intersec

Whitepaper

18 myths about public warning systems — debunked.

PUBLISHED IN 2026

- Common misconceptions
- Technical misconceptions
- Operational misconceptions
- Public misconceptions

INTRODUCTION

The UN's Early Warning for All initiative (EW4All) is gaining momentum. Technological readiness assessments, national roadmaps, and new financing mechanisms are multiplying. Public-private collaboration is accelerating delivery, bringing years of accumulated experience and domain expertise to bear on national deployments.

The results speak for themselves. FR-Alert, France's national warning system, spans 21 mobile network operators and serves over 1,000 operator users across mainland France and its overseas territories. In Kuwait, a Cell Broadcast system was deployed in under 10 days — in the middle of an active regional conflict.

And yet progress remains uneven. In the Global South especially, implementation stalls — not always for lack of funding or political will, but because of persistent misconceptions that distort decision-making before it begins. "Too expensive." "Too complex." "Too intrusive." "It takes months to deploy." These objections are heard repeatedly, and they are rarely examined critically.

This whitepaper addresses them directly. Across 18 myths — spanning fundamentals, technology, system design, and public perception — we set out to separate fact from fiction, and to offer the clearer picture that sound decisions require.

PODCAST SERIES
Debunking the most common misconceptions

Myths covered in this whitepaper are debunked episode by episode in our podcast series, available on all major platforms.
Same facts, same expertise, on the go.

YouTube Spotify DEEZER
Apple Podcasts music

Table of content

MYTH #1

Early warning systems are only for natural disasters.

A common misconception is that Early Warning Systems (EWS) are designed exclusively for natural disasters. In practice, their scope is significantly broader. An EWS enables the collection, integration, and analysis of diverse data sources in order to detect risks and trigger timely alerts when a threat or emergency arises. While much of the existing literature and public awareness focuses on natural hazards —such as earthquakes or floods—these represent only a subset of potential applications.

The underlying technological architecture of EWS is adaptable to a wide range of contexts. Beyond natural disasters, such systems can support responses to security threats (including conflict situations or terrorist attacks), industrial and technological incidents (such as gas explosions or chemical spills), public health emergencies (as illustrated during the COVID-19 pandemic), and societal use cases such as missing persons alerts.

The effectiveness and scope of an EWS depend largely on the availability and integration of relevant data. These data streams may include mobile network information, inputs from connected sensors (e.g., river level or environmental monitoring devices), and national or regional geographic information systems. When combined, they enable a comprehensive, real-time operational picture.

As a result, modern EWS should not be understood solely as alerting tools. Increasingly, they function as integrated crisis management platforms, providing a consolidated and dynamic view of evolving situations. In this capacity, they can also interoperate with Public Safety Answering Point (PSAP) systems, enhancing emergency response through improved situational awareness and more accurate caller location.

MYTH #2

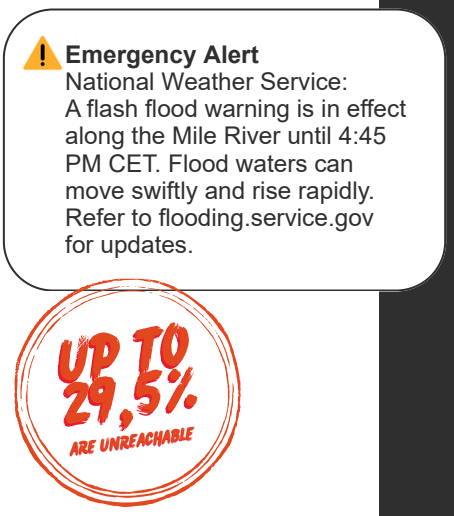
Cell Broadcast (CB) is the best channel for severe emergencies.

CB transmits messages to all mobile devices in a defined area, regardless of device type, subscription, or data connectivity, making it highly effective for rapid, large-scale alerts. However, incident severity alone doesn't determine the best alerting channel.

But fit depends on context, not just severity. Only a narrow set of scenarios genuinely require notifying entire populations within seconds. In most cases, more targeted communication is preferable, focusing on individuals directly exposed to the risk within a defined area. Technologies such as location-based SMS can support this level of precision without necessarily overloading mobile networks.

Opt-out rates are a significant blind spot. The systematic use of Cell Broadcast raises considerations related to public engagement and effectiveness. Overuse of mass alerting channels may contribute to alert fatigue, potentially leading individuals to disable notifications. A 2024 U.S. study (Parker) found that up to 29.5% of adults had opted out of at least one Wireless Emergency Alert category. This means up to one in four people in some areas may never receive a CB alert. Alert fatigue is a key driver: overuse of mass alerts leads people to disable notifications entirely.

EXAMPLE OF CB ALERT



CB has real operational limitations. For end users, messages are transient and may disappear once acknowledged, with limited awareness of how to retrieve them. For emergency management authorities, the absence of delivery confirmation and the inability to easily issue follow-up or targeted messages constrain operational feedback and adaptability.

Consequently, rather than positioning Cell Broadcast as a universal solution, current best practice emphasizes a multi-channel alerting strategy. Combining CB with complementary tools, such as location-based SMS, broadcast media (television and radio), sirens, official websites, and social media, enhances both reach and relevance.

MYTH #3

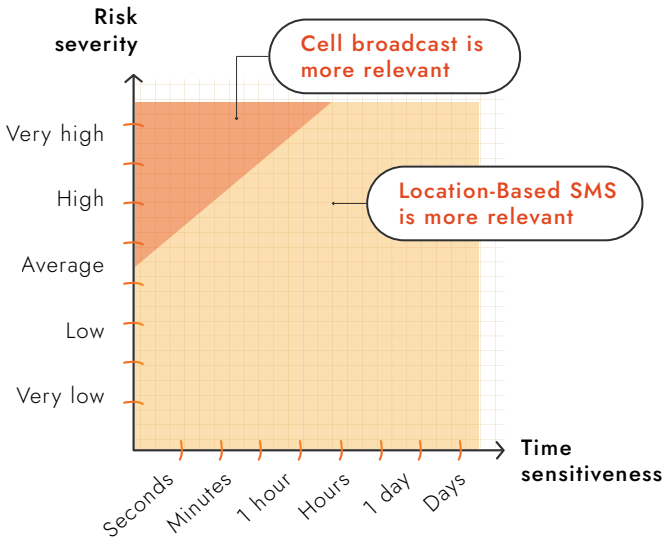
CB is for urgent interruption; LB-SMS is for informational continuity.

It is reductive to assume that Cell Broadcast (CB) is only for urgent interruption while Location-Based SMS (LB-SMS) is reserved for informational follow-up. The decision to issue an alert should instead be guided by three key criteria:

1. **Immediacy of the threat**
2. **Potential severity**
3. **Geographical scope**

- For example, in the case of flooding, LB-SMS is sufficient in most situations. Even if the threat is imminent, it is generally predictable and affects a clearly defined area.
- Cell Broadcast, in practice, is useful in relatively few cases: when a threat is large-scale, imminent, affecting a broad population, and requires the shock effect produced by the distinctive CB alert sound to immediately capture attention.

A simple question authorities can ask themselves is: Do we need to wake people up in the middle of the night to deliver this message? If the answer is yes, there is a strong likelihood that the criteria are met and that a CB alert should be triggered. If the answer is no, LB-SMS will likely be sufficient, allowing for more comprehensive and contextualized crisis communication.



GSMA and major Mobile Network Operators - including VEON, KDDI, Globe, Safaricom, Telefónica, MTN, and Axiata Group - have issued a call to action to deploy both CB and LB-SMS.

At the 2025 CAP Workshop, the European Emergency Number Association (EENA) listed this recommendation as a best practice for EWS implementation in the EU.

MYTH #4

Combining CB and LB-SMS is too expensive.

It has now been demonstrated multiple times that combining both technologies allows emergency services to get the most out of their public warning investments. Our experience shows that adding LB-SMS typically represents only an incremental cost when building on an existing CB project. The added value, however, is significant, and the return on investment quickly becomes positive when considering the cost of not having both technologies in place - especially given that the populations most exposed to climate disasters are often the poorest*, and many of these countries cannot afford to make the wrong technological choices.

The private sector is also mobilizing to support the wider adoption of effective public warning technologies, particularly in vulnerable or resource-constrained countries. At Intersec, we have introduced Accessibility Frameworks designed to reduce both technological and financial barriers to deploying advanced public warning capabilities. This initiative aims to make mobile-based early warning solutions more accessible to eligible governments - including those in EW4All priority countries, Small Island Developing States (SIDS), Least Developed Countries (LDCs), and conflict-affected regions - by simplifying deployment models, lowering entry costs, and enabling faster, more flexible implementation.

ACCESSIBILITY FRAMEWORKS, BY INTERSEC

REGIONAL SOLIDARITY ALLIANCE	SOVEREIGN PRIORITY ACCESS
Overview: Budget optimization through cross-border cooperation: By pooling deployment across neighboring nations or those sharing common security challenges, we maximize financial resources and foster system interoperability for borderless protection.	Overview: Prioritizing immediate deployment by removing capital barriers through a direct bilateral approach to accelerate national security. We neutralize initial financial burdens (CAPEX) to enable instantaneous operational activation.
The mechanism: Tiered investment support based on the number of participating nations. Up to a 35% reduction on the global infrastructure costs.	The mechanism: Full waiver of activation and integration fees. Only the operational subscription and maintenance costs remain the responsibility of the State.

*UNDP global Multidimensional Poverty Index

MYTH #5

No grants, no early warning system.

The United Nations' Early Warnings for All (EW4All) initiative has opened access to significant funding through international institutions, including the Green Climate Fund and multilateral development banks, aimed at accelerating global coverage.

MULTILATERAL CLIMATE FUNDS

ADAPTATION FUND · CIF · gef global environment facility · GREEN CLIMATE FUND

Even when projects are approved, however, timelines can be long, and funds are not always fully available for deployment. In some cases, a substantial portion of grants is allocated to preparatory studies, leaving limited resources for actual system implementation.

There are, nonetheless, multiple avenues to support EWS projects financially:

01
Targeted programs
CREWS and the GSMA Innovation Fund provide funding for feasibility studies, pilot projects and testing.

02
Multi-country projects
Shared cloud environments with dedicated workspaces achieve economies of scale, particularly suited to SIDS and other resource-constrained regions.

03
Private-sector frameworks
Accessibility Frameworks lower technological and financial barriers, and we help governments secure long-term affordable loans through partner financial institutions. Cf. Myth #4

With this combined approach - leveraging international funding, multi-country cooperation, and private-sector support - deploying an effective Early Warning System becomes not just a question of budget, but a practical and achievable strategy for building resilience against crises.

MYTH #6

It takes months to deploy a national PWS.

Deployment timelines have shortened dramatically. While complexity and national context vary, a functional system can be operational within days in urgent situations.

In Kuwait, in response to the country's urgent security needs amid the ongoing regional conflict in the Middle East, Intersec deployed a fully operational cell broadcast system in six days.

Several factors made this possible.

- A cloud-first approach — going live on vendor infrastructure immediately, with migration to sovereign infrastructure on a separate timeline — eliminates the most common bottleneck: waiting for local infrastructure to be ready.
- Kuwait's regulator, CITRA, also played a decisive role by mandating multi-operator cooperation from the outset; without a single authority empowered to align competing operators, that alone can stall deployments by weeks.

Beyond speed, cloud-based deployment brings lasting operational benefits: continuous upgrades, 24/7 monitoring, and managed services that frequently outperform on-premise alternatives in both reliability and cost.

More broadly, the Kuwait case illustrates that the barrier to rapid deployment is less technical than organizational. With the right regulatory authority, a cloud-first architecture, and MHEWS readiness treated as a standing priority rather than a crisis response, the sector can realistically meet the UN's target of universal public warning coverage by 2027.

> **"Exceptional circumstances require exceptional teamwork. All teams worked around the clock, and we are extremely proud of what we have achieved together. We selected Intersec for its proven experience in deploying such systems across multiple countries, as well as its innovative approach it proposed to meet the ten-day challenge, and they have not disappointed.**
>
> — Eng. Abdullah Alawadh, Head of Security Operation Centre at CITRA

CITRA
الهيئة العامة للاتصالات وتقنية المعلومات
COMMUNICATION & INFORMATION TECHNOLOGY REGULATORY AUTHORITY

MYTH #7

Mobile network operators will never accept.

Some believe that EWS are “not commercially interesting” or that “there’s no mandate in our country.” While governments are responsible for EWS, telecom operators often bear a significant portion of the financial burden. Without incentives, these systems may not seem commercially attractive. However, our experience shows that national ministries and telecom regulatory agencies play a critical role in highlighting the multiple benefits EWS technology brings at the national level.

EWS can create immediate synergies with telecom obligations, such as supporting law enforcement investigations. They also provide a foundation for innovation and new growth, making platform-based approaches appealing to operators.




Our platform approach - for civil and internal security, compliance, and advanced geolocation use cases - has proven successful in several countries. For example, investing in upgraded network capabilities can quickly lead to cost savings by detecting patterns of telecom and banking fraud.

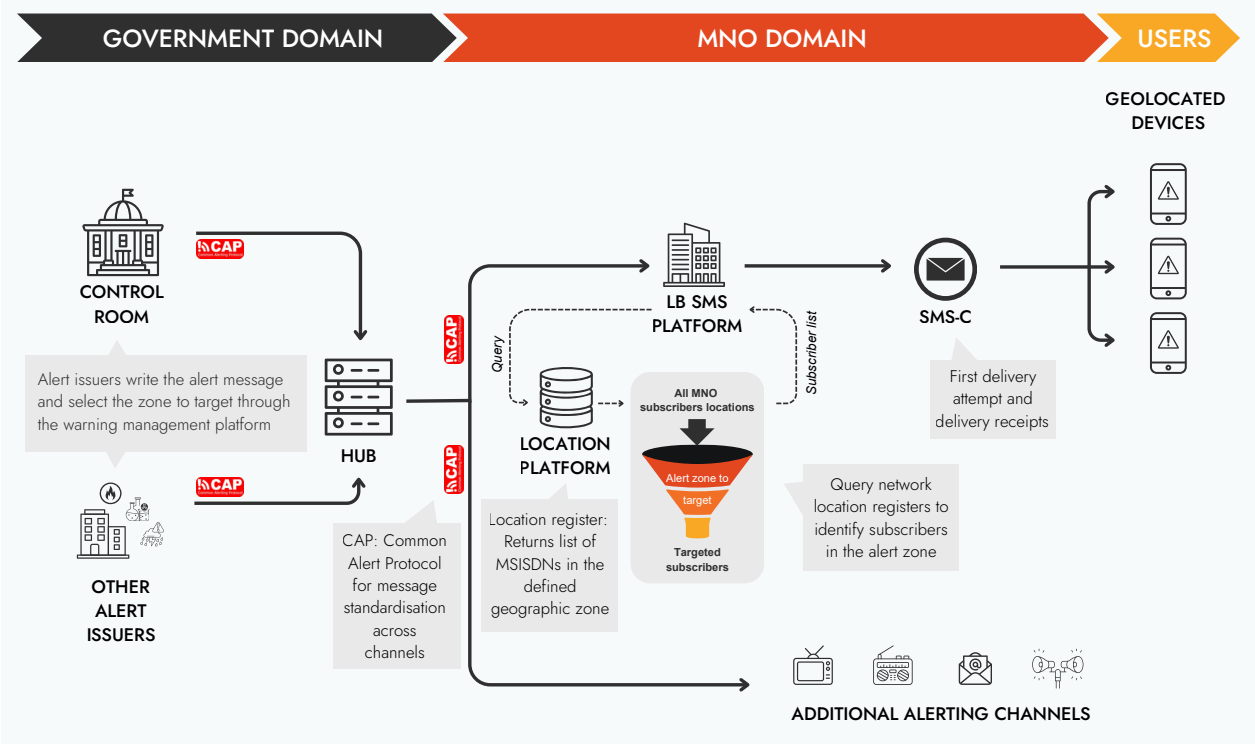
Beyond the commercial and regulatory aspects, public perception plays a key role. In the eyes of citizens and customers, it becomes almost inconceivable that MNOs would not provide alert systems, much like it would be unthinkable for them not to enable emergency calls.

MYTH #8

LB-SMS means network congestion.

In practice, this is not necessarily true, though the concern has a technical basis. LB-SMS alerts travel through the SMSC, the platform that handles all standard SMS traffic across a mobile operator's network, both person-to-person (P2P) and application-to-person (A2P). Sending a large volume of alerts in a short window does require higher throughput than a typical SMSC is configured for, and expanding that capacity can be costly for operators.

The solution is architectural: Intersec deploys a dedicated SMSC module for public warning, entirely separate from regular traffic and supporting only A2P messages. It is capable of processing tens of thousands of messages per second with a minimal hardware footprint. This means LB-SMS alerts have no impact on existing SMS traffic, and authorities can obtain a precise estimate of the time needed to reach the full target population.



In practice, very few alert scenarios require reaching millions of people simultaneously. In the vast majority of cases, a dedicated SMSC is more than sufficient to warn the affected population quickly and effectively, while preserving all the targeting and delivery advantages of location-based SMS.

MYTH #9

LB-SMS does not work for roamers.

A common misconception is that LB-SMS cannot reach roaming subscribers. However, a Mobile Network Operator can effectively target both types of roamers using Passive Location data.

To understand the delivery mechanism, we must distinguish between the two types of roamers:

01

INBOUND ROAMERS (foreign subscribers on the local network)

The PWS delivers LB-SMS to inbound roamers using a custom call flow that identifies the subscriber's current serving node. This method employs an HLR Bypass technique, which allows the MNO to deliver the alert directly without routing it through the subscriber's Home Network. This not only ensures faster delivery but also avoids international roaming interconnection fees.

02

OUTBOUND ROAMERS (local subscribers abroad)

The Passive Location Database tracks when a local SIM attaches to a foreign network. This data allows the PWS to filter and send targeted SMS alerts to all local subscribers currently residing in a specific foreign country or region, ensuring they receive critical information even while abroad.

In summary, roaming does not prevent location-based alerting. With passive location intelligence, MNOs can reliably deliver LB-SMS to both foreign visitors on the local network and their own subscribers traveling abroad.

MYTH #10

LB-SMS multi-language alerts are too many alerts.

Sending multilingual LB-SMS alerts does not mean every user receives the same alert repeated in different languages. Targeting capabilities allow authorities to associate each language version with a specific SIM card nationality, so each user receives only the message corresponding to their SIM card's language — typically the local language for residents, with one or two additional languages assigned to roaming users. This reduces overall network load rather than increasing it.

One important clarification: this language matching is a configuration applied at alert creation by the authorities, not an automatic translation performed by the network. The message each user receives is always the one written directly by the issuing authority — the network routes it to the right audience, but does not generate or translate it.

This differs from Cell Broadcast, where all language versions of the alert are broadcast simultaneously by the network, and each device selects which version to display based on its own settings.

MYTH #11

Cell broadcast alerts are too intrusive.

Yes, Alert Level 1 (also called the Presidential Alert) is intentionally intrusive, with a loud warning sound. That is exactly its purpose, and it is reserved only for the most critical emergencies.

L1	**PRESIDENTIAL · loud, mandatory, intentionally intrusive** — reserved for life-threatening emergencies. No disable option.

However, Cell Broadcast includes a broad range of alert levels:

L2	**EXTREME · loud alert tone and strong vibration** — for the most severe threats, like hurricanes or tornadoes.
L3	**SEVERE · loud alert tone and strong vibration** — serious threats to safety, but considered less critical.
L4	**INFORMATION · option to send "silent alerts"** — for example, at night or during an active shooter situation.
MISSING PERSONS	**CHILD ABDUCTION · loud alert tone and strong vibration** — rapid alerts play a crucial role in returning a missing child.
TEST	**EXERCICE · Testing of operators in the security alert system** — at the authority's discretion.

For all levels other than Level 1, authorities can define how the alert behaves on a device: whether it rings, vibrates, or stays quiet. End users can also choose to opt out of these alerts. The phone will still technically receive the alert, but depending on the user's settings, it may or may not be displayed. Notably, silent Level-4 alerts are considered good practice for signalling when an emergency has ended, especially helpful if the initial alert was issued during nighttime.

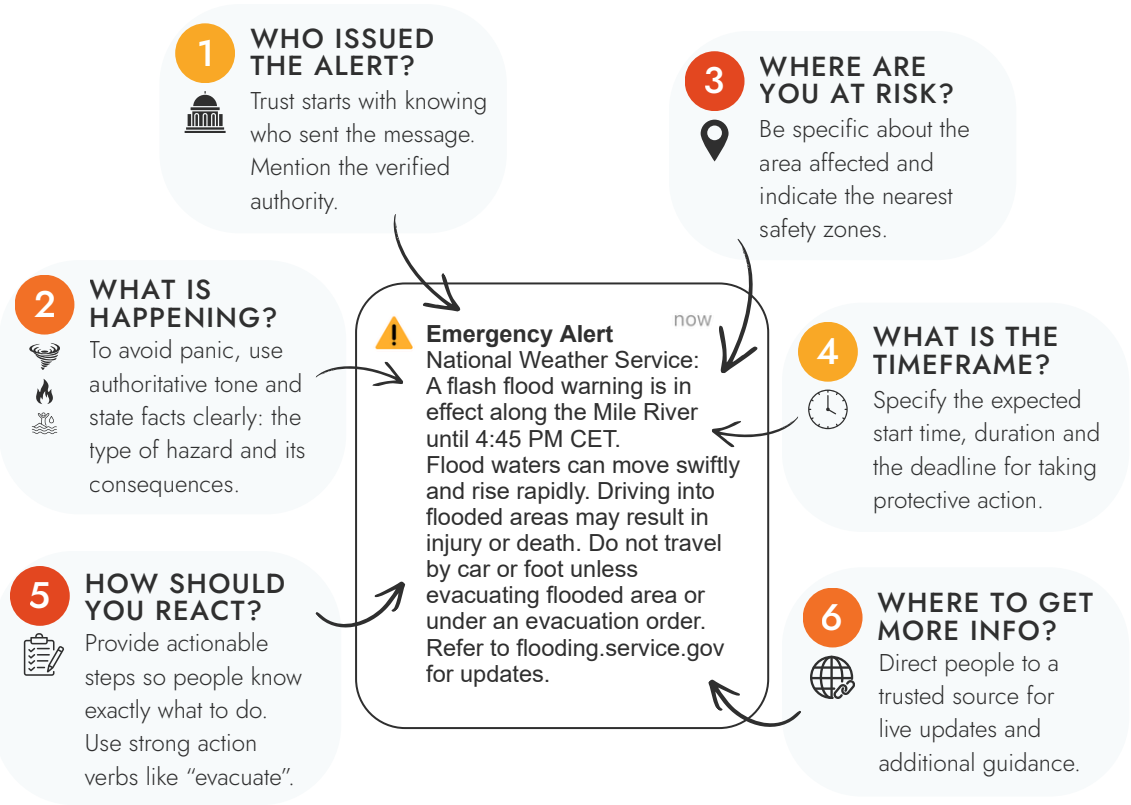
In short, the Cell Broadcast system gives both authorities and end users flexible options to reduce intrusiveness.

MYTH #12

The alert message must include maximum details.

Specifically for LB-SMS, the time required to reach the population depends on both the number of messages sent and the size of each SMS. If an SMS is too long, the network splits it into multiple parts, increasing the total volume of messages that must be delivered.

A better practice is to keep the alert concise: provide short, clear instructions and direct recipients to a more detailed source of information, such as a national website, where they can access comprehensive guidance and behavioural advice.



GOLDEN RULE

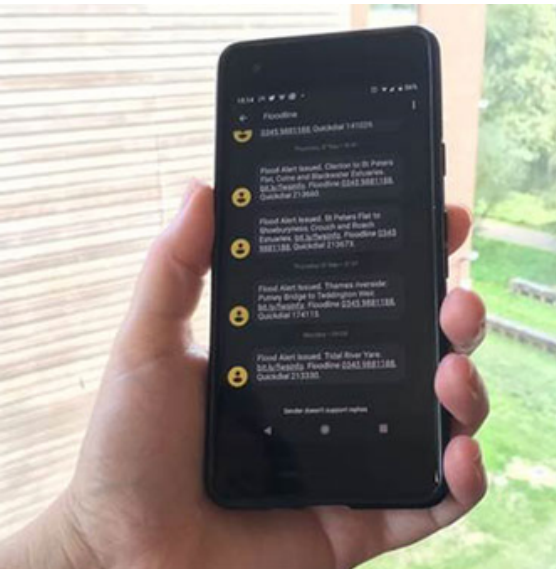
If someone reads it once in 5 seconds, will they know what to do? If yes — your warning works.

MYTH #13

A system without mobile alerts isn't a real warning system.

LB-SMS and CB are the two primary mobile alerting technologies, but they are not the only ones, and for some populations, they are not sufficient.
Even with close to 98% of the global population covered by mobile networks, connectivity remains uneven, and some communities simply do not own a mobile phone. Reaching them requires integrating complementary channels into the national warning architecture.

Registration-based SMS is one of the most underestimated.



Rather than targeting people by physical location at the time of an alert, it allows citizens to register points of interest — a secondary home, a child's school, an elderly relative's address — and receive alerts whenever a threat affects those areas. This address-based, contact-driven approach is particularly powerful for slow-onset hazards like flooding. Intersec contributed to the modernization of the UK Environment Agency's flood warning system, which now serves 2.6 million registered users and issues approximately 3,000 alerts per year.

Beyond SMS, a truly inclusive system draws on a broader set of channels: radio for areas without stable internet infrastructure, IoT-connected sirens for high-risk geographies, community actors such as Local Resilience Agents who relay warnings door-to-door, and voice calls via IVR for populations with low literacy. Television, digital signage, mobile apps, and social media complete the picture.

The goal is not a single universal channel, but the right combination of channels for each community, ensuring that no one is left behind because of the device they carry, or the one they don't.

MYTH #14

AI-powered alerts may lead to errors with tragic consequences.

Imagine evacuation chaos caused by incorrect instructions in an alert message, perhaps due to corrupted data. Intersec applies four discipline lines to any AI feature in the alerting stack.

01 **Trusted high-volume data only.**
AI features should only be applied to data that is nationwide and cannot be spoofed — network data is the prime example.

02 **Explainability.**
The technology provider must be able to show users the steps and reasoning that led to the AI agent's conclusions.

03 **Audits and certifications.**
Regular tests and audits following the most stringent certification and labelling requirements, including those related to cybersecurity risks.

04 **Human-in-the-loop, always.**
AI can automatically trigger internal alerts for operators, helping detect and even predict risks. But in 99% of cases, it would not be reasonable to let an AI agent disseminate a public warning on its own. The remaining 1% — immediate, life-threatening events such as missile launches or earthquake detection — still demands extremely well-designed workflows to eliminate any risk of error.

MYTH #15

A centralized RFP process is always best.

Not necessarily. The optimal approach depends on a country's infrastructure, governance model, and specific context. We have experience with various architectures, including both centralized and decentralized selection and deployment processes. For example:

01

FRANCE

Decentralised ✔

The Ministry of the Interior ran a national RFP process but requested that each mobile network operator (MNO) conduct its own selection process. Intersec was selected by the Ministry and by 15 out of 21 MNOs. A mediation layer allowed the remaining operators, which chose to build their solution in-house, to integrate seamlessly with the national architecture.

02

CROATIA

Centralised ✔

The State ran a national RFP system that included both the Ministry-level application solution and the MNO solutions. All components worked together to ensure full compatibility, while providing a thorough understanding of each operator's constraints and capabilities. A key success factor was that the Intersec team collaborated with a local integration partner, bringing experience and expertise in working with both authorities and operators, in Croatian.

MYTH #16

I must subscribe to receive messages.

It depends on the warning dissemination technology.

- For Cell Broadcast (CB) and Location-Based SMS (LB-SMS), subscriptions are not required. Messages are received automatically: no registration, app installation, or data connection is needed, only a connection to the mobile network. The message is displayed automatically on the phone screen upon receipt, accompanied by an audio signal: a very loud beep for CB messages, and a standard SMS notification sound for LB-SMS messages.
- Registration-based alerting systems are sometimes implemented as a complement to mobile alerting systems, especially to meet specific needs. In England, for example, the Environment Agency uses a registration-based system because floods put homes along rivers at risk. Currently, 2.6 million people have subscribed, as floods represent the main natural disaster risk.

MYTH #17

The state accesses my device location.

The system does not collect or process personal data, nor does it track which mobile phones receive the alert. No personal information, such as phone numbers, is used in emergency alerts.

How does it work? Authorities select a geographic zone on a map, draft the alert, and, upon validation, the system at the telecom operator's level executes the message based on the defined parameters. Mobile subscribers' information remains entirely with the operators, and the phone numbers or identities of individuals are never visible to the authorities in the application solution.

MYTH #18

Authorities will use the system to send commercial or political messages.

Public warning technology allows simultaneous mass messaging to mobile phone users within a defined geographic area without using individual phone numbers at the authority level.

For Cell Broadcast messages, the system does not even require the recipient's number, and it is physically separated from public communication networks to prevent intrusions.

At Intersec, our solution also incorporates a range of security mechanisms designed to prevent misuse of the alerting system and ensure that it is used primarily for emergency notifications in situations of danger.

FRENCH AUTHORITIES TEST FR-ALERT DURING THE 2022 DOMINO EXERCISE. THE INTERFACE ALLOWS AUTHORITIES TO DEFINE AN ALERT AREA ON A MAP AND WRITE A MESSAGE BEFORE OPERATORS BROADCAST THE ALERTS TO THE PUBLIC.

CONCLUSION

Intersec has been deploying public warning systems since 2018, growing from a European pioneer to a global civil protection leader. Today, 47 systems are deployed across Europe, the Middle East, Africa, Asia-Pacific, and Latin America, protecting 460 million people worldwide — with more deployments underway.

Our systems are multichannel and not limited to mobile alerts, integrating traditional and digital channels including mobile apps, emails, sirens, TV, and radio. Our cloud-native architecture allows production-ready deployment in under 10 days, removing the infrastructure bottleneck that has historically delayed national rollouts. We are experienced in crisis management and contextualized messaging in multiple languages, assisted by AI, and all solutions follow the international CAP standard (Common Alerting Protocol).

47
national alerting systems deployed around the world

460M
people protected worldwide with more deployments underway

<10 days
production-ready, cloud-native deployment

We are active members of the ITU, collaborate closely with the GSMA Humanitarian Innovation Team, and work alongside specialized agencies and local partners. Drawing on this experience, we propose solutions tailored to each country's reality: there is no one-size-fits-all approach. Early warning systems are a serious matter, and our goal is to guide public authorities and mobile network operators toward the best decisions for their country, ensuring technology works effectively for the long term.

Rooted in European values of independence, neutrality, and accountability, we are proud to deliver cutting-edge AI technologies developed in Europe to support safe, resilient communities worldwide.

LEARN MORE AT INTERSEC.COM