, or by following the official instructions, and fortunately there were no victims in Samos from the tsunami****. But we have once again seen citizens remain close to the shore and immortalise the phenomenon with their mobile phones. After*

*a strong earthquake of long duration, any citizen near the coast, to **move as quickly as possible to higher altitude**. At the Geodynamic Institute of the NCA, the National Tsunami Warning Center operates, with the aim of warning the state and foreign states of the possibility of a tsunami as a result of an earthquake, as well as monitoring the evolution of the phenomenon. Information on the operational operation, services and actions of the National Tsunami Warning Centre can be found on the website: http://hl-ntwc.gein.noa.gr*
**The image is from a video by Manolis Pyrgiotis in Vathi, Samos #noa #asteroskopeio #ethnikoasteroskopeioathinon #nationalobservatoryofathens*

Other posts placed emphasis on advertising the facilities or role of the observatory as a way to promote the visitors center and increase interest in the facilities. Similarly, news and research conducted by the observatory were also included in the feed. However, with only 109 posts since February 2018 (approximately one every two weeks) is perhaps too low to provide vital information in the context of 7SHIELD where information may need to be shared within a very short period of time.

3.2.2. Finnish Meteorological Institute

FMI has an interesting social profile with content being made available through all three channels (Twitter, Facebook, Instagram) often with different purposes as seen in Table 3-5

@meteorologit	Twitter	7,500 posts	194,000 followers
@IlmaTiede	Twitter	6,200 posts	16,500 Followers
@FMISpace	Twitter	1,300 posts	9,300 Followers
@IlmatieteenLaitos	Instagram	270 posts	2,600 followers
@FMIBeta	Facebook	75 posts	4,400 followers

Table 3-5 - FMI associated social accounts

Each of the accounts has different purposes, for example @meteorologit is focused solely on providing weather-related information and is generally quite active with at least one post per day (i.e., a weather update). They also commonly @reply to users' comments generating increased levels of engagement and creating a platform for bi-directional communication with users as could be required in a crisis incident Figure 3-2.

The service is seeing increasing engagement (Figure 3-3) with its content over time, especially with users favouriting (i.e., liking) tweets which has been growing over time. Building this sort of engagement and interactions can be particularly useful for when an incident does strike as the chances of the content being seen by users across the service increases.

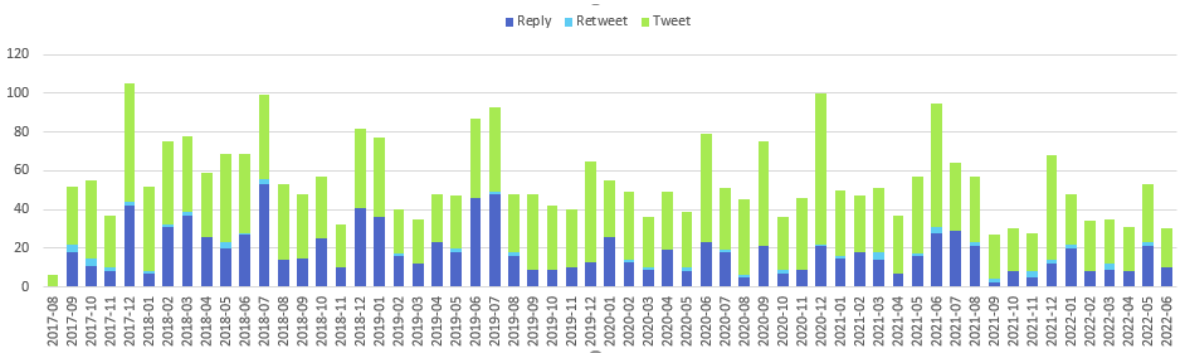


Figure 3-2 - Tweets per month for the @meteorologit account

Overall, we see with this type of content, it is the content that contains some form of media that generates higher levels of engagement as seeing in Figure 3-4 below.

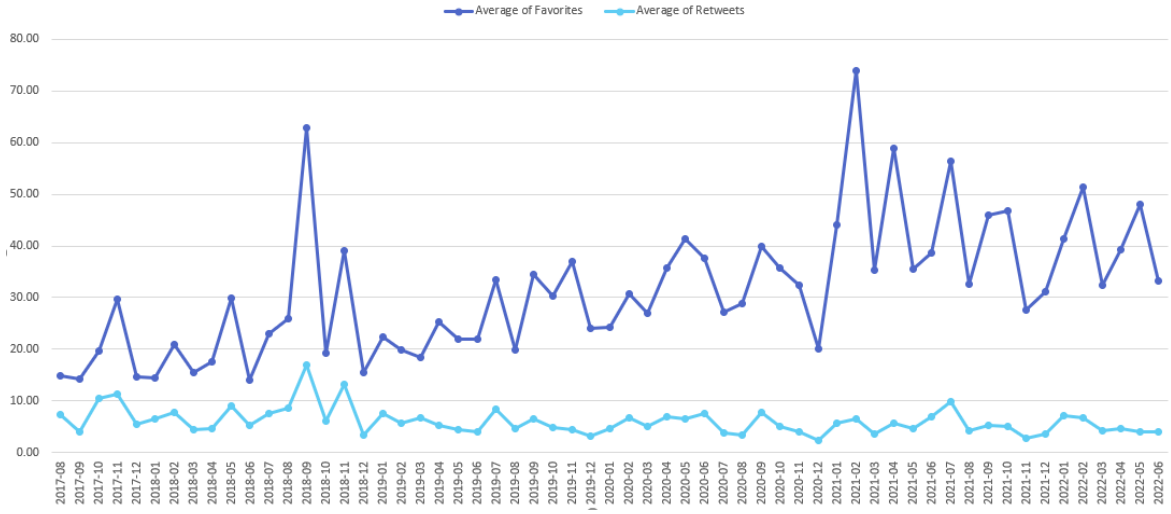
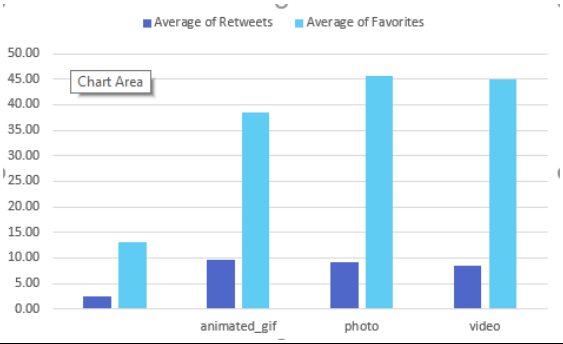


Figure 3-3 - @meterologit - user engagement with tweets posted

In this account the most highly liked and engaged with posts are those that are conversational or fun. For example, the post with the most likes was a reply about a mismatch between a weather prediction and the actual weather, while the second was an



announcement about inability to take proper measurements due to the interference of birds perched on the sensors.

Figure 3-4 - @meteorologit - engagement depending on included media type

This account also shares a lot of similarities with the Instagram account Ilmatieteen Laitos which also posts mainly about the weather phenomenon with warning and information to citizens on how they should react to different weather conditions and the impact upon them. It also covers some promotional content for the service and its researchers. For example,

"Sunglasses out! 🕶The weather is warming this week, and the gray rain clouds change to the soft white air and sunshine. ⛅ operation #summer #weather"

The second Twitter account – IlmaTiede - focuses on promoting research carried out FMI. Again, this is highly used account, but it is interesting to note that plain textual content is has more 'favourites' compared to video-style content although for retweets the numbers are similar (Figure 3-5).

Finally, the FMISpace account focuses specially on the space applications of FMI. While this the most relevant account for 7SHIELD activities the majority of the content informs readers about the current Space Weather activities and specifically predictions on the appearance of the Northern Lights.

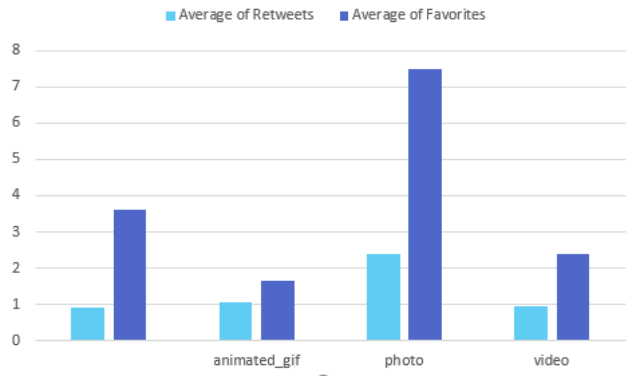


Figure 3-5 - IlmaTiede - engagement depending on media type

However, there is some information content about service disruption as well as details of incidents both detected by the institute as well as incidents affecting the institute. For example, (translated from Finnish) and individual account removed),

"@xxx Nurmijärvi has a telecommunications problem, the meter works but the information does not go from there. The Christmas holiday season has delayed solving the problem."

This was a response to a user querying the lack of information about the Northern Lights in a specific place. Service information is also provided (also often with a Northern Lights emphasis), e.g.,

"We are testing a new product that evaluates the likelihood of Northern Lights. It is based on the magnetic field change rate, like the current images of the Space weather page, but now there is one more stairs. We hope for feedback, for example, as comments below. (1/5)"

Other information about the provision or new satellites or sensor monitoring qualities are also provided:

"Next night we will be launched #esa #umetsat #metopc satellite that continues together with #metopa and #metopb, among others. Global monitoring of air quality. @Ilmietiee included in all metopes eg. #Uvatoration as the developer of the algorithm and @atmospheric_saf director."

We can also analyse how the use of features of Twitter such as hashtags and mentions (Figure 3-6) impact upon interactions with the content. At least for @FMISpace the impact of including hashtags or mentions within the tweet context do not bear out in greater levels of engagement with the content directly, especially in comparison to the use of media.

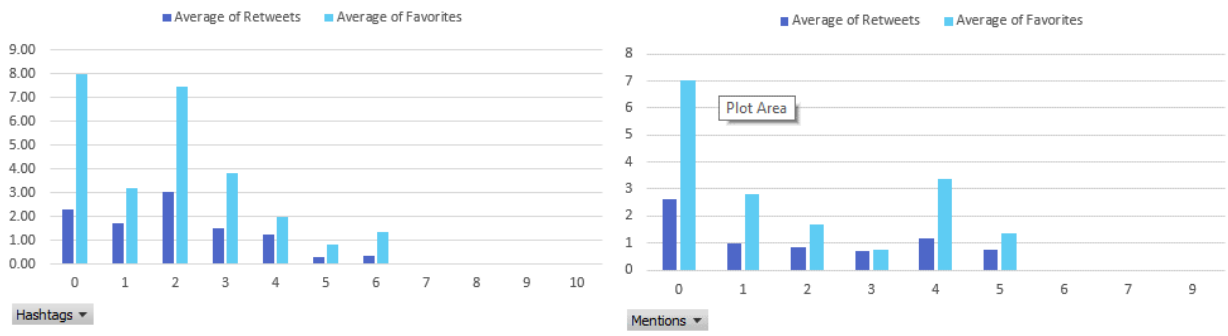


Figure 3-6 - FMISpace - Impact of the use of hashtags and mentions on interactions

Lastly, the FMIBeta page is a relatively new Facebook page that promotes FMI's latest weather app as well as encouraging citizen participation in reporting weather phenomena. The page has just under 4,000 followers but good engagement with the page overall as seen in Table 3-6.

Post Type	Average of Total Interactions	Average of Likes	Average of Comments	Average of Shares
Link	31.93	25.47	1.93	4.13
Photo	34.89	24.02	6.50	3.33
Status	9.83	7.50	0.83	1.17
YouTube	13.00	11.00	0.00	2.00

Table 3-6 - Interactions for the FMI Beta Facebook page

Particularly relevant for 7SHIELD is the information it provides about its Open Data Portal and API and other services including opportunities and disruptions. For example, the three

most highly performing (according to CrowdTangle overperforming metrics) posts are those about the FMI open data portal:

- More weather history data opened! The data from the Finnish Meteorological Institute has now opened real -time weather observations from 1959 in machine -readable form. (Until now, real -time weather observations have been available from open data since 2010.) Real -time weather observations include continuous measurements. Measurements are made at or in the immediate vicinity of the observation stations. Depending on the position and year, observations have been made from a few observations daily to current observations, up to 1 minute. Weather observations include temperature, pressure, air humidity, wind, visibility, prevailing weather, cloudiness, rainfall and snow depth. The data opening on Tuesday also includes pilots from 1961-2014 and new hourly surveys for weather observations. More information about open data: https://ilmatieteentaitoitos.fi/avoivan-data
- Open Data interfaces of the Finnish Meteorological Institute now also available without API key at https://opendata.fmi.fi/wfs (wfs) and https://openwms.fi/geoserver/wms (WMS)/Mikkov.
- The Finnish Meteorological Institute will publish a new demo service for open data at: http://beta.fmi.fi/data/3/wfs/sofp you can download Hirlam and Harmonie weather forecasts and Finnish observations. The service follows the new WFS3 standard and thus Openapi practices. More information at GitHub: https://github.com/fmidev/smartmet-sofp-backen is a demo. We strive to keep the service upright at least this year, but of course we will not give it any guarantee. We are also ready to develop the service based on your feedback! Give feedback by responding to this thread or making a github ignition: https://github.com/fmidev/smartmet-sofp-backend/issues

The content related to the service provision is some of the most highly interacted with content (exceeded only by that relating specifically to the operation of the newly launched mobile application). In particular, we also saw high numbers of average comments on these posts (4.76 comments per post) and an average of over 24 likes per post). Therefore, it is possible to conclude that such accounts across the different platforms used by FMI would be able to successfully spread and inform users about adverse events in the scope of a crisis.

3.2.3. ONDA DIAS

Compared to the NOA and FMI online accounts, ONDA DIAS (Data and Information Access Service) is specifically providing a service to its users and therefore the posts have a different orientation and emphasis: (1) to attract users to the service through the presence of news and research outcomes; (2) to highlight new features and capabilities of the service; and (3)

to connect to the users of the service including providing information about service disruption. The page currently has just over 170 likes and so the interaction figures are relatively high although it is clear that the majority of these interactions (Table 3-7) are likes rather than comments with some shares. Interestingly, it is the YouTube content that has the greatest engagement on this account.

Type	Average of Total Interactions	Average of Likes	Average of Comments	Average of Shares
Link	6.62	5.54	0.00	1.03
Native Video	5.00	4.33	0.00	0.33
Photo	6.33	5.65	0.03	0.61
Status	4.50	4.00	0.00	0.50
YouTube	8.50	7.75	0.00	0.75

Table 3-7 - Average interactions for ONDA DIAS

Considering the posts about the service, this includes posts that advertise upcoming changes to the service:

- ❗ *New Object Storage technology soon on ONDA* ❗ *Announcing that ONDA is planning to progressively integrate the new #OVHcloud #ObjectStorage solution accessible through #S3API to replace the current storage technologies.* 👉 *https://bit.ly/3wU6KVR:=:https://www.onda-dias.eu/cms/new-storage-technology-soon-available-in-onda/*
- *Do you require access to a massive volume of data for your application? We are happy to launch our new MOST service, which allows you to:* ☑ *optimize performance in accessing ONDA data* ☑ *reduce costs* ☑ *improve productivity* ➡ *Request your private storage in the ONDA archive and automate your journey!* ℹ *Read more: https://bit.ly/2HIb5Wv:=:https://www.onda-dias.eu/cms/services/catalogues/most-managed-onda-storage/ #peopleONDAta*
- 📣 *The ONDA Catalogue has now surpassed the milestone of* ➡ *30 million products, all physically stored on our infrastructure! Including Copernicus EU #Sentinel data full archive, Envisat, Landsat 8, CMEMS, CLMS, CAMS. More on our Data offer: https://bit.ly/2UHON9x:=:https://www.onda-dias.eu/cms/data/catalogue/ #OpenData #peopleONDAta*

The ONDA services are also the first significant example of an organisation posting about an incident caused by an outage on a dependent service, along with subsequent updates about its affected services. The first post stated the following: (emphasis and markup added)

- *Following a **major incident** this morning on OVH Cloud infrastructure in Strasbourg [problem description], all of our services have been **temporarily disabled** [service update]. We are in contact with OVHcloud to restore them back to normality in the shortest possible time [current actions and time frame] and will update on the situation as it progresses [next steps]. Please bear with us!*

This content provided information that there had been an incident although not the context of the incident itself, the current statement of the status of the service and what the organisation plans to do next. There is no action for the users of the service. Two days later an update is provided, noting that there are still issues with the service and highlighting where more information can be found. The post seeks to reassure customers about the service and indicates that parts of the service are still operational and well as apologising to customers and again providing a link to the update.

- *Update on the OVHcloud incident: **we are working hard to restore our services in the shortest possible time**! [reassurance] You can find the OVHcloud updates on the **status** on https://bit.ly/38ADub5:=:https://corporate.ovhcloud.com/en-ie/newsroom/news/informations-site-strasbourg/ [more information] We wish to stress that all virtual resources located in other datacenters are **fully operational** and accessible.[reassurance and service availability] In addition, new resources can be created as well - please contact us. Concerning the ONDA Data Access services, the historical archive of Earth observation **data is safely stored on the ONDA Cloud Archive**, redundant in other centers. [service update] We **apologize** for the difficulties caused by this incident: we are continuously assessing the impact [contrition], and further updates will follow on the solutions and services restoration. www.onda-dias.eu:=:https://www.onda-dias.eu/cms/ [further information].*

Four days later a further update was provided providing more details about the action the company was taking and a more detailed assessment of the impact of the incident as well as acknowledging that some customers will be facing issues and their proposed next steps. A current service update was also provided as well as again a link for further information.

- *Update on the OVHcloud incident that took place on 10 March [time] at the Strasbourg datacenter: 🔵 The restoration activities are progressing as planned. [organisational response] 🔵 Based on the OVHcloud assessment of on the status of the ONDA assets, most Virtual resources are recoverable and will be accessible again as soon as the restoration activities are completed [service update]. 🔵 Those users with resources that unfortunately are not recoverable will soon be contacted by our support team to arrange the replacement. [next steps] 🔵 The ONDA Catalogue is up and running again - for the moment a limited subset of metadata is exposed and searchable and the full set of metadata will be made accessible gradually.[current status] For the latest information from OVHcloud, please check the status page:*

https://bit.ly/3eLbeX2:=:https://corporate.ovhcloud.com/en/newsroom/news/informations-site-strasbourg/ Or contact us: https://bit.ly/3bT0wvX:=:https://www.onda-dias.eu/cms/contact-us/ [further information]

A final update was provided three further days later providing information on the general current service status, remaining issues, actions to be taken by users where necessary, actions to be taken by the service provider and again where to find further information.

- *Update on the ONDA status further to the OVHcloud incident: The **ONDA User Portal is accessible and operational** since 17 March [service update] (users already registered might need to register again). [user actions] The ONDA Public Dashboard has also been restored, and provides updated information about the current status of ONDA services and published datasets. [detailed service update] A few services still unavailable will restart in week 12. [remaining issues] Replacements for the non-recoverable resources are being arranged. [service provider actions] More info: https://bit.ly/3c0sGVH:=:https://www.onda-dias.eu/cms/updates-on-major-incident-at-ovhcloud-infrastructure-12-march-2021/ [further information]*

Looking at the interaction metrics there were very few interactions from followers of the Facebook page about the incident or the service updates. Only the second message, receiving five likes had any significant acknowledgement.

Cross-checking across the data collected from the @ondadias Twitter feed, we see that much the same information is reported albeit in a briefer format but with slightly higher levels of engagement as can be seen in the table below (Table 3-8).

Text	Timestamp	Favourites	Retweets
Update on @OVHcloud incident: the User Portal is operational since 17 March, the Public Dashboard has been restored and other services will restart in week 12. We are arranging replacements for those users with non-recoverable resources. More info: https://t.co/h6WlRXzVCp	2021-03-19 15:48	4	0
Update on @OVHcloud incident: restoration activities progressing as planned, with most users VMs recoverable. A replacement will be arranged for unrecoverable resources of impacted users. The ONDA Catalogue is available with a limited subset of metadata. https://t.co/XrLDrORvV0	2021-03-16 09:58:15	1	1
Update on @OVHcloud incident: we're working hard to restore our services as early as possible. Resources located in other datacentres are operational & new ones can be created on request. The EO data historical archive is safely	2021-03-12 16:24:47	6	3

stored on our Cloud Archive. Updates will follow.			
RT @OVHcloud : Statement on the incident at our Strasbourg site https://t.co/0L3GOK5Jx5 https://t.co/IMM2bqGFcL	2021-03-10 11:58:15	0	0
Following a major incident this morning on OVH Cloud infrastructure in Strasbourg, all of our services have been temporarily disabled. We are in contact with @OVHcloud to restore them in the shortest possible time and will update on the situation, please bear with us!	2021-03-10 09:40:44	5	2

Table 3-8 - Onda DIAS tweets in relation to cloud incident

Another interesting aspect when looking at the @ondadias tweets over time is the feed is used only as an information provision to users and not used to engage in two-way conversation. Figure 3-7 below shows that the majority of content is either organic tweets or retweets with only one reply in the entire dataset.

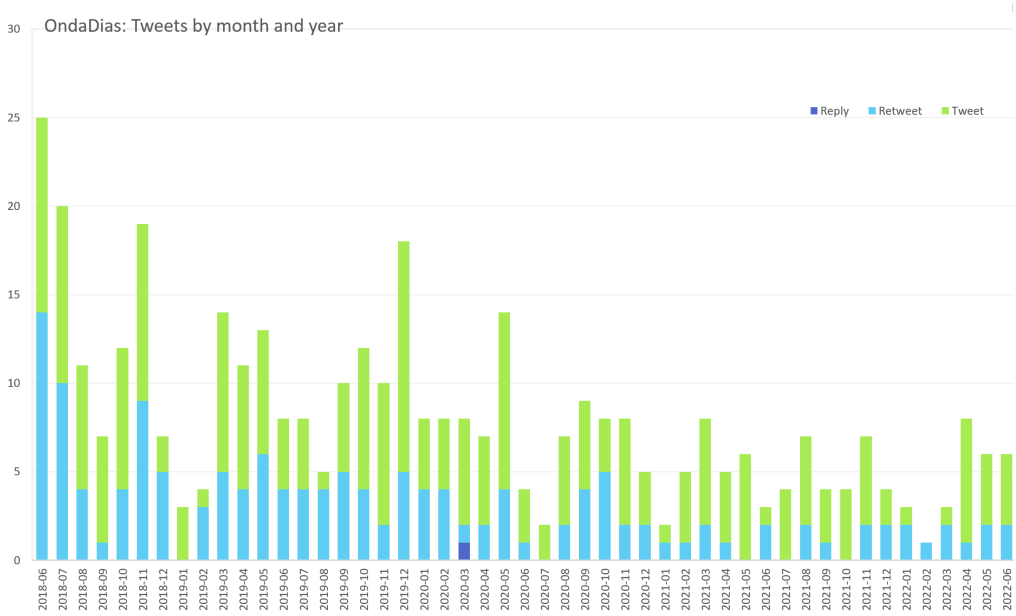


Figure 3-7 - Onda DIAS tweets over time

3.2.4. Ice Cubes Service

Similar to ONDA DIAS the Ice Cubes Service operated by SpaceApplications has both a Twitter and Facebook page to connect with users of the service and to promote the services' capabilities, especially to the research community. While the Facebook account has a very limited number of posts the Twitter feed has over 600 posts stretching back to 2016. From the Twitter account it can be see (Figure 3-8) that most of the posts are oriented towards organic tweets or retweets with a couple of occasions where replies spike; however, a closer examination of the data highlights that the replies are replies from the Ice Cubes account and therefore are not communications with external accounts.

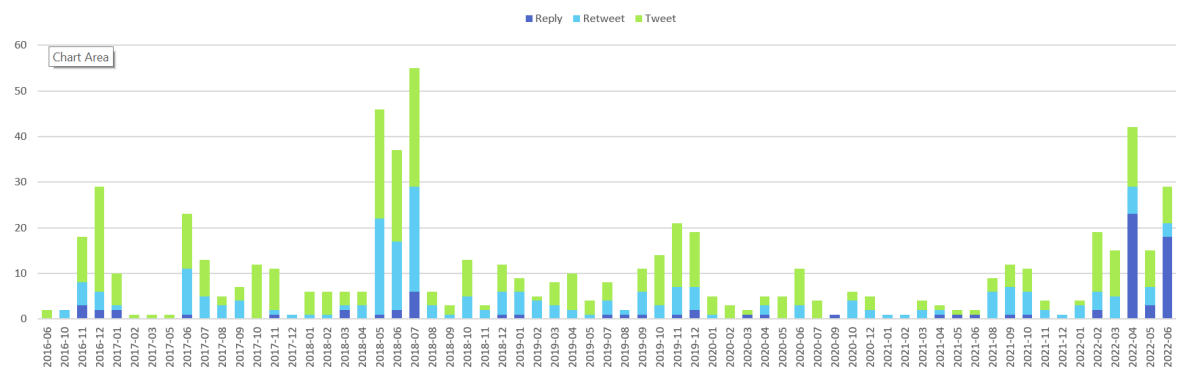


Figure 3-8 - Ice Cubes Service - tweets over time

The IceCubes' account does provide service update and information about the functionalities available through the service as well as the possibility for users and researchers to engage with the platform going forward. The majority of the content focuses on promoting existing research with the service and the potential outcomes that can be achieved. For example,

"The ISS gives access to a unique environment with assets that cannot be reproduced on Earth and that can offer applications for Earth and Space R&D" #ElevateYourResearch

"Built around a @GoPro camera, our ICE Cubes Media Set will be connected to the ICE Cubes Facility on board the ISS, enabling users to engage in real-time audio and video communication with the #ISS from their own premises around the world, on a #commercial basis. 💥🚀*"*

The Facebook account also posts message with a similar theme: for example,

"#ElevateYourResearch Competitive advantage. That is what doing research and development for your products in microgravity can get you. Your product development process can benefit from superior results, way better than those obtained in conditions of gravity. 🚀 *In a world where companies are increasingly innovative, the ICE Cubes Service gives you the opportunity to ride on the microgravity train and take your business forward!* 💭 *What is the experiment you would want to see on board the ISS?* 💙 *#space #experiments #research #microgravity #icecubes #technology #innovation"]*

Overall, however, the Ice Cubes service currently uses its social accounts to promote the capabilities and research potential of the services, due to this they engage in little bi-directional communication and overall engagement on the page is low. However, as this is a niche area it is unlikely that high engagement would be expected overall.

The Space Applications accounts were not evaluated as they focus on the YouTube[15] and LinkedIn[16] platforms; however, the content is a similar style to that of the Ice Cubes' pages.

[15] Space Applications Services NV/SA. YouTube. https://www.youtube.com/channel/UCaylo0mjGppV5V-knTJRuiA
[16] Space Applications Services NV/SA. LinkedIn. https://www.linkedin.com/company/space-applications-services

3.2.5. Elecnor DEIMOS

Elecnor DEIMOS operates space infrastructure and technology in Spain. It has an active Twitter account which is supported by a further account on Instagram. The Twitter account has just over 2,500 followers and has tweeted updated regularly since inception in 2011. While the number of tweets has changes over the years, we can see the change in strategy for the account by looking at the tweets, retweets and replies over time. As can be seen in Figure 3-9, while the majority of tweets were originally organic tweets, during the period of 2015 to 2018 a high proportion of tweets were retweets while although the overall number of posts has decrease in recent years this appears to be due to the concentration on organic posts. While there are some replies for the most part this is limited, again demonstrating that most accounts are set up for informing but not for bidirectional engagement.

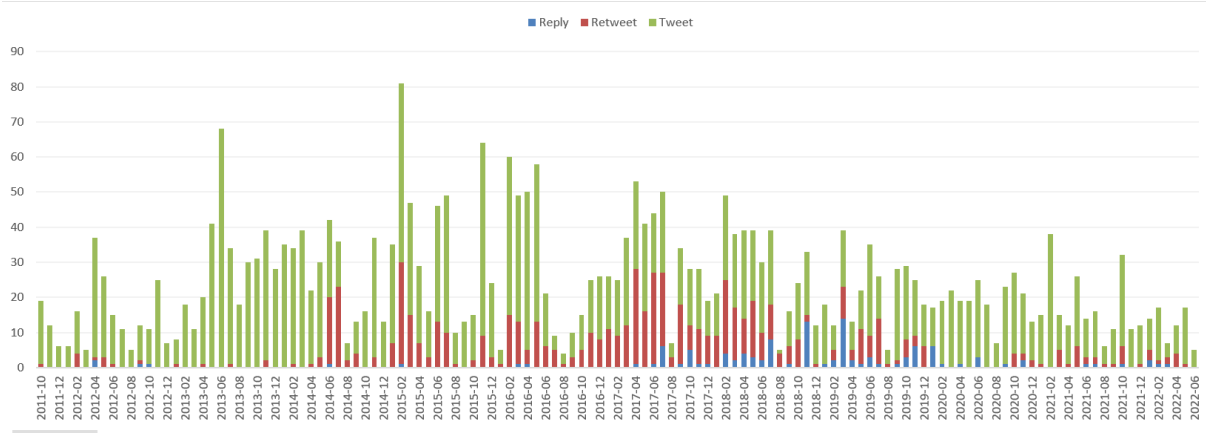


Figure 3-9 - Elecnor DEIMOS - tweets over time

As well as news, general posts and events, the account also provides service updates to supports customers or users. These are often announcing new partnerships with other services or newly updated services, for example:

- *"Very happy to announce our MoU with Dragonfly Aerospace 🪐 With this agreement we will be providing Dragonfly's #nanosatellite cameras with on-board processing capacity with our #Insight4EO product. Check it out 👇 https://t.co/MsDNAgQ8zD";*
- "Announcing our agreement with Skylabs 🤝 Deimos' new Attitude and Orbit Control System #AOCS product will incorporate SkyLabs' On-Board Computer #OBC and Remote Terminal Unit #RTU 👇 https://t.co/8Dga3zt5gp #smallsatellites #deimosFlightSystems #deimosSatelliteSystems;
- *"Centu-1 is one of the 4 telescopes comprising #DESS, Deimos Sky Survey, an advanced complex for surveillance, tracking and catalogue of near-Earth objects, like #satellites and #spacedebris 🚀 #deimosSpaceSafety https://t.co/ohF9V73mWi".*

As Elecnor DEIMOS also provides other services beyond the space sector some posts are related to other domains.

The Instagram account is also relatively active considering it has only been in operation for approximately 18 months and the content is limited to posts or short videos. There have been 61 posts and mainly focus on highlighting their presence and conferences and events as well as other information particularly suited to the visual medium. Instagram is generally not considered a strong platform for two-way engagement, and this is reflected in the interactions with almost all interactions being in the form of likes with almost no comments across all of the posts. Therefore, it is more likely that Elecnor DEIMOS would use the Twitter account to post in the event of a incident or service disruption.

3.3. Outcomes of analysis

Based on the above analysis it is clear that space and ground segment operators are taking advantage of social media to communicate with the public, their service users and customers. Most of the pages have a reasonable following of online users (relative to the size and scope of their service) and thus are achieving what is suggested for many organisations who may have to communicate in a crisis – already have a connection to your audience. In terms of the posts themselves, most of the current communication falls into the awareness raising categories posting general news, events interesting space/satellite imagery. This is also important for raising awareness, potential engagement and building an overall community given that posts made during a crisis, no matter how effectively they are constructed, will not have the desired impact unless they reach the correct people.

In terms of crisis or incident communication there are good examples from NOA, FMI and ONDA DIAS posting about site closures and service disruptions. ONDA in particular demonstrated how to post clear information about service interruptions containing all relevant information segments that a user or consumer may need to know to respond and update their own services accordingly.

A note of caution across most accounts is the relatively one directional orientation of posts (authorities to citizens). This means that potentially little information coming in the opposite direction is being leveraged to inform other incident response or address gaps and challenges. While this may also be an artefact of the limited number of incidents faced during the data collection period, it is something that organisations should be aware of in case of a major incidents as it is significantly more difficult to set up such monitoring processes during an incident than beforehand.

4. Case studies – communication in CI incidents

In addition to the analysis in the previous section it is also important to consider how other CI operators have approached crisis communications when an incident has occurred. We have selected several incidents from the past five years to review how they have approached the crisis communications response in the event of an interruption to their services and where possible also considered any lessons learned that have been published. Each case study presents a short timeline of the events, the outcomes of the incident and then the associated communication media and whether this response was considered to be a success.

4.1. Case Study 1 – WannaCry: Disruption of the NHS

4.1.1. Timeline of Events

On the 12th of May 2017, a global ransomware attack labelled "WannaCry" was recognised in affecting over 200,000 computers operating Microsoft Windows in over 100 countries [51]. WannaCry can be understood as an example of cryptocurrency ransomware, whereby malicious software is used to encrypt valuable files and/or data and requests the payment of Bitcoin as ransom.[17]Noted by multiple reports, the WannaCry attack has been identified as one of the largest and most globally damaging ransomware attacks to date [52][53].

Victims of the attack included large-scale organisations such as the Spanish company Telefonica, FedEx and Nissan Motor Manufacturing in the Tyne and Wear, UK. A well-documented victim however was the National Health Service (NHS) in England and Wales who were significantly affected by WannaCry, although it was not the specific target. At 13:00 on the 12th of May, the NHS Digital's CareCERT service alerted the Department of Health and Social Care after reports of ransomware attacks were raised by four NHS trusts. This later increased to 16 trusts by 16:00. Upon receiving these reports, NHS England and NHS Digital declared a "national major incident" [54]. NHS England made declaration of a major incident and in response initiated its "Emergency, Preparedness, resilience and Response (EPRR)" action plan. Within this, NHS England with the support from NHS Digital and NHS Improvement acted at the single point of contract for coordinating and managing the incident [55].

The response made by the NHS can be seen divided into three phases which began from the 12th of May. The first consisted of securing the emergency care pathway. Then, assurance was made to ensuring that the primary care of patients was stable from an operational perspective. Following this, the wider system actions and anti-virus updates were implemented. During this period, a series of communications activities occurred both internal and external to the NHS. Included in this was a CareCERT cyber bulletin which was

[17] Kaspersky (n.d.) What is WannaCry ransomware? https://www.kaspersky.co.uk/resource-center/threats/ransomware-wannacry

disseminated across the NHS, providing a technical overview of the ransomware and advice on remediation. This was primarily focused on prevention, which also included a "kill switch" which was discovered that prevented the malware from spreading more broadly. In all the incident lasted a week, ending at 17:30 on Friday the 19th of May 2017 [56].

Overall, the WannaCry incident had a significant, immediate and long-term impact on the NHS. It was estimated that at least 80 out of 236 trusts, 603 primary care and 595 GP practices were affected due to the ransomware itself or by turning off the devices/systems as a precautionary measure. This led to a 34% disruption rate of trusts within England, however the full extent of the incident is unknown. This disruption included an estimated 19,000 cancelled appointments, breakdown of radiology and pathology departments of whom relied on MRI scanners for example and significant delays in updating patient information and sending test results. It was therefore estimated by the UK government that the costs to the NHS were £19 million in disruption to services and £73 million in direct technical costs [57].

Following the incident, significant efforts were made by the Department of Health and Social Care to build resilience against any future attack. For example, £21 million was funnelled into addressing vulnerabilities in critical elements of NHS systems such as ambulance trusts, and to find solutions to resolve essential technology weaknesses [51].

4.1.2. Vulnerability Factors and Review

Following the WannaCry incident, the NHS was subject to critical reviews by the UK Government and other stakeholders to determine the causes of the attack, the response made and build recommendations to build resilience against future attacks.

A key finding was that the WannaCry ransomware was able to infect segments of the NHS due to organisations not maintaining a good standard of cyber-security practice. Specifically, the Department of Health [51] identified a common vulnerability across the trusts that were infected as having an outdated Windows operating system which was exploited by WannaCry. Due to this, WannaCry was able to exploit the security vulnerabilities in the Windows software, including DoublePulsar and EternalBlue [59]. Applying the update was communicated by NHS Digital to the trusts prior to the attack on the 17th of March, however this was not implemented by all trusts. If the update has been implemented, it is believed that the systems would have been protected from WannaCry.

The preparedness of the NHS for addressing cyber-attacks was also evaluated. Prior to the attack, NHS Digital provided trusts with an on-site inspection labelled CareCERT to assess the effectiveness of their cyber-security. This was however voluntary, which means only 88 out of 236 trusts were inspected by the 12th of May. Based on the 88 trusts, none passed the inspection. A conclusion found was that trusts were unaware of the risks of cyber-security to patients and overestimated their ability to respond to and manage a cyber-attack. Following this, CareCERT provided advice and guidance to the trusts to improve

their security, which were acted upon by trusts with more mature cyber-security arrangements, but not by the more vulnerable trusts. Despite the clear vulnerabilities highlighted, NHS Digital argued that this reflects a lack of understanding of the impact and scale of cyber attacks such as WannaCry, rather than neglecting cyber security arrangements [51].

In a review by NHS England, tangible actions can also be seen undertaken following the WannaCry attack to improve the cyber security of the institution. Included are dissemination materials such as the "Cyber Handbook" [56] which outlines the approach to be taken by NHS England, Digital and Improvement in the event of another cyber-attack affecting the NHS. Furthermore, funding (£25 million) has been provided to help NHS trusts that identified as being non-compliant against cyber security assessments. This funding will support them in strengthening IT hardware and software. They also provided a set of recommendations for local NHS organisations to build resilience in a 'bottom-up' approach. Included in the recommendations is the development of local action plans that will be compliant with the Cyber Essential Plus standard. Another action plan was to implement cyber incidents within local organisations' business continuity and disaster recovery plans [56].

4.1.3. Online Communications

In tangent with the attack and the events that unfolded within the NHS, NHS Digital was a large contributor to the communication efforts. Specifically, it provided updates to NHS staff and the wider public on the investigation. For instance, it provided a statement (Figure 4-1) at the early reporting stage to note that several reports have been made about a ransomware attack and that no evidence has emerged which indicates that patient data has been accessed.

Figure 4-1 - NHS statement on WannaCry incident

However, the communication from NHS Digital was criticised as being delayed in providing NHS trusts with vital communications. For instance, it took four hours from receiving the

first report NHS Digital to sending out any advice or communications to the organisations who were in need of advice on how to respond [60]. Furthermore, many organisations shut down communication connections to prevent being affected by the attack. This resulted in not all populations receiving the information needed on how to prepare themselves or prevent being affected by the attack [61].

On Twitter, corresponding stakeholders communicated about the attack. For example, on the 12th of May Action Fraud posted about how users can protect themselves from WannaCry (Figure 4-2):

Figure 4-2 - Twitter post by ActionFraud about the NHS WannaCry incident

However, this post does not provide any information on what actions anyone who is currently infected should take. Nonetheless, following the attack NHS Digital became a key speaker in communicating and raising awareness to building effective cyber security. For instance, in October for 'Cyber Security Month' NHS digital began posting advice and links to best practices in reducing the risks in being affected by ransomware (Figure 4-3).

Figure 4-3 - Post-crisis messages in preparation for future incidents

This reflects the changing landscape in the NHS institution in relation to cyber security and ensuring that trusts are implementing effective measures and approaches to improve

resilience. As noted by Hoeksma [62] the WannaCry incident has been a "valuable wake up call" for the NHS to improve its resilience and preparedness for future cyber-attacks.

In terms of other communication, due to the incident, many NHS services were struggling to communicate and official reports noted that WhatsApp was utilised as an internal communication tool in the absence of email and other services [51]. In fact, what is striking about the WannaCry attack is the limited analysis or information about communication to patients and other affected groups with most post-hoc reviews focusing on the effectiveness of internal communication. Other reports stated that stakeholders were relying on the BBC News website for ongoing information about the incident.

4.2. Case Study 2 – Texas Power Grid Failure

4.2.1. Overview of events

In Texas, United States a major power crisis was caused by a short period of three extreme winter storms in February 2021. The storms caused significant issues with the power supplies leading to an inability of several million residents to access power and subsequently heat, food and water supplies. Official estimates put the death toll at almost 250 people with other estimates believing the toll could have been even higher [63]. Texas rarely experiences extreme low temperatures (up to -19°C in this case) and buildings and homes are generally not equipped to retain heat; therefore, during the storms demand for power increased significantly. This was combined with a failure of infrastructure – natural gas, coal and nuclear power plants had all suffered mechanical failures or had frozen up while wind turbines and solar energy had also suffered. The increased demand for energy exceeded existing modelling and demand expectations almost leading to a complete grid failure.[18] In addition to the energy failures, water supply was interrupted due to burst or frozen pipes and many stores either ran out of food or had to close due to the energy power failure.

4.2.2. Official Communications

The impact of the #TexasFreeze was so severe that Twitter has published their own case study on the range of communications conducted over its platform during the crisis in conjunction with the Sprout Social platform. The communications happening over Twitter about the crisis were extensive. The case study [64] notes the following from Andrew Caravella, VP of Global Partnerships at Sprout Social:

"The conversation around #TexasFreeze, #TexasSnow and #TexasPowerOutages included more than 186,000 Tweets, which received over 625,000 engagements and had a total reach of more than 825 million impressions, proving the power of Twitter to not only engage locally but drive awareness and create connection globally."

[18] 2021 Texas Power Crisis (2022) Retrieved June 15, 2022 from https://en.wikipedia.org/wiki/2021_Texas_power_crisis

While the case study highlights the effectiveness of citizen-to-citizen communications and the ability to raise awareness and build a sense of community what most people were lacking was effective communication from those in authority (government officials, energy providers, etc.) [65]. This was emphasised by the review of the crisis communications from Schuman [66], firstly noting that it is easy for crisis communications can easily be deprioritised if the organisation is focused on dealing with the actual crisis itself but that ultimately this can lead to citizens missing crucial advice or lead to reputational damage in the long-term. The Texas Power Grid incident was exacerbated by the fact that Texas has separated itself from the national power grid leaving it uniquely vulnerable in times of crisis. Therefore, it is the responsibility of ERCOT (Electric Reliability Council of Texas) to manage the electricity provision in the state.

At the start of the crisis, ERCOT shared a number of messages (Figure 4-4) but these did not convey the potential seriousness of the impending crisis.[19,20]

Figure 4-4 - Initial tweets from ERCOT at the beginning of the crisis

It was only the following day that the messages became more urgent, first stating that 'energy conservation is needed'[21] and then ultimately confirming the implementation of rotating outages due to generators going offline.[22] As time went ERCOT continued to provide a range of information including confirming at one point that 2.7 million households were still without power[23] and only acknowledging the difficulties faced by customers after three days.

"We know this is hard. We continue to work as quickly and safely as possible to restore power. We gained some MWs overnight but are back to 14,000 MW of load shed; lost east

[19] https://twitter.com/ERCOT_ISO/status/1359960036718632964
[20] https://twitter.com/ERCOT_ISO/status/1360964580126699526
[21] https://twitter.com/ERCOT_ISO/status/1361197991659503618
[22] https://twitter.com/ERCOT_ISO/status/1361215084010352644
[23] https://twitter.com/ERCOT_ISO/status/1362007980485451779

DC-tie imports due to Midwest power emergency. We hope to reduce outages over the course of the day."[24]

The government also drew criticism for the lack of communications around the outage [67], noting that in the immediate onset of the storms there was very little communication and it took until several days into the crisis to hold a press conference although there were some limited communications. Research from Busby et al. [68] has particularly noted that:

"Texans did not receive adequate warning from the governor or other public officials to prepare for the storm and what steps they should take to protect themselves or reduce energy demand. This lack of emergency preparedness communications was notable and could have exacerbated risk to life and property."

This indicates a critical failure in the crisis communication efforts exacerbated by a lack of "coordinated, consistent, and timely emergency communication".

The Texas power crisis highlights several failures of communication, firstly during the pre-crisis stage the messages were not communicated with enough urgency or actionable information for citizens to take appropriate action to conserve energy. By the time that more urgent communications were shared the power had already been lost in several areas and thus people were no longer able to access up to date information over the internet. Further, as the case study from Twitter shows, many citizens were communicating about their experience of the freeze, this could have provided an opportunity to capitalise on the key elements of this information and follow up with appropriate advice and warning messages.

4.3. Case Study 3 – Colonial Pipeline Hack

4.3.1. Timeline of Events

On Thursday 6th of May 2021, the US-based Colonial Pipeline Company was the target of a ransomware cyberattack which has since been labelled as the most significant attack on critical national infrastructure in history. The Colonial Pipeline Company operates the Colonial Pipeline, a 5,500-mile-long pipeline which delivers refined oils to 12 states, carrying 45% of the East Coast's fuel supplies. Beginning in Texas and terminating in New Jersey, Colonial's pipeline delivers nearly 2.5 million barrels of fuel each day, servicing jet fuel to major airports and gasoline for automobiles and transport systems.

Upon discovery, on the 7th of May the Colonial Pipeline Company were forced to shut down its operations after hackers seized 100 gigabytes of data before encrypting software systems with ransomware and demanding payment through cryptocurrency. Contrary to reports, the Colonial Pipeline Company paid nearly $5 million in ransom fees to restore its operations [69].

[24] https://twitter.com/ERCOT_ISO/status/1362046636956913667

On the 8th of May, Colonial released an initial statement on their website and social media stating that the company became aware of the attack on the 7th of May and that they have identified that it was ransomware related. In addition, they stated that they had alerted and would now be working with the relevant law enforcement and federal agencies who helped take systems offline and stop the flow of stolen data to the hackers. The agencies involved included the White House, NSA, the CISA (Cybersecurity and Infrastructure Security Agency), the F.B.I., and the Energy Department.

On the 9th of May, Colonial released a secondary statement detailing out its action in the previous 48 hours. This involved addressing that the company had determined the attack was ransomware related, its further cooperation and investigation with relevant agencies, and stating its intent to bring the fuel lines back into operation once it is safe to do so. Also on the 9th, the U.S. Department of Transportation declared a temporary hours of service exemption allowing for greater transportation of fuel along the East Coast.

On Monday the 10th of May, despite President Biden declining to implicate Russia, the F.B.I. confirmed that DarkSide – a Russian affiliated hacker group – were involved in the ransomware attack. On the same day, Colonial also released a statement detailing its goal to restore its operations back to full capacity by the end of the week alongside highlighting that some of its smaller fuel lines were in now manually operational.

On the 11th of May, Colonial described a number of different fuel transporting systems that were now in place in an effort to ease demand. Colonial's website also went down and has not begun operating again since (Date 17/5/21). On the same day, the U.S. Environmental Protection Agency (EPA) released two statements explaining their issuing of an emergency fuel waiver to help prevent fuel shortages in the affected states.

On the 12th of May, amid a sea of panic buying down the East Coast of the US – and with more than 1,000 fuel stations running out of gasoline – Colonial stated that it would be restarting its operations at 5pm, although it would take a number of days for operations to return to normal.

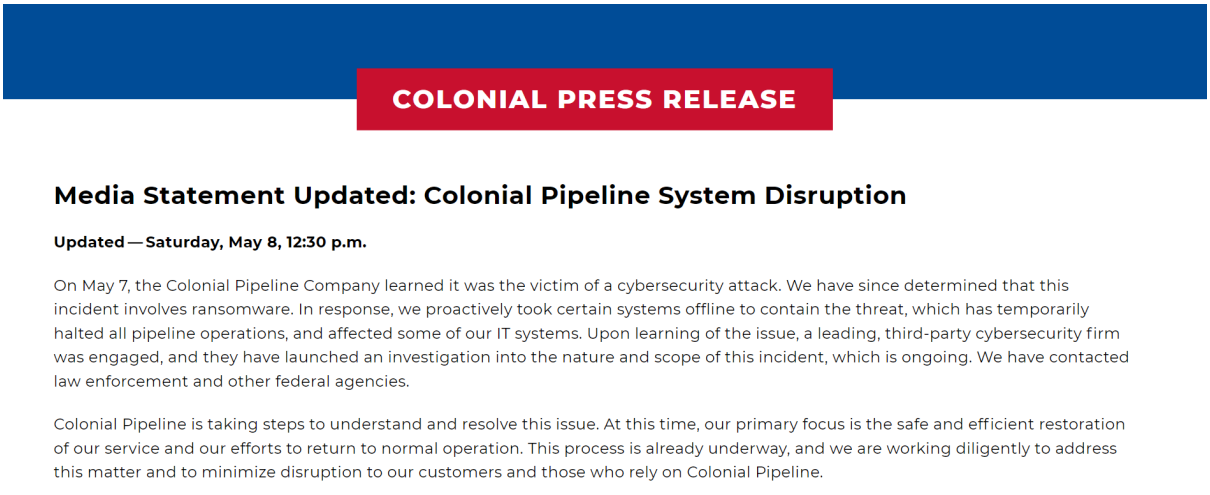
On the 13th of May, it was revealed that Colonial had paid nearly $5 million in ransom to DarkSide. In contradiction to earlier reports that Colonial had no intention of paying the ransom, Bloomberg reported that Colonial had paid the ransom on the 7th, the day the hack began [69]. On this day, President Joe Biden also released his first statement on the attack detailing out their coordinated response.

On the 15th of May, Colonial stated on Twitter that all of its markets were now receiving fuel from their pipelines alongside detailing its commitment to IT and cybersecurity over the past 5 years. 'We have increased total spending on our IT program – including cybersecurity, information governance and IT infrastructure – by more than 50% since 2017, when we appointed our new Chief Information Officer.

4.3.2. Communications on social media

The first evident communications of the cyber-attack from the associated agencies on Twitter was on the 8th of May from CISA. This communication briefly detailed out CISA's awareness of the ransomware incident and stressed their ongoing cooperation with Colonial and other agencies.

Following CISA's statement on Twitter, on the 9th of May, the Colonial Pipeline's company released a statement detailing out its awareness of the attack. Released via Twitter, the company continued to release a statement on the attack and its response in the following 3 days: the first statement read as in Figure 4-5 below [70].



COLONIAL PRESS RELEASE

Media Statement Updated: Colonial Pipeline System Disruption

Updated — Saturday, May 8, 12:30 p.m.

On May 7, the Colonial Pipeline Company learned it was the victim of a cybersecurity attack. We have since determined that this incident involves ransomware. In response, we proactively took certain systems offline to contain the threat, which has temporarily halted all pipeline operations, and affected some of our IT systems. Upon learning of the issue, a leading, third-party cybersecurity firm was engaged, and they have launched an investigation into the nature and scope of this incident, which is ongoing. We have contacted law enforcement and other federal agencies.

Colonial Pipeline is taking steps to understand and resolve this issue. At this time, our primary focus is the safe and efficient restoration of our service and our efforts to return to normal operation. This process is already underway, and we are working diligently to address this matter and to minimize disruption to our customers and those who rely on Colonial Pipeline.

Figure 4-5 - First Colonial press statement

Again, on the 9th of May the F.B.I. released a similar statement on social media demonstrating its awareness of the attack alongside highlighting Darkside's involvement [71].

Initially, Colonial posted a link to their service disruption page with no additional text or context to their Twitter platform – these posts were made on the 9th, 10th and 11th May 2021. Most of the communications on social media surrounding the attack were released on the 11th of May, four days after the attack. Amongst those statements from officials, the White House held a press briefing detailing out its response to the attack but mainly to the future of cyber security in the US. Within this briefing, Secretary Jennifer Granholm (Secretary of Energy) briefly asked consumers to look out for price gouging and fuel hoarding in the affected areas stressing that there is no shortage of fuel, but that there were just experiencing a fuel crunch. She then went on to stress and detail out the affected areas. In the communications from Colonial there was no mention of the impact (or lack thereof) on customers or what actions they should/should not take in order to not multiply the effect of the attack. In fact, Colonial did not make any posts about the incident itself, it only

provided links to more information and then finally started posting when systems began to come back online. For example:

- *Thanks to the commitment and dedication of the many Colonial team members who worked safely and tirelessly through the night, Colonial product delivery has commenced in a majority of the markets we service. Latest update: https://t.co/kpWNw0UQve*[25]*;*
- *As we previously reported, Colonial Pipeline initiated the restart of pipeline operations at approximately 5 p.m. ET on Wednesday, May 12. Since that time, we have returned the system to normal operations, delivering millions of gallons per hour to the markets we serve.*[26]*.*

Between the 11th and 15th of May, until the pipeline resumed operations, the Department of Energy and Secretary Jennifer Granholm's Twitter handle released a series of tweets stating their continued dedication to getting the fuel pipeline back online (Figure 4-6). Within these tweets, there were videos released by the secretary where she again stressed the need to identify price gouging and prevent fuel hoarding.[27] Alongside this, President Joe Biden also released a statement on the 13th of May detailing out the government response to the incident and future cyber security threats.

Figure 4-6 - Tweet from Jennifer Granholm about the hoarding of gas during the Colonial pipeline incident.

[25] https://twitter.com/Colpipe/status/1392829931651059718
[26] https://twitter.com/Colpipe/status/1393529174598504454
[27] https://twitter.com/SecGranholm/status/1392892537598189572

However, despite these tweets from officials, the communications surrounding the attack on Twitter were predominantly monopolised by news anchors alongside ordinary citizens. Articles released on the attack by news anchors mainly explained the nature (ransomware) of the attack alongside warning of fuel shortages but without crisis messages outlined by the Energy Secretary. This led to panic, widespread fuel hoarding, and gas stations running out of fuel in a number of East Coast states, including Florida – a state which the Colonial Pipeline does not service. Other government entities took a proactive approach to ensure they were able to get the message out to the public:

- *"Alabama Gov. Ivey spoke with Department of Energy officials who told her the pipeline should be operational within a few days. She says the gas shortage hasn't hit Alabama and people should not panic buy. "Only fill up you if you need to and do not fill up multiple containers.""*

An example of the type of information shared on social media from news organisations include the following. As can be seen in these posts, these cover the incident itself, the impact on the fuel situation and broader commentary of the state of the United States' cyber security defences:

- *"The shutdown at Colonial Pipeline, which stretches from Texas to the Northeast, is stretching into its third day with an "all-hands-on-deck" effort to restore operations and avoid disruptions in the fuel supply."*[28]*;*
- *UPDATE on #ColonialPipeline: This morning, @redacted is reporting "the majority of our travel centers are stocked with fuel at this time.";*
- *"Colonial's decision late Friday to shut down a pipeline that is the main source of gasoline, diesel and jet fuel for the East Coast, represents a dangerous new escalation in the fight against ransomware, which President Biden's administration has identified as a priority.".*

Some journalists were also providing more details about the mechanics of the attack and its implications for Colonial's systems:

- *"Colonial's op network controls flow of fuel from pipeline to distributors then passes info to ticketing system on IT network to automatically invoice distributors. If ticket system is locked and pipeline is still flowing Colonial can't monitor flow and send invoices to get paid."*[29]

Similarly, as we previously discussed there are limited opportunities to extract soft intelligence from social media during an incident. While it is extremely difficult to anticipate an incident ahead of time by extracting the needle from the haystack of social media, intelligence about how citizens or the public are acting during the incident or further

[28] http://twitter.com/FOX26Houston/status/1391535999575023621
[29] http://twitter.com/KimZetter/status/1391574630163304450

cascading effects may be significantly easier to detect. For example, the posts range from citizens with relevant expertise to the situation:

- *"the Colonial pipeline shutdown will have the biggest impact on prompt (retail) gasoline and diesel prices…likely this will not affect the curve unless it becomes a prolonged incident";*
- *"Colonial pipeline went down ... get ready for even higher gas prices in the southeast and east coast if it's not resolved quickly".*

While other citizens were focused on the impact of the gas price rises, hoarding and other panicked activities from other citizens:

- *"It increased because people panicked, and stations are gouging. Supply shortened due to the ransomware attack taking Colonial offline. There is no "shortage," this is the same as people standing in line to buy toilet paper (again). Brent and WTI both priced below $70.".*

And others were perhaps contributing to some aspects of the ensuring mass panic:

- *"If you live in the Southeast or on the East coast...Go Get GAS NOW!! Stations are selling out or limiting gas. #ColonialPipeline".*

Finally, the following social media post is particularly interesting for 7SHIELD's approach and the need to have action plans in place to deal with security incidents:

- *"The @CISAgov and @FBI are ratcheting up warnings and best practices education, especially related to critical public infrastructure assets after an attack on the Colonial pipeline. http://ow.ly/tbe750ELSDc".*

Overall, Colonial drew immediate criticism for their communication approach to the incident with Forbes publishing one article specifically highlighting the 30-hours delay between the incident and the first official communication [72]. Even when the organisation did start to communicate, there was very limited use of social media to get the message out, correct any false information or contribute to the allaying of fears around gas shortages. After days of limited communication some of this activity was then picked up by US government officials to try to calm the fears of ordinary citizens about potential gas shortages and prevent panic buying.

4.4. Case Study 4 – Irish Health Service Attack

4.4.1. Background and timeline

On the 14th May 2021, the Health Service Executive (HSE) – the Republic of Ireland's public health system – experienced an organisation wide cyber-attack with hackers demanding around 20 million euros in ransom. Dubbed the greatest cyber-attack on the Irish state to

date, the attack involved Conti ransomware which resulted in a nationwide shutdown of HSE's public health IT systems [73].

These systems compromised include 2,000 systems (laptops, computers etc.) and 4,500 servers used by HSE [74]. HSE on average, normally treats around 15,000 outpatients per day, but this dropped by around 50% creating an intense backlog of patients seeking treatment [75]. The attack hit national, regional, and local systems in the early hours of the 14th of May which caused HSE to shutdown all online systems, with systems still not operational almost two weeks later – significantly longer than the NHS incident. Their rationale for shutting down the systems were 'precaution' and to 'protect' other health systems from the cyber-attack [76].

Following the shutdown, there was an enormous impact on hospital services and procedures with some areas experiencing an 80% drop in scheduled appointments [74]. These include routine appointments, out-patient appointments, screening and radiology services. Covid testing and vaccine rollout has however not been affected, with the public being urged to walk in to testing and vaccine sites. Alongside this, hospitals had to resort back to using a paper-based system causing extensive delays and severe risk for patients.

Alongside the attack on HSE, on the 13th of May the National Cyber Security Centre was made aware of suspicious cyber activity on the Department of Health's (DoH) network. The next day, the Department of Health (DoH) was the victim of a malicious cyber-attack. However, in this case, the ransomware was detected and prevented from encrypting files and shutting down the DoH's network.

In addition, on the 16th of May, the Irish Department of Social Protection (DoSP) also experienced an attempted cyber breach. The department suspended its communication channels with HSE and they were able to withstand the attack through anti-virus software and the deployment of other tools which have not been named. It has since been assumed that the attacks on HSE, the DoH, and DoSP were part of the same campaign targeting Ireland's health sector. This data includes patients' test results, admission records, staff employment contracts and financial information, patient addresses and mobile numbers. Since the attack, on social media, HSE repeatedly urged staff members to refrain from logging into their online accounts and using company network connected devices. As a result of the stolen data, HSE obtained a high court injunction prohibiting the sharing of this stolen information.

It has since been revealed that private data was stolen during the attack, with the Financial Times identifying 'samples' of private data which was distributed online. The 27 files include personal records of 12 individuals. One file reviewed by the FT includes admission records and laboratory results for a man who was admitted to hospital for palliative care. The broad details in that file matched a subsequent death notice seen by the FT [77]. This was reported as early as the 19th May 2021.

As HSE updated on the 26 May 2021: "*The HSE is seriously concerned about risks to patients arising from the absence of many services in the health services. While progress is being made on the IT front, it will be some time before this translates into a restoration of services in very many cases.*"[30]

Systems did not start to be restored until the 27th May 2021, this was almost two weeks after the incident began with many systems still offline at that point. The HSE was still concerned about bringing such systems online: "*In opening up our system, the firewall is the big question. We have a lot of very nervous people about that because as soon as we open that up anything can get in".[75]*

By the 2nd June progress was being made in some hospitals and health service sites on restoring IT systems. But many health services were continuing to operate essential and urgent services only, without access to critical IT systems or with limited access to these systems. Services around the country are continuing to see significant impacts and disruptions to services with the HSE urging patients to "*check updates on services that are affected on the HSE website service updates page*" [78].

4.4.2. Response

Immediately following the attack, HSE set up a web page which provides updates on the attack, services and appointment arrangements and cancelations [79]. HSE worked with the National Cyber Security Centre (Ireland lead cyber security agency), the Garda (Irish police) National Cyber Crime Bureau, the Army (Irish Defence forces) and international partners such as Europol and Interpol. The NCSC, who led the response, activated its crisis responses measures and provide direct assistance to HSE [80]. Alongside these domestic and international organisation, HSE contracted US-based cybersecurity firms McAfee and FireEye to lessen the impact of the attack and monitor the dark and deep web for stolen data that has been published online.

4.4.3. Ransomware

Wizard Spider, believed to be operating out of Saint Petersburg, Russia, have since been identified as the group responsible for the attack. They have conducted over 300 malicious cyber attacks since 2019 and are responsible for hundreds of attacks around the world [81]. Wizard Spider are an organised crime group, with supposedly around 80 staff members. The FBI, NCA, Interpol, and Europol have been targeting the group for a number of years. Using a type of Conti ransomware named Colbalt Strike – a remote access penetration testing tool – the attackers were able to, once access had been gained, trawl through and infest HSE systems. Cobalt Strike has since been identified in HSE systems, which allowed them to be controlled and for HSE software to be deployed via a remote desktop.

[30] https://www.hse.ie/eng/services/news/media/pressrel/hse-cyber-security-incident.html

4.4.4. Communication on social media

As part of the full organisational investigation into the incident, the HSE released a timeline of the attack from when the servers first became compromised [82]. This timeline clearly shows that although the HSE recognised that there were failings in several areas in the preparation and management of the incident time from discover to communication was relatively swift. The timeline notes that the first systems were encrypted around 1am on the 14th May, by 7:28 the organisation has posted its first tweet[31] about the incident (Figure 4-7) and national news organisations were all starting to be on top of the story for the first news cycle of the day.

Figure 4-7 - First posts from the @HSELive account

By 10am the website had been updated with relevant information and a programme of stakeholder communication including to health service staff was also underway. Even during these first couple of days the team remained active on social media answering queries about the incident as well and the COVID19 vaccine rollout that was interrupted while the systems were under attack. What is positive about the communication is not only the speed at which information was being disseminated but also that the content of the messages includes all relevant information: what has happened, what action has been taken by @HSELive at this point, an apology to citizens/service users and a clear indication of

[31] https://twitter.com/HSELive/status/1393090933361623042

which services are affected currently (vaccinations) while services that are not (ambulance dispatch).

As well as communicating with the public, HSELive also used social media to emphasise the message sent to their staff to implement safety measure or mitigation actions to prevent further spread of the ransomware to additional computer hardware.

"Reminder to HSE staff: do not turn on your work PC or Laptop. If you have your PC or Laptop turned on, please power it off."

As the incident continued for several days the communication strategy also evolved to inform different services (from radiography to recruitment) as well as managing to maintain the vaccination programme. Compared to the Colonial Pipeline strategy, as discussed in the previous section, it is important to see in this case that the organisation owned the crisis from the start and was relatively proactive in their communication of the current status of the incident and not relying on other government organisations to manage the communication approach.

4.5. Gatwick airport drone sightings

In December 2018, Gatwick Airport serving London, UK had its runways shut down due to a report from a security guard that a drone had been spotted flying near the runway. Being close to the Christmas holiday period this caused significant flight disruption and standing many thousands of passengers. Over the next day several other sightings were also reported again leading to further cancellations and runway shutdowns. The police and the Ministry of Defence as well as the airport's own security team were all involved in the response. To this day, no one has ever been identified as the drone pilot and there is some scepticism that the drones existed at all [83].

Due to the unusualness of the incident, several agencies and organisations have already looked into the communication strategies employed in this situation. Crisis Shield [84] has a particularly good review of the approach the organisation took, noting that the airport quickly published a tweet explaining the suspension of as well as setting out which other organisations they were working with in order to manage the incident. Crisis Shield credit the airport with following best practice guidance to ensure that the airport is 'leading the narrative' and getting ahead of the media. They highlight the need to state facts, as well as demonstrate sympathy and empathy to those that are impacted. The airport also took the step of apologising directly for the disruption from the outside[32] (Figure 4-8). Perhaps surprisingly the number of interactions with the content is not that high, this could also be related to the time of day the information was posted.

[32] https://twitter.com/Gatwick_Airport/status/1075522187946221569

Figure 4-8 - Gatwick airport - first tweet about the disruption

The airport continued to post information about the impact of the sightings on the airport operations throughout the day including advice for passengers as well as empathising with their situation (Figure 4-9) [84].

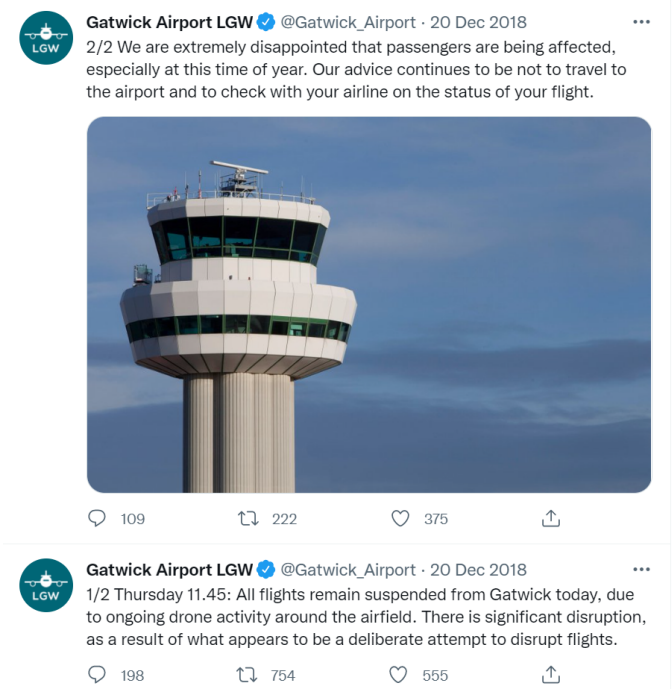


Figure 4-9 – Gatwick Airport – explanatory and empathising posts

The Gatwick drone sightings was a particularly interesting case because although the operator was on top of their crisis communications from the outset supporting their customers and directing them to further information the confusion about whether the drones actually existing, policing failings in arresting an innocent couple and subsequent statements [83] casting doubt on the existence of the drones at all highlighted another key

element of crisis communications – that all organisations need to be communicating a consistent message.

4.6. British Airways – cyber-attack and subsequent data breach

*4.6.1. Introduction – **Ground Zero***

British Airways (BA) the UK flag carrier airline formed in 1974 and is now a part of the holding company the *International Airlines Group*.[33] The IAG is an Anglo-Spanish business with an office in Madrid and British Airways in the United Kingdom. British Airways falls under the remit of the United Kingdom's Information Commissioner's Office (ICO) founded in 1984 which was introduced into the United Kingdom to provide safety for data and digital rights of consumers in all contexts which involve the processing or handling of Personal Data as an ombudsman [87]. At the time of the incident the UK was still subject to GDPR which holds specific requirements for organisations to adhere to when processing and handling Personal Data, in the case of BA personal data constitutes passport information, boarding information, credit and debit card details, disabilities etc. The issue, however, stems from the events that occurred after a malicious actor (the attacker) successfully gained access to personal data of BA customers and travellers. These events that took place resulted in the largest fine being handed out under *Section 155 of the Data Protection Act* by the ICO to British Airways of £20,000,000 due to a preventable data leak that occurred.[34]

4.6.2. Data Breach & Failures – What happened and who was at fault?

From 21st August 2018 to the 5th September a malicious actor gained access to the British Airways domain (www.britishairways.com) where the attacker successfully altered the JavaScript file on the British Airways website which altered the domain to www.BAways.com. This domain did not take the user, to the British Airways website but to an external site where the attacker successfully extracted cardholder data from users by posing as a fake purchasing system. The access to these JavaScript by the attacker was done via credentials that were compromised to the '*Citrix Remote Access Gateway*.[35]" British Airways were found to have negligently caused a data leak of personal data due to poor management of security. Due to their omissive behaviour it resulted in an estimated 429,612 people worldwide (UK, EU, and the rest of the world).[36] This figure included customers and staff members, their names, address, payment, and card numbers (CCV) of 244,000 was also given access to a malicious group. There were instances also of high-level security breaches when usernames and passwords of employees and administrators of BA account holders were also leaked – including 612 executive club members.[37] This highlights

[33] International Airlines Group (2022) 'Our Brands' retrieved from https://www.iairgroup.com/en/our-brands
[34] Information Commissioner's Office (2020) Penalty Notice *COM0783542 7.53*
[35] Information Commissioner's Office (2020) Penalty Notice *COM078354 1.2*
[36] Information Commissioner's Office (2020) Penalty Notice *COM0783542* 4.1
[37] ibid

the severity of the breach due the scale of what was leaked plus the new areas of possible vulnerabilities; especially when the Data Breach was only identified in September after the first attack occurred on the 22nd of June 2018 [88].

After the event the requirement to find what the responsible factors for the Data Breach's occurrence was a priority by the ICO. It was highlighted that there were 'numerous measures BA could have used to mitigate or prevent the risk of an attacker.'[88] Section 6 of the *Penalty Notice* provided to British Airways in October 2020 detailed the breaches of British Airways which either caused or exacerbated the possibility of a data breach incident. Section 6 recommends that BA should have placed their system through more 'rigorous testing' such as a 'penetration test.'[38] The ICO also highlighted that BA violated the *National Institute for Standards and Technology* guidance when referring to 'Multi Factor Authentication' (MFA). These standards founded a rule that 'you should use MFA *whenever possible*, especially when it comes to your most sensitive data' [89] this was failing area which was found not to be practiced as highlighted in 6.16 of the Penalty Notice that was submitted to BA. [39]

The breach that entailed once discovered required that the appropriate communications took place to ensure that information was provided to the public and the ICO so the breached data subjects could be informed accordingly. The following section will detail how British Airways responded to the breach, including the impact of social media and news tabloids and their opinion regarding the loss of data from British Airways.

Figure 4-10 - First communications from British Airways

4.6.3. Communication Strategy – How did BA inform the public of the data breach and what was the media response?

The communications that took place between British Airways and the Information Commissioner's Office took place on the 7th of September 2018 and reported that 496,636 customers were affected due to the data breach of information. The first communication

[38] Information Commissioner's Office (2020) Penalty Notice COM0783542 6.56
[39] Information Commissioner's Office (2020) Penalty Notice COM0783542 6.16

that took place between British Airways and the consumers was a public notification on their Twitter account explaining that there was a 'Theft of Customer Data' as highlighted in Figure 4-10. The initial discovery on the 5th September at 21.45 BST 2018 was then revealed to the public on 6th September 2018. This was a prompt investigation from British Airways which was launched to find the causative factors into what caused the breach. It was detailed that by the 2nd day of the Breach, all affected customers were contacted by British Airways regarding the loss of any of their Personal Data to the attackers.

The weblink takes users to a British Airways page with further information that addresses most of the elements required for a crisis communications message (Figure 4-11)

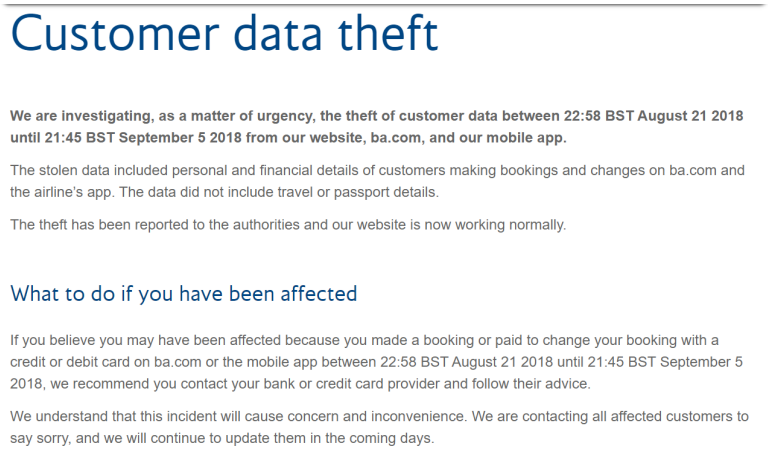


Figure 4-11 – Information posted to the British Airways website

After the announcement online of the Data Breach, chairman Álex Cruz faced the headlines and newspapers that were attacking the credibility of his business. In a statement made on the 7th September on BBC Breakfast he stated that '[We are] Deeply sorry, we know that the information that has been stolen is name, address, email address, credit card information [92].' Cruz also informed the public via BBC Breakfast that they would compensate the losses of all customers so that they could 'feel close to them again' post the breach of personal data.

The communication strategy that British Airways accepted accountability for their poor cybersecurity standards due to penetrative measures are not tested or any form of MFA or 2FA in their systems. British Airways continued to support affected members of the breach by providing an 'undisclosed' sum for compensation regarding their losses. The communicative responses from British Airways were effective in resolving the outcomes of a 'sophisticated data breach' [92] as stated by Alex Cruz. The outcomes, however, of the open communication of this event has led to high-level discussions and requirements for securities in business and the requirements to ensure that all personal data is protected by a strong unbreachable wall in the digital environment

4.7. Key Findings

- Always get ahead of the event that is happening, breaking the news first allows the operator to be in control of the narrative
- Internal communication and coordination are important, but don't neglect external communications
- Demonstrate compliance with all regulatory functions and commit to making amends
- Use citizen-to-citizen and citizen-to-authority communication to your advantage to identify gaps and challenges, address misinformation as soon as possible in your response
- Don't wait to convey the urgency of the message in critical situations
- Web pages can be used to provide extended information, but ensure that important information is directly addressed at source (e.g., in the social media post)

5. Warning Message Generation for 7SHIELD

The previous three sections have discussed how warning messages have been utilized for crisis communications and for public communication in both the crisis and disaster resilience sector as well as the critical infrastructure sector. Much of this research noted that the use of templated messaging can help to support the crisis and incident management functions. We have also considered how the current end users within 7SHIELD employ social media to communicate generally and specifically about incidents or service updates. Several case studies focused on different aspects of the critical infrastructure have been assessed and analysed to inform approaches to the warning message generation framework set out in the following sections. These results have been combined with contextual knowledge from the project and existing standards and approaches to develop a warning message generation framework that can be applied in 7SHIELD for the purpose of informing citizens, customers, service users and other relevant stakeholders about critical incidents related to the ground segment or other infrastructure.

5.1. Warning Message Framework

The core of the warning message generation framework (WMG) comes from the underlying CAP model, the aforementioned gold-standard for public alerting and warning as well as the best practices from research. As mentioned above, in Section 2.3.5, CAP messages are comprised of four main components – the alert segment, information segment, resource component and the area component. In the context of 7SHIELD the location aspect will only be relevant in some forms of alert depending on the type of information to be disseminated.

CAP is a widely used standard that has increasing adoption for both the generation of system communication of warning messages and information as well as providing basis for the construction of templated messages. Based on the analysis of CAP above in combination with the previous analysis the following information could be included in a standard warning message (summarised in Table 5-1) with one additional element – the current actions of the organisation as this was stressed as being important multiple times during the research and demonstrates that the organisation is committed to solving or addressing the current incident.

CAP Level One	CAP Level Two	Sutton et al. Effective Warning Content	ISO 22322: 2015	Gold Standard Framework Element
Alert	Message Type		Alert type	
Information	Event Category	Hazard	Hazard/Threat type	Crisis Type
	Severity			Crisis Severity
	Effective Date / Time	Time	When	Timeframe
	Onset Date / Time		When	Timeframe
	Event Description	Consequences	What to expect	Impacts
	Audience		Reciever	

	ResponseType & Instructions	Guidance	Actions (who, why, what, when)	Reccomended actions
	Expiration Date / Time			
	SenderName	Source	Issuer	
	Contact Info			Contact Details
	Information URL		Further Info	Further Info
Resource	Description / URI			Magnet Media
Location	Area Description	Location	Location	Location

Table 5-1 - Mapping between key CAP elements and other messaging standards

5.1.1. Standard categories for 7SHIELD CAP components

Having defined they key components that will make up the warning message generation framework, the next step is to consider two core elements that will make up the standardised content of the messages in order to support both the rapid construction of the messages themselves and the ability to translate content between languages to ensure that information can be rapidly disseminated in the local language of the facility where the incident occurs. For each component we discuss the core relevant terms for each constituent CAP element used the framework.

The first element is the **Alert: Message Type.** This provides the overall type of notification to be included within the system. Such message types can also be linked to the crisis phase, whereby some messages are more suited to before or during the initial onset phase of the crisis whereas others are suited to providing updates or indicating that the crisis or incident is over and the next phase of management of the incident can be started. For 7SHIELD, we consider the following six types of alerts that could be raised within the WMG framework from most to least serious type of alert. The following alert types are based on previous alert types suggested from the US National Weather Service (NOAA) [93] and Neußner [34]:

- **Alert**: to be used when an event is already occurring, imminent or very likely to occur and there is a need to take some form of immediate action;
- **Warning**: to be used when an event is already occurring, imminent or very likely to occur;
- **Advisory**: to be used when an event is occurring, imminent or very likely to occur but is less serious than a *warning* alert type;
- **Caution**: to be used when an event may happen and there is a need to potentially take defensive or preparedness action;
- **Update**: to provide an update on previous information ;
- **All Clear**: to signify that the event or incident has passed and that normal operations can resume;

- **Informational**: is not related to a specific incident but where a service update may need to be provided and can be achieved through the same approach as the overall WMG framework.

The second information type indicated the **Information: Severity** component of the system. In CAP, severity is defined as the 'intensity of the impact'. In this component we stick to the traditional and worldwide standard of a traffic light style nomenclature (red, yellow, green). Whilst CAP proposes the use of extreme, severe, moderate, minor and a fifth state of unknown, the use of these colour coded alerts comes from the ISO standard (ISO 22324:2015) and further division of severity many cause more confusion and misunderstanding – e.g., is yellow or amber more severe? The difference between the alert type (described above) and the severity score is that the alerts consider only how likely or not an event is about to occur whilst the severity score indicates the potential harmfulness of such an event.

- **Red** – to be associated with danger and used to notify people to take action immediately
- **Yellow** – to be associated with caution and used to notify people of an 'at risk' situation and that they should be prepared to take action
- **Green** – to be associated with safety and that no action is required.

The use of only the three elements keeps the severity score simple and also aligns better with the natural language required in the message generation approach. Furthermore, correspondence with the traffic light approach is a relatively universal standard (as evidenced by its inclusion in the ISO standard) and thus should be readily understood across languages and cultures.

The definition of the **Information: Category** element is inspired by the pilot use cases and also the common threats identified as being as a risk to the space sector as well as common cyber related incidents that could impact up on a service. For example, several reports have been complied about potential attack or threats to space based systems, national critical infrastructure sites [8][94]:

- **Unauthorised entry to grounds** – a person evades security checks to enter the perimeter of the site;
- **Trespasser on site (single person)** – a single person enters the site (can be malicious or careless);
- **Trespasser on site (multiple people**) – multiple people enter the ground segment site (e.g., for a protest or with an intention to cause disruption);
- **Unauthorised UAV** – an unmanned aerial vehicle is sighted in the vicinity of the ground segment;
- **Unauthorised entry to building** – a person gains unauthorised access to a building;

- **Unauthorised system access (remote)** – a person has gained unauthorised access to the computer systems
- **System unavailability** - the system is unavailable for an unspecified reason;
- **Cyber-attack** – the systems are under an unspecified cyber attack;
- **DDoS attack** – services are unavailable due to a denial of service attack;
- **Jamming attack** – services are unavailable due to a jamming incident;
- **Ransomware** - data has been rendered inaccessible due to a ransomware attack;
- **Data breach** – a breach of data within the system (non-personal);
- **Personal data breach** – the personal data within the system has been identified;
- **Natural disaster** – a natural disaster has affected services;
- **Severe weather** – a severe weather incident has disrupted services / makes the site inaccessible;
- **Flood** – a flood has disrupted services / makes the site inaccessible;
- **Earthquake** – an earthquake has disrupted services / requires an evacuation;
- **Wildfire** – a wildfire has spread close to the facility;
- **Terrorist attack** – a terrorist attack has taken place;
- **Serious incident** – a generic serious incident is underway;
- **Datacentre malfunction** – the datacentre is offline or has suffered damage in some form;
- **Service offline** – the service is offline for an unspecified reason;
- **Threat detected** – a generic threat has been detected;
- **Custom/Free text.**

The aim of the WMG is to be as extensible as possible and therefore the above categories should be able to be extended as required to suit the need of an evolving threat landscape.

The **Information: Event Description** category provides a space for the organisation to add any further relevant information that is important for them to communicate directly with the public, service users, customers or employees as necessary. This should be an optional component as it will not be possible to translate directly unless the organisation is able to provide the translation themselves.

Including who the warning message is targeted at is particularly important when operating in a space where different incidents will require different groups of personnel to be made aware of the incident, response and required actions. Therefore, the **Information: Audience** segment consist of the following core target groups:

- Citizens;
- Visitors;
- Employees;
- Users;
- Custom/Free text;

While it is not possible to consider every possible action that could be take in response to an incident the **Information: Instructions** segment captures the high-level actions that may need to be taken by receivers of the information. These are divided into three main categories: physical actions that a person may need to undertake for their own personal safety, communication actions and information technology related actions that are needed to protect systems in the event of a cyber incident:

- go to [location];
- avoid [location];
- evacuate immediately;
- shelter in place;
- return to building;
- continue as normal;
- alert physical security team;
- alert cyber security team;
- log out of all systems;
- shut down your personal computer or laptop;
- change password;
- log into system;
- wait for updates;
- avoid making system requests;
- enable MFA;
- contact [organisation];
- Custom/Free text.

Similarly, these are infinite numbers of potential actions an organisation may need to take to respond to an incident. Therefore, the **Information: Response Type** pre-set fields cover certain scenarios however, as with all fields there is scope to include additional actions. Furthermore, the framework is designed to be as extensible as possible therefore additional

actions or responses should be easily added to the pre-set fields in the case of organisational needs:

- Investigating the cause;
- Resetting services;
- Updating service;
- Recovering data from backups;
- Coming back online;
- Informing perimeter security team;
- Informing incident response team;
- Searching for the perpetrators;
- Sending help;
- Referred to [police/civil protection/etc.];

Furthermore, not considered within the scope of the immediate warning message generation is the impact and/or cascading effects of such a problem with a space facility that may have downstream effects on other services. For example, the comprehensive report on the cascading effects of a GNSS failure cites potential impacts upon several other sectors including healthcare, air, maritime and ground transportation, energy and other utilities, other emergency management operations, and financial services [95]. The impacts on these services are summarised as including disruption of emergency services, supply chain logistics including food shortages, stranding of people overseas or in remote places due to lack of available transport and other effects. These impacts would then need to be communicated by the operators of such services.

Other information segments include the followings that are generally language agnostic in the first place such as the description of time-based information (**Information: Active Date/time, Information: Expiration Date / Time)** and further information sources either through **Information: Contact Info or Information: Information URL.**

5.1.2. Generic warning message structure

Based on the above discussion and inspired by CAP and other template warning message approaches we have created a master message structure that incorporates all possible message components that can be used to construct various warning messages in the event of different types of incidents. The finalised list of elements is the following:

- Basic message:
  - Severity – colour coded levels (mandatory);
  - (Warning) type (mandatory);

- Category – simple description of the crisis (mandatory);
- Start time/date (mandatory);
- Until time / date (optional);
- Location (optional).

- Extended message:
  - Event description (optional);
  - Audience (mandatory);
  - Instructions – actions to be taken by the audience (mandatory);
  - Organisation – Organisation that the information is being communicated from (optional);
  - Response – actions the organisation is taking to resolve the situation (optional);
  - Update date/time – when the next update can be expected (optional).
- All messages:
  - Contact information (optional);
  - URL – weblink for more information (optional);
  - Additional media – associated images / video as necessary (optional).

Based on the above categories we have developed a basic and extended warning message structure that can be used to form the basis of crisis messages and warning of incidents. The basic and extended messages are there to align with the potential availability of information and the limitations on the number of characters that can be included in a message on some platforms (e.g., Twitter).

Therefore, a generic warning message structure would look like the following:

[severity] [type] for [category] active from [time/date] {until [time/date]} {at [location]}. {[event description]}. [audience] should [instructions]. {[organisation] is [response].} {Update is expected at [date/time]}. Visit [url] for more information {or contact us using [contact info]} [additional media]

In this case the green represents mandatory inputs and blue optional inputs whilst the underlined sentence is a simple warning message while other content can be included/excluded depending on the situation. This could then be realised into the following examples:

System disruption – unknown cause

- ***Simple message:*** *Red warning for system unavailability active from 10/06/2021 14:49:00 until 11/06/2021 at Sheffield. Visit www.example.com for more information.*

- ***Extended message (without event description):*** *Red warning for system unavailability active from 10/06/2021 14:49:00 until 11/06/2021 at Sheffield. Users should log out of all systems. CENTRIC is updating services. Update is expected at 16:00. Visit www.example.com or contact @organisation*
- ***Extended message (with event description):*** *Red Warning for system unavailability active from 10/06/2021 14:49:00 until 11/06/2021 at Sheffield. Communication systems are down and log on servers are unavailable. Users should log out of all systems. CENTRIC is Updating services. Update is expected at 16:00. Visit www.example.com for more information or contact @organisation*

Weather-related disruption

- **Simple message**: *Yellow caution for severe weather active from 30/05/2022 14:00:00 until 06/06/2022 16:00:00 in Northern England. Visit www.example.com for more information.*
- ***Extended message:*** *Yellow caution for severe weather active from 30/05/2022 14:00:00 until 06/06/2022 16:00:00 in Northern England. Risk of severe flooding and road closures Citizens should evacuate immediately. Operator is sending help. Updated is expected 01/06/2022. Visit www.example.com for more information.*

Cyber Incident

- ***Simple message****: Red advisory for threat detected active from 30/05/2022 14:00:00 until 06/06/2022 16:00:00 in system network. Visit www.example.com for more information.*
- ***Extended message****: Red advisory for threat detected active from 30/05/2022 14:00:00 until 06/06/2022 16:00:00 in system network. Unusual activity detected in logs Employees should avoid making system requests. Operator is updating services. Updated is expected 01/06/2022. Visit www.example.com for more information.*

Due to the approach of standardising as many elements as possible, this allows for the integration of a multi-lingual and language agnostic approach to the warning message framework where translations of the different segments can be pre-prepared and the user can easily navigate between the different translations of the same message. The approach is full extensible and for example we can recreate the above system disruption message (extended message without event details) in a relatively straightforward manner.

Spanish

Roja advertencia por indisponibilidad del sistema activo desde 10/06/2021 14:049:00 hasta 11/06/2021 in Sheffield. Los usuarios deben desconectarse de todos los sistemas. CENTRIC està servicios de actualización. Se espera una actualización en 16:00. Visitar www.example.com para más información o contáctenos usando info@email.com.

French

Rouge avertissement for indisponibilité du système actif à partir de 10/06/2021 14:049:00 jusqu'à 16:00:00 à Sheffield. Utilisateurs devoir se déconnecter de tous les systèmes. CENTRIC is mise à jour des services. La mise à jour est attendue 16:00:00. Visite www.example.com pour plus d'informations. ou contactez-nous en utilisant @organisation.

Italian

Rosso avvertimento for indisponibilità del sistema attivo da 10/06/2021 14:49:00 fino a 16:00:00 di Sheffield. Gli utenti dovere disconnettersi da tutti i sistemi. CENTRIC is aggiornamento dei servizi. L'aggiornamento è previsto 17:00. Visita www.example.com per maggiori informazioni. oppure contattaci utilizzando @organisation.

The above translations are indicative and further translations will be developed also for the Finnish and Greek models. It should be noted that the translation between the models is not expected to provide word perfect sentences but to allow organisations to rapidly contact and reach more people in the event of a crisis than would be possible by using a single language model. As will be explained in the next section, there will be further possibilities to customise the pre-set fields as required in the full warning message generation system. Existing translations are also provided for Spanish, Italian and French in Annex 1.

5.2. Towards the 7SHIELD warning message generation system

The 7SHIELD warning message generation (WMG) system would be based on the above examples and construction of templated messages in multiple languages utilising many of the standardised fields defined in CAP. The WMG system would aim to transform inputs from the user into a standardised warning message that can be distributed through several media channels such as Twitter, Facebook, SMS, and other short form messaging systems.

Previous research into warning message generation approaches have been investigated by Doerman et al. [96] in the context of short form message generation for the transmission of information about wildfires. Doerman et al. designed a short form questionnaire to enable to rapid construction of standardised messages whilst also including useful features such as a character count. The generator is designed as a series of prompts which steer the user towards creating an effecting warning message. An example of the questionnaire and the subsequent warning message generated is shown in Figure 5-1 and Figure 5-2.

	Message:	Ventura County Sheriff's Office: WILDFIRE EMERGENCY located between Santa Paula, Ventura, Ojai moving toward Santa Barbara County. Wildfires can burn down homes/other structures, block roads/evacuation routes. If you are located in the southern coast of Ventura County EVACUATE NOW. Do not delay to pack belongings. Check readyventuracounty.org for updates.	
	Characters Left:	3	
Guidance	Prompt 13	What is the main purpose of this message?	
		Select the main purpose of this message:	Evacuation
Source	Prompt 1	What agency should be listed as the source of this message?	
		Enter the agency sending this message:	Ventura County Sheriff's Office
Source	Prompt 2	Does this agency use an acronym that is more common than its official title?	
		Select Yes or No:	No
Source	Prompt 3	Prompt not applicable. Continue to next prompt.	
Hazard	Prompt 4	What type of emergency is happening or about to happen?	
		Select the type of emergency:	Wildfire Emergency
Hazard	Prompt 5	What wildfire consequences should the public be aware of? "Wildfires can..."	
		Select consequence #1: *(you MUST select at least one consequence)*	burn down homes/other structures
		Select consequence #2: *(select 'none' if no other consequences should be included)*	block roads/evacuation routes
			35
Location	Prompt 6	Which will be used to identify the current location of the hazard?	
		Select which will be used to identify the location of the hazard:	town/city/county (all or portion)
Location	Prompt 7	The hazard is located between which town/city/county (all or portion)?	
		Select the proximity of the hazard to the town/city/county (all or portion):	between
		Enter the town/city/county (all or portion) the hazard is located between: (separate multiple with 'and' or ',')	Santa Paula, Ventura, Ojai
Location	Prompt 8	Which will be used to identify the direction the fire is spreading?	
		Select which will be used to identify the direction the fire is spreading:	town/city/county (all or portion)
Location	Prompt 9	What is the name of the town/city/county (all or portion) that the fire is moving towards?	
		Enter the town/city/county (all or portion) that the fire is moving towards:	Santa Barbara County
Location	Prompt 10	Is there a specific region of people who should evacuate?	
		Select Yes or No:	Yes
Location	Prompt 11	People located in which region(s) should evacuate?	
		Select the proximity of the evacuation area to the region:	in
		Enter the region(s) of people who should evacuate: (separate with ',' if more than 1)	the southern coast of Ventura County
Timeline	Prompt 12	When should people take action?	
		Select when people should take action:	now
			-
			-
Guidance	Prompt 14	What specific actions should the person receiving this message take?	
		Select action #1: *(You MUST select at least one action)*	Do not delay to pack belongings.
		Select action #2: *(select 'none' if no other actions should be included)*	none
			35
Guidance	Prompt 15	What should people do for update information?	
		Select action: *(select 'none' if no update information should be included)*	Check {website} for updates.
		Fill-in Website Address:	readyventuracounty.org

Figure 5-1 - Doermann et al. - wildfire message generation questionnaire

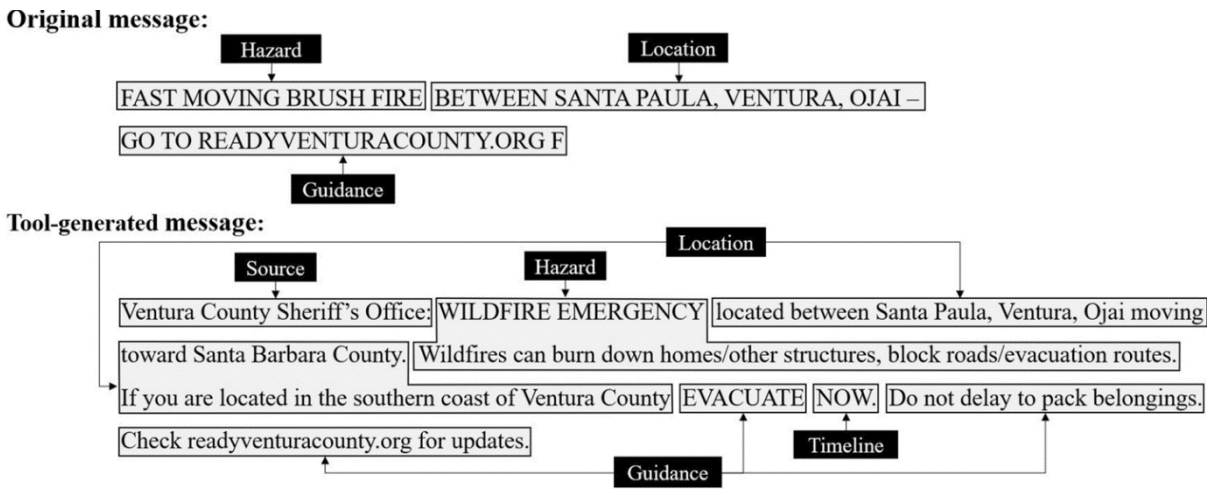


Figure 5-2: Doermann et al. - example of a generated message

The warning message generation framework itself has three core components that underpin the development of the standard warning message itself. This involves selecting the:

- Message type: basic or extended;
- Language selection;
- Automated message construction.

In 7SHIELD our primary focus is on the development of warning messages that should be transmitted in the crisis phase, while some messages may be suited for the pre or post crisis phase our main concern is the communications that need to go out in the heat of a crisis. Within this, depending on the country and the type of event, different organisations have different responsibilities in terms of about which events they should communicate when they these are the core responsibility of another organisation. Therefore, some options may be more relevant than others especially as 7SHIELD has a relatively broad range of potential incidents to cover. Table 5-2 below demonstrates the pre-set fields for each element of the warning message.

Segment	Standard Elements	
Severity	• Red • Yellow • Green	
Type	• alert • warning • advisory • caution	• update • all clear • information • [custom text field]
Category	• unauthorised entry • trespasser on site (single person) • trespasser on site (multiple people) • unauthorised UAV • unauthorised entry to building • unauthorised system access (remote) • system unavailability • cyber attack • DDoS attack • jamming attack • ransomware	• data breach • personal data breach • natural disaster • severe weather • earthquake • wildfire • terrorist attack • serious incident • datacentre malfunction • service offline • threat detected • [custom text field]
Effective date/time	active from • [free text] - date / time / time decriptor (e.g., today, tomorrow, etc.)	

End data / time	until • [free text] - date / time / time decriptor (e.g., today, tomorrow, etc.)	
Location	in • [custom text field]	
Event Description	• [custom text field]	
Audience	• Citizens • Visitors • Employees • Users	
Instructions	should • go to [location] • avoid [location] • evacuate immediately • shelter in place • return to building • continue as normal • alert physical security team • alert cyber security team • log out of all systems	• shut down your personal computer or laptop • change password • log into system • wait for updates • avoid making system requests • enable MFA • contact [organisation] • [custom text field]
Organisation	• [custom text field]	
Response Type	is • investigating the cause • resetting services • updating services • recovering data from backups • coming back online • informing perimeter security team	• informing incident response team • searching for the perpertrators • sending help • referred to [police/civil protection / etc.] • [custom text field]
Update data / time	Update is expected • [free text] - date / time / time decriptor (e.g., today, tomorrow, etc.)	
URL	Visit • [url] For more information	
Contact Info	or contact us using • [custom contact details – phone number, email, etc.]	

Table 5-2 - Overview of all templated message content

The flow of generating a warning message is envisioned as follows (Figure 5-3).

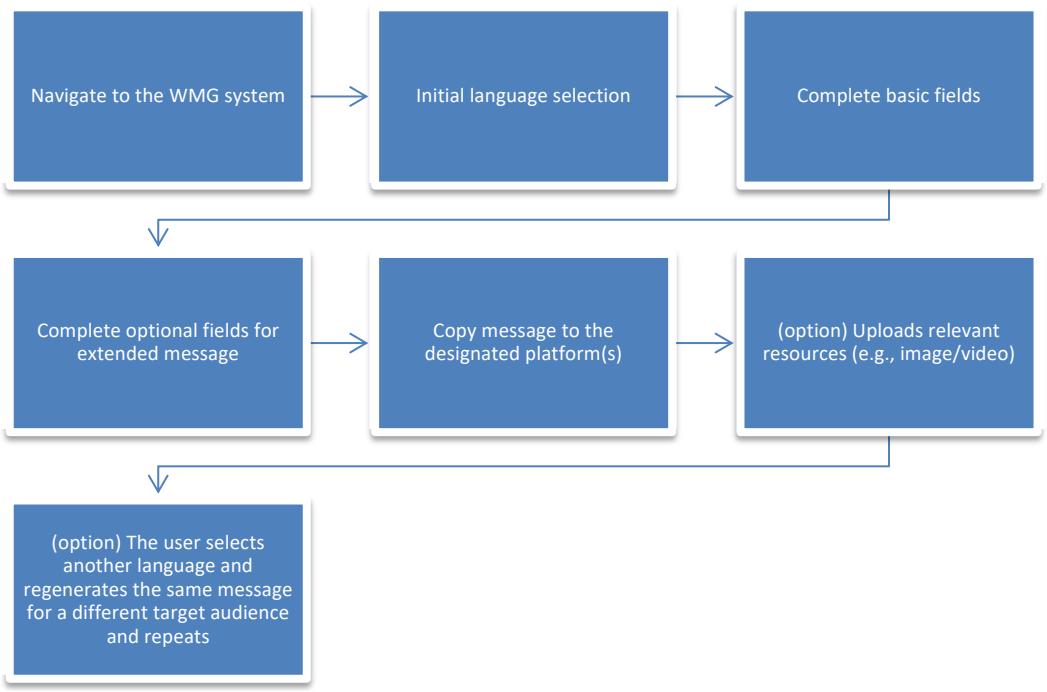


Figure 5-3 - Envisioned warning message generation process

A further mock up how the message generation system will work is demonstrated in the section below. The user should be able to simply input the fields they require into the system and the message will be automatically generated for them to transfer into the relevant service (Figure 5-4).

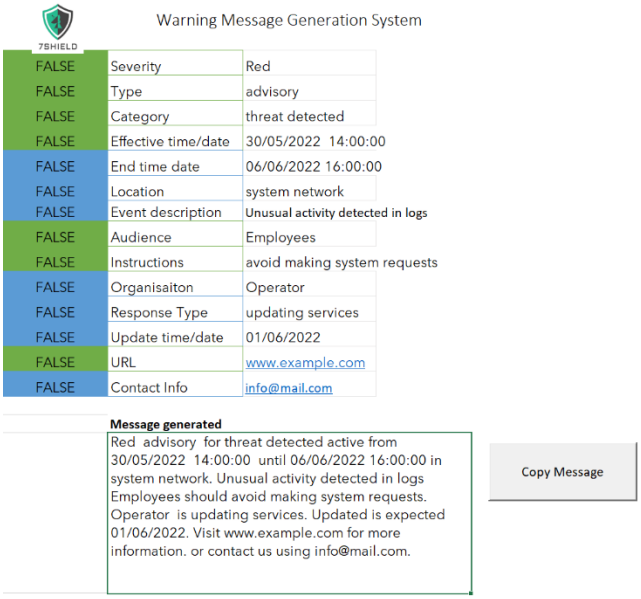


Figure 5-4 - Mock up of message generation interface

The message interface will be available in the languages of the pilot organisations (as well as English) – Spanish, Italian, Greek, Finnish and French. The integrated version will be in the form of a simple web application that will allow users to quickly generate and export messages.

6. Conclusions and next steps

During a crisis, major incident, service disruption or event, it is vital to communicate with stakeholders – whether that is citizens, visitors, customers, service users, employees or other relevant persons. Ensuring that they have access to valuable information and that this is delivered in clear, concise and consistent formats with a degree of regularity can significantly help in mitigating or recovering from the effects of a crisis or incident.

Within 7SHIELD the need for public warning and communication is oriented towards enabling those using the services of the space station or (for whatever reason) find themselves in (or expecting to be) in the vicinity of the ground segment when an incident takes place and there is a threat to their safety or security.

Many organisations have been able to harness social media to effectively deliver public warning information and content while significant research has gone into identifying what content should be contained in such messages to disseminate as much information as possible about the incident, expected response and actions.

In this deliverable, we have investigated best practices for the communication of warning messages and how successfully these strategies are actually implemented during an actual crisis situation or incident. Even when organisations deal with a crisis in an effective manner, they can still find themselves in a toxic or viral environment and therefore this makes the need to communicate well all the more imperative. Crisis communications do not have to be limited to uni-directional communications (authorities to citizens) and organisations themselves can also benefit from the information received from citizens in the other direction – both through direct replies/messages but also through incidental mentions that can inform their social media strategy and response and ensure that their crisis communications are effectively addressing the public conversation.

Upon analysing the existing social media content and messages from the 7SHIELD end users it is clear there is a leaning towards uni-directional conversations. While in some cases, the use for the operators' services is oriented towards a relatively niche community, especially compared to other types of CI operators disruptions to any services that may result in cascading effects to other services and areas increases the chances of getting caught up in an incident that also requires reputation management as well as resolving the original incident.

Finally, existing research also recognised the potential benefits of templating or prepare message in advance of a crisis or incident so they can be rapidly deployed (and without needing to wait for communications' team's sign off). While templating messages can speed up and introduce consistency within messages, operators still have to be careful to ensure that their content remains authentic and that they can deviate from the script where the evolution of the crisis calls for it.

The development of the warning message framework will provide 7SHIELD end users the opportunity to benefit from content that can be rapidly generated whilst providing all the information needed to communicate across a range of crisis and to a range of audiences. The support for multiple languages can easily be extended with the translation of the pre-set message templates and moving between the same message in multiple languages should be relatively straightforward for the user.

Finally, while template messages can be extremely beneficial it is also important to recognise that they do not have to be the only messages in the crisis communications army – other content can support and supplement this approach especially for facilitating a greater level of bi-directional engagement with target audiences and affected communities.

.

7. References

[1] Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

[2] Proposal for a Directive of the European Parliament and of the Council on the resilience of critical entities. COM/2020/829 final

[3] European Commission (2020) The Commission proposes a new directive to enhance the resilience of critical entities providing essential services in the EU. Migration and Home Affairs. 16 December 2020. Available at: https://ec.europa.eu/home-affairs/news/commission-proposes-new-directive-enhance-resilience-critical-entities-providing-essential-services-2020-12-16_en

[4] Communication from the Commission on a European Programme for Critical Infrastructure Protection /* COM/2006/0786 final */

[5] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code

[6] Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2017). European expectations of disaster information provided by critical infrastructure operators: Lessons from Portugal, France, Norway and Sweden. International Journal of Information Systems for Crisis Response and Management (IJISCRAM), 9(4), 23-48.

[7] Manulis, M., Bridges, C. P., Harrison, R., Sekar, V., & Davis, A. (2021). Cyber security in new space. International Journal of Information Security, 20(3), 287-311.

[8] Graczyk, R., Esteves-Verissimo, P., & Voelp, M. (2021). Sanctuary lost: a cyber-physical warfare in space. arXiv preprint arXiv:2110.05878. Available at: https://arxiv.org/abs/2110.05878

[9] Hermann, C. F., (1963) Some Consequences of Crisis which Limit the Viability of Organization, Administrative Science Quarterly 8, 61–82.

[10] Olsson, E.-K. (2014). Dimensions of Crisis Communication Revisited. Journal of Contingencies & Crisis Management, 22: 113-125.

[11] Seo, Y., Ravazzani, S., Jun, H., Jin, Y., Butera, A., Mazzei, A., & Reber, B. H. (2021). Unintended Effects of Risk Communication: Impacts of Message Fatigue, Risk Tolerance, and Trust in Public Health Information on Psychological Reactance. Journal of International Crisis and Risk Communication Research, 4(3), 4.

[12] 't Hart, P.—, and A. Boin. 2001. "Between Crisis and Normalcy: The Long Shadow of Post-Crisis Politics." In Managing Crises: Threats, Dilemmas, Opportunities, eds. U. Rosenthal, A. Boin, and L. C. Comfort. Springfield, IL: Charles C. Thomas.

[13] Reuter, C. Hughes, A.L. & Kaufhold, M-A. (2018) Social Media in Crisis Management: An Evaluation and Analysis of Crisis Informatics Research, International Journal of Human–Computer Interaction, 34:4, 280-294

[14] Coombs, W. T. (2019). Ongoing crisis communication: Planning, managing, and responding. Sage Publications.

[15] Reynolds, B., & W. Seeger, M. (2005). Crisis and emergency risk communication as an integrative model. Journal of health communication, 10(1), 43-55.

[16] Sutton, J., Hansard, B., and Hewett, P. (2011) Changing Channels: Communicating Tsunami Warning Information in Hawaii. Proceedings of the 3rd International Joint Topical Meeting on Emergency Preparedness and Response, Robotics, and Remote Systems, Knoxville, Tennessee, USA, 7-10 August.

[17] CERC (2018) Message and Audiences – 2018 update. Crisis and Emergency Risk Communication Available at: https://emergency.cdc.gov/cerc/ppt/CERC_Messages_and_Audiences.pdf

[18] Serafinelli, E., Reilly, P., Stevenson, R., Petersen, L., Fallou, L., & Carreira, E. (2017). A communication strategy to build critical infrastructure resilience. In Improver Project Deliverable 4.2 (pp. 1-72).
[19] Eriksson, M. (2018). Lessons for crisis communication on social media: A systematic review of what research tells the practice. International Journal of Strategic Communication, 12(5), 526-551.
[20] ISO 22322:2015 Societal security — Emergency management — Guidelines for public warning. International Organization for Standardization
[21] FEMA (2020) National Preparedness: Mission Areas and Core Capabilities. Federal Emergency Management Agency. Available at: https://www.fema.gov/emergency-managers/national-preparedness/mission-core-capabilities
[22] EENA (2019) Public Warning Systems – Update. Version 3.0. European Emergency Number Association. Available at: https://eena.org/wp-content/uploads/2019_03_30_PWS_Document_FINAL_Compressed.pdf
[23] Roshan, M., Warren, M., & Carr, R. (2016). Understanding the use of social media by organisations for crisis communication. Computers in Human Behavior, 63, 350-361.
[24] Petersen, L., Fallou, L., Reilly, P., & Serafinelli, E. (2017, May). Public expectations of social media use by critical infrastructure operators in crisis communication. In ISCRAM.
[25] Boamah, M. D. (2019). Analysing crisis communication strategies of airline companies in United States: a case study of Southwest Airline 2016 power outage crisis. Stud. Media Commun., 7, 7-16.
[26] Benoit, W. L. (2018). Crisis and image repair at United Airlines: Fly the unfriendly skies. Journal of International Crisis and Risk Communication Research, 1(1), 2.
[27] Liverpool Women's Hospital (2021) Updates following recent incident at Liverpool Women's Hospital. https://www.liverpoolwomens.nhs.uk/news/updates-following-recent-incident-at-liverpool-women-s-hospital
[28] Petersen, L., Fallou, L., Reilly, P., Serafinelli, E., Carreira, E., Utkin, A. (2016). Social resilience criteria for critical infrastructures during crises. IMPROVER project, Deliverable 4.1, European Commission H2020
[29] Temnikova, I., Vieweg, S., & Castillo, C. (2015, May). The case for readability of crisis communications in social media. In Proceedings of the 24th international conference on world wide web (pp. 1245-1250).
[30] World Health Organization. (2021, April 20). WHO Strategic Communications Framework for effective communications. Available at: WHO: https://www.who.int/mediacentre/communication-framework.pdf
[31] Sutton, J., Spiro, E., Johnson, B., Fitzhugh, S., Gibson, B. and Butts, C. (2014) 'Warning Tweets: Serial Transmission of Messages During the Warning Phase of a Disaster Event'. Information, Communication and Society, 17(6): 765-787.
[32] Doermann, J. L., Kuligowski, E. D., & Milke, J. (2021). From social science research to engineering practice: Development of a short message creation tool for wildfire emergencies. Fire Technology, 57(2), 815-837.
[33] Murphy, J., Rutland, K., Dyson, J., Leck, A., Rundle, S., Greer, D., & Dootson, P. (2018). Public information and warnings (Australian Disaster Resilience Handbook Collection, Handbook 16).
[34] Neußner, O. (2021). Early warning alerts for extreme natural hazard events: A review of worldwide practices. International Journal of Disaster Risk Reduction, 60, 102295.
[35] Kelman, I., Fearnley, C. (2021) Warnings as social processes. Anticipation Hub. https://www.anticipation-hub.org/news/warnings-as-social-processes
[36] Pannocchia, D., Sahar, A., McAlpine, A (2021) D6.1 Social Engagement Guidelines. Aqua3S - Enhancing standardisation strategies to integrate innovative technologies for Safety and

Security in existing water network. Funded under the H2020 research and innovation programme under Grant Agreement No. 832876.
[37] Coombs, W. T. (2019). Ongoing crisis communication: Planning, managing, and responding. Sage Publications. (p.94)
[38] Sutton, J., & Kuligowski, E. D. (2019). Alerts and warnings on short messaging channels: Guidance from an expert panel process. Natural Hazards Review, 20(2), 04019002.
[39] European Commission (2022) Electronic communications laws. Available at: https://digital-strategy.ec.europa.eu/en/policies/electronic-communications-laws
[40] Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code
[41] ETSI TS 102 900 v1.3.1 (2019-02) Emergency Communications (EMTEL) and European Public Warning System (EU-Alert) using the Cell Broadcast System. Available at: https://www.etsi.org/deliver/etsi_ts/102900_102999/102900/01.03.01_60/ts_102900v010301p.pdf
[42] Lasschuyt, E., van Hekken, M., Treurniet, W., & Visser, M. (2004). How to make an effective information exchange data model or the good and bad aspects of the NATO JC3IEDM. TNO Physics and Electronics Lab Hague (Netherlands). Available at: https://www.sto.nato.int/publications/STO%20Meeting%20Proceedings/RTO-MP-IST-042/MP-IST-042-09.pdf
[43] OASIS (2010) Common Alerting Protocol Version 1.2. July 2010. Available at: http://docs.oasis-open.org/emergency/cap/v1.2/CAP-v1.2.html
[44] NSTC (2000) Effective Disaster Warnings. Report by the Working Group on Natural Disaster Information Systems Subcommittee on Natural Disaster Reduction. National Science and Technology Council. Archived version available at: https://web.archive.org/web/20060513144112/http://www.sdr.gov/NDIS_rev_Oct27.pdf
[45] National Weather Service (n. d.) Watch Warning Advisory Explained. National Oceanic and Atmospheric Administration (NOAA). Available at: https://www.weather.gov/sjt/WatchWarningAdvisoryExplained
[46] EENA (2019) Public Warning Systems – Update. Version 3.0. European Emergency Number Association. Available at: https://eena.org/wp-content/uploads/2019_03_30_PWS_Document_FINAL_Compressed.pdf
[47] Vigili del Fuoco (2011) Profilo CAP Vigili del Fuoco e modalità preferenziali di trasmissione. Available at: http://www.vigilfuoco.it/aspx/ReturnDocument.aspx?IdDocumento=4857
[48] Oh, S. H., Jung, W. S., Lee, Y. T., & Kim, K. S. (2021, February). Disaster Warning and Alerting Integrated Systems Based on CAP profile. In 2021 23rd International Conference on Advanced Communication Technology (ICACT) (pp. 155-159). IEEE.
[49] Rossi, C., Falcone, G., Frisello, A and Dominici, F. (2018) Best practices on Public warning systems for climate induced natural hazards. EC Joint Research Centre. Available at: https://drmkc.jrc.ec.europa.eu/Portals/0/innovation/SupportSystem/11_Lithuania/JRC_PublicWarningonNaturalHazard_05_PWS_final.pdf
[50] Australian Government (2018) CAP-AU-STD : the Specification, its Validation and Implementation. Bureau of Meteorlology. http://www.bom.gov.au/metadata/CAP-AU/Spec.shtml
[51] National Audit Office (2018) Investigation: WannaCry cyber attack and the NHS. Department of Health. 25 April 2018. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf
[52] Kaspersky (n.d.) What is WannaCry ransomware? https://www.kaspersky.co.uk/resource-center/threats/ransomware-wannacry
[53] Clearswift (n. d) WannaCry Fallout: What the ransomware epidemic means for the future of business. Clearswift by HelpSystems. https://www.clearswift.com/blog/wannacry-fallout-what-ransomware-epidemic-means-future-business

[54] Kroustek, J. (2017) WannaCry ransomware that infected Telefonica and NHS hospitals is spreading aggressively, with over 50,000 attacks so far today. Avast https://blog.avast.com/ransomware-that-infected-telefonica-and-nhs-hospitals-is-spreading-aggressively-with-over-50000-attacks-so-far-today
[55] Flagg, M. (2022) Holding the NHS to ransom. PRAcademy. https://pracademy.co.uk/insights/holding-the-nhs-to-ransom/
[56] Smart, W. (2018) Lessons learned review of the WannaCry ransomware attach. Department of Health and Social Care. NHS England. https://www.england.nhs.uk/wp-content/uploads/2018/02/lessons-learned-review-wannacry-ransomware-cyber-attack-cio-review.pdf
[57] Hughes, O. (2018) Government puts cost of WannaCry to NHS at £92m. Digital Health .12 October 2018. https://www.digitalhealth.net/2018/10/dhsc-puts-cost-wannacry-nhs-92m/
[58] Martin, G., Ghafur, S., Kinross, J., Hankin, C., & Darzi, A. (2018). WannaCry—a year on. BMJ, 361 k8231, https://spiral.imperial.ac.uk/bitstream/10044/1/61546/2/wannacry.pdf
[59] Aylien (n.d.) Media monitoring case study: WannaCry Malware Attack. https://aylien.com/blog/media-monitoring-case-study-wannacry-malware-attack
[60] D'Arcy, M. (2017) WannaCry: NHS Digital addresses comms errors exposed by cyber 'Armageddon'. Highland Marketing. 3 October 2017. https://highland-marketing.com/commentary-analysis/wannacry-nhs-digital-addresses-comms-errors-exposed-cyber-armageddon/
[61] Robinson, J (2017) NHS Digital admits it did not communicate effectively during cyber attack. The Pharmaceutical Journal. 28 September 2017. https://pharmaceutical-journal.com/article/news/nhs-digital-admits-it-did-not-communicate-effectively-during-cyber-attack
[62] Hoeksma, J. (2017). NHS cyberattack may prove to be a valuable wake up call. BMJ, 357.
[63] Patrick Svitek (2022). "Texas puts final estimate of winter storm death toll at 246". The Texas Tribune. Retrieved January 3, 2022. https://www.texastribune.org/2022/01/02/texas-winter-storm-final-death-toll-246/amp/
[64] Twitter (n.d) Exploring #ExtremeWeather: The Texas Freeze. Twitter Developer Platform. https://developer.twitter.com/en/use-cases/build-for-good/extreme-weather/texas-freeze
[65] Lake, H. (2021) Crisis Communication for the Texas Winter Storm 2021. ROXO Agency. 28 February 2021. https://www.roxoagency.com/post/crisis-communication-for-the-texas-winter-storm-2021
[66] Schuman, N. (2021) Texas Storm Communications Show Stark Messaging Contrasts. PR News. 22 February 2021. https://www.prnewsonline.com/texas-storm-communications/
[67] Connelly, J (n.d) Communication in a crisis: How two Texas organisations responded to the deep freeze. https://clydegroup.com/communicating-in-a-crisis-how-two-texas-organizations-responded-to-the-deep-freeze/
[68] Busby, J. W., Baker, K., Bazilian, M. D., Gilbert, A. Q., Grubert, E., Rai, V., ... & Webber, M. E. (2021). Cascading risks: Understanding the 2021 winter blackout in Texas. Energy Research & Social Science, 77, 102106.
[69] Turton, W., Riley, M. , Jacobs, J. (2021) Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom. Bloomberg UK. 13 May 2021. https://www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom
[70] Colonial (2021) Statement: Colonial Pipeline system disruption https://web.archive.org/web/20210508235404/https://www.colpipe.com/news/press-releases/media-statement-colonial-pipeline-system-disruption
[71] FBI (2021) FBI statement on compromise of Colonial pipeline networks. Federal Bureau of Investigation. 10 May 2021. https://www.fbi.gov/news/press-releases/press-releases/fbi-statement-on-compromise-of-colonial-pipeline-networks

[72] Segal, E. (2021) Colonial pipeline was silent for more than a day about cyber attack . Forbes. 9 May 2021. https://www.forbes.com/sites/edwardsegal/2021/05/09/colonial-pipeline-is-mum-on-status-of-response-to-cyber-attack/
[73] Lessons Learned from the HSE Cyber Attack (2022) Leadership for IT security & privacy across HHS https://www.hhs.gov/sites/default/files/lessons-learned-hse-attack.pdf
[74] BBC News (2021) Cyber-attack on Irish health service 'catastrophic'. BBC News. 20 May 2021 https://www.bbc.co.uk/news/world-europe-57184977
[75] Carswell, S., McQuinn, C. (2021) HSE uneasy about restarting record-sharing system between hospitals. The Irish Times. 27 May 2021. https://www.irishtimes.com/news/health/hse-uneasy-about-restarting-record-sharing-system-between-hospitals-1.4576215
[76] Crouch, H. (2021) Irish health iT remain shut down following significant ransomware attack. Digital Health. 17 May 2021. https://www.digitalhealth.net/2021/05/irish-health-it-services-shut-down-over-significant-ransomware-attack/
[77] Financial Times, Laura Noonan and James Shotter, 2021 https://www.ft.com/content/13d33a08-ce83-4f8a-8d93-a60a5e097ed8
[78] Regan, E., Schiller, R. (2021) 100,000 out-patient appointments cancelled due to HSE hack. Independent. 27 May 2021. Available at: https://www.independent.ie/irish-news/health/100000-out-patient-appointments-cancelleddue-to-hse-hack-40474312.html
[79] Heath Service Executive (2021) Health Service Disruptions http://web.archive.org/web/20210521145823/https://www2.hse.ie/health-service-disruptions/
[80] National Cyber Security Centre (2021) Ransomware attack on health sector – update. National Cyber Security Centre. 15 May 2021. https://www.ncsc.gov.ie/pdfs/HSE_Conti_140521_UPDATE.pdf
[81] Reynolds, P. (2021) The anatomy of the health service cyber attack. RTE. 23 May 2021. https://www.rte.ie/news/analysis-and-comment/2021/0523/1223337-cyber-attack-hse/
[82] PWC (2021) Conti cyber attack on the HSE – Independent post incident review. PWC. 3 December 2021. https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf p. 138
[83] Shackle, S (2020) The mystery of the Gatwick drone. The Guardian. 1 December 2020. https://www.theguardian.com/uk-news/2020/dec/01/the-mystery-of-the-gatwick-drone
[84] Wang, M., Robinson, S. (2019) Crisis review: Gatwick airport's drone incident. 5 December 2019. https://www.crisisshield.com.au/post/crisis-review-gatwick-airport-s-drone-incident
[85] https://twitter.com/Gatwick_Airport/status/1075522187946221569
[86] International Airlines Group (2022) 'Our Brands' retrieved from https://www.iairgroup.com/en/our-brands
[87] International Commissioner's Office (2022) 'History of the ICO' retrieved from https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/
[88] Information Comissioner's Office (2020) "ICO fines British Airways £20m for data breach affecting more than 400,000 customers" 16 October 2020 retrieved from https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/
[89] National Cyber Security Centre (2022) Multi-factor authentication for Online Services retrieved from https://www.ncsc.gov.uk/guidance/multi-factor-authentication-online-services
[90] BBC Breakfast Broadcast on the 7 September 2018 by Alex Cruz
[91] Alex Cruz talking on BBC Breakfast on the 7 September 2018 retrieved from https://twitter.com/BBCBreakfast/status/1037988972998340613

[92] Borner, P. (2020) "British Airways suffers Sophisticated Data Breach" 8 September 2018 Data Privacy Group retrieved from https://thedataprivacygroup.com/us/blog/british-airways-suffers-sophisticated-data-breach/
[93] National Weather Service (n. d.) Watch Warning Advisory Explained. National Oceanic and Atmospheric Administration (NOAA). Available at: https://www.weather.gov/sjt/WatchWarningAdvisoryExplained
[94] Consultative Committee for Space Data Systems. (2006). Security threats against space missions. CCSDS 350.1-G-3. CCSDS Secretariat: Washington, DC, USA.
[95] Pescaroli, G., Green, L. M., Wicks, R. T., Turner, S., & Bhattarai, S. (2019). Cascading effects of global positioning and navigation satellite service failures.
[96] Doermann, J. L., Kuligowski, E. D., & Milke, J. (2021). From social science research to engineering practice: Development of a short message creation tool for wildfire emergencies. Fire Technology, 57(2), 815-837.

Annex I: Translated messages

Spanish translations

Segment	Standard Elements	
Severity	• Red • Yellow • Green	• Roja • Amarilla • Verde
Type	• alert • warning • advisory • caution • update • all clear • information • [custom text field]	• alerta • advertencia • aviso • precaución • actualización • toda clara • información
Category	• unauthorised entry • trespasser on site (single person) • trespasser on site (multiple people) • unauthorised UAV • unauthorised entry to building • unauthorised system access (remote) • system unavailability • cyber attack • DDoS attack • jamming attack • ransomware • data breach • personal data breach • natural disaster • severe weather • earthquake • wildfire • terrorist attack • serious incident • datacentre malfunction	• entrada no autorizada • intruso en el sitio (persona sola) • intruso en el sitio (varias personas) • UAV no autorizado • entrada no autorizada al edificio • acceso no autorizado al sistema (remoto) • indisponibilidad del sistema • ataque cibernetico • ataque DDoS • jamming attack • secuestro de datos • filtración de datos • violación de datos personales • desastre natural • tiempo severo • terremoto • incendio forestal • ataque terrorista • incidente grave • mal funcionamiento del centro de datos

	• service offline • threat detected • [custom text field]	• servicio sin conexión • amenaza detectada
Effective date/time	active from • [free text] - date / time / time descriptor (e.g., today, tomorrow, etc.)	activo desde
End data / time	Until • [free text] - date / time / time descriptor (e.g., today, tomorrow, etc.)	hasta
Location	In • [custom text field]	in
Event Description	• [custom text field]	
Audience	• Citizens • Visitors • Employees • Users	• Los ciudadanos • Las visitantes • Los empleados • Los usuarios
Instructions	should • go to [location] • avoid [location] • evacuate immediately • shelter in place • continue as normal • alert physical security team • alert cyber security team • log out of all systems • shut down your personal computer or laptop • change password • log into system • wait for updates • avoid making system requests • enable MFA	deben • ir a [location] • evitar [location] • evacuar inmediatamente • refugiarse en el lugar • volver al edificio • continuar con normalidad • alertar al equipo de seguridad física • alertar al equipo de seguridad cibernética • desconectarse de todos los sistemas • apagar su computadora personal • cambiar la contraseña • los ciudadanos deben iniciar sesión en el sistema • esperar actualizaciones • evitar hacer solicitudes al sistema

	• contact [organisation] • [custom text field]	• habilitar MFA • contactar a [organisation]
Organisation	• [custom text field]	
Response Type	is • investigating the cause • resetting services • updating services • recovering data from backups • • coming back online • informing perimeter security team • informing incident response team • searching for the perpertrators • sending help • referred to [police/civil protection / etc.] • [custom text field]	es • investigando la causa • restablecer servicios • actualizando los servicios • recuperar datos de copias de seguridad • volviendo a estar en línea • informando al equipo de seguridad perimetral • informar al equipo de respuesta a incidentes • buscando a los perpetradores • enviando ayuda • referido a [policía/protección civil/etc.]
Update data / time	Update is expected • [free text] - date / time / time decriptor (e.g., today, tomorrow, etc.)	Se espera una actualización en
URL	Visit • [url] For more information	Visitar … para más información
Contact Info	or contact us using • [custom contact details – phone number, email, etc.]	o contáctenos usando

French translations

Segment	Standard Elements	
Severity	• Red • Yellow • Green	• Rouge • Jaune • Vert
Type	• alert • warning • advisory • caution • update • all clear • information • [custom text field]	• alerte • avertissement • consultatif • prudence • mettre à jour • tout est clair • information
Category	• unauthorised entry • trespasser on site (single person) • trespasser on site (multiple people) • unauthorised UAV • unauthorised entry to building • unauthorised system access (remote) • system unavailability • cyber attack • DDoS attack • jamming attack • ransomware • data breach • personal data breach • natural disaster • severe weather • earthquake • wildfire • terrorist attack • serious incident • datacentre malfunction • service offline	• entrée non autorisée • intrus sur place (personne seule) • intrus sur place (plusieurs personnes) • UAV non autorisé • entrée non autorisée dans le bâtiment • accès non autorisé au système (à distance) • indisponibilité du système • cyberattaque • Attaque DDoS • attaque de brouillage • rançongiciel • violation de données • violation de données personnelles • catastrophe naturelle • temps violent • tremblement de terre • wildfire • attaque terroriste • incident grave • dysfonctionnement du centre de données • service hors ligne

	• threat detected • [custom text field]	• menace détectée
Effective date/time	active from • [free text] - date / time / time descriptor (e.g., today, tomorrow, etc.)	actif à partir de
End data / time	Until • [free text] - date / time / time descriptor (e.g., today, tomorrow, etc.)	jusqu'à
Location	In • [custom text field]	à
Event Description	• [custom text field]	
Audience	• Citizens • Visitors • Employees • Users	• Citoyens • Visiteurs • Salariés • Utilisateurs
Instructions	should • go to [location] • avoid [location] • evacuate immediately • shelter in place • return to building • continue as normal • alert physical security team • alert cyber security team • log out of all systems • shut down your personal computer or laptop • change password • log into system • wait for updates • avoid making system requests •	devoir • aller à [emplacement] • éviter [emplacement] • évacuer immédiatement • abri en place • retour au bâtiment • "continuer comme d'habitude • alerter l'équipe de sécurité physique • alerter l'équipe de cybersécurité • se déconnecter de tous les systèmes • éteignez votre ordinateur personnel ou votre ordinateur portable • changer le mot de passe • se connecter au système • attendre les mises à jour • éviter de faire des demandes système

	• enable MFA • contact [organisation] • [custom text field]	• activer l'authentification multifacteur • contact [organisation]
Organisation	• [custom text field]	
Response Type	is • investigating the cause • resetting services • updating services • recovering data from backups • coming back online • informing perimeter security team • informing incident response team • searching for the perpertrators • sending help • referred to [police/civil protection / etc.] • [custom text field]	est • enquêter sur la cause • réinitialisation des services • met à jour des services • récupération de données à partir de sauvegardes • revenir en ligne • informer l'équipe de sécurité du périmètre • informer l'équipe d'intervention en cas d'incident • à la recherche des perpertrators • envoi d'aide • référé à [police/protection civile/etc.]
Update data / time	Update is expected • [free text] - date / time / time decriptor (e.g., today, tomorrow, etc.)	• La mise à jour est attendu
URL	Visit • [url] For more information	Visite … pour plus d'informations
Contact Info	or contact us using • [custom contact details – phone number, email, etc.]	ou contactez-nous en utilisant

Italian translations

Segment	Standard Elements	
Severity	• Red • Yellow • Green	• Rosso • Giallo • Verde
Type	• alert • warning • advisory • caution • update • all clear • information • [custom text field]	• allarme • avvertimento • consultivo • cautela • aggiornare • tutto chiaro • informazione
Category	• unauthorised entry • trespasser on site (single person) • trespasser on site (multiple people) • unauthorised UAV • unauthorised entry to building • unauthorised system access (remote) • system unavailability • cyber attack • DDoS attack • jamming attack • ransomware • data breach • personal data breach • natural disaster • severe weather • earthquake • wildfire • terrorist attack • serious incident • datacentre malfunction • service offline	• ingresso non autorizzato • trasgressore in loco (persona singola • trasgressore in loco (più persone) • UAV non autorizzato • ingresso non autorizzato all'edificio • accesso non autorizzato al sistema (remoto) • indisponibilità del sistema • attacco informatico • Attacco DDoS • attacco jamming • ransomware • violazione dei dati • violazione dei dati personali • disastro naturale • maltempo • terremoto • wildfire • attacco terroristico • incidente grave • malfunzionamento del datacenter • servizio offline

	• threat detected • [custom text field]	• minaccia rilevata
Effective date/time	active from • [free text] - date / time / time descriptor (e.g., today, tomorrow, etc.)	Attivo da
End data / time	Until • [free text] - date / time / time descriptor (e.g., today, tomorrow, etc.)	Fino a
Location	In • [custom text field]	di
Event Description	• [custom text field]	
Audience	• Citizens • Visitors • Employees • Users	• Cittadini • Visitatori • Personale • Gli utenti
Instructions	should • go to [location] • avoid [location] • evacuate immediately • shelter in place • return to building • continue as normal • alert physical security team • alert cyber security team • log out of all systems • shut down your personal computer or laptop • change password • log into system • wait for updates • avoid making system requests • enable MFA • contact [organisation] • [custom text field]	Dovere • vai a [posizione] • evitare [posizione] • evacuate immediately • riparo sul posto • ritorno all'edificio • continuare normalmente • avvisare il team di sicurezza fisica • allertare il team di sicurezza informatica • disconnettersi da tutti i sistemi • spegni il tuo personal computer o • cambia password • accedere al sistema • attendere gli aggiornamenti • evitare di effettuare richieste di sistema • abilita MFA • contatto [organizzazione]
Organisation	• [custom text field]	

Response Type	is • investigating the cause • resetting services • updating services • recovering data from backups • coming back online • informing perimeter security team • informing incident response team • searching for the perpertrators • sending help • referred to [police/civil protection / etc.] • [custom text field]	é • indagare sulla causa • reimpostazione dei servizi • aggiornamento dei servizi • recupero dei dati dai backup • tornare online • informare il team di sicurezza perimetrale • informare il team di risposta agli incidenti • ricerca dei perpertratori • invio di aiuto • riferito a [polizia/protezione civile/ecc.]
Update data / time	Update is expected • [free text] - date / time / time decriptor (e.g., today, tomorrow, etc.)	L'aggiornamento è previsto
URL	Visit • [url] For more information	Visita …per maggori informazioni
Contact Info	or contact us using • [custom contact details – phone number, email, etc.]	oppure contattaci utilizzando

Horizon 2020
European Union Funding
for Research & Innovation

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 883284