PSCEurope
Public Safety Communication Europe
www.psc-europe.eu

fidal field trials beyond 5G
Co-funded by the European Union

6GSNS
Funded by the European Union's Smart Network Services Joint Undertaking
Grant Agreement No 101096146

# WHAT SECURITY IN FUTURE COMMUNICATION?

PSCE Spring Conferences 2024 - Workshop Report

## THE EVENT IN A NUTSHELL

- A collaborative session exploring the nature of **technology risk** in the field.
- 10 teams choosing strategies to **maintain communication in a disaster scenario**.
- **Threats and challenges** introduced unexpectedly to see how they impacted the scenario.
- The aim was to **elicit tacit information** from the teams about real-world scenarios.

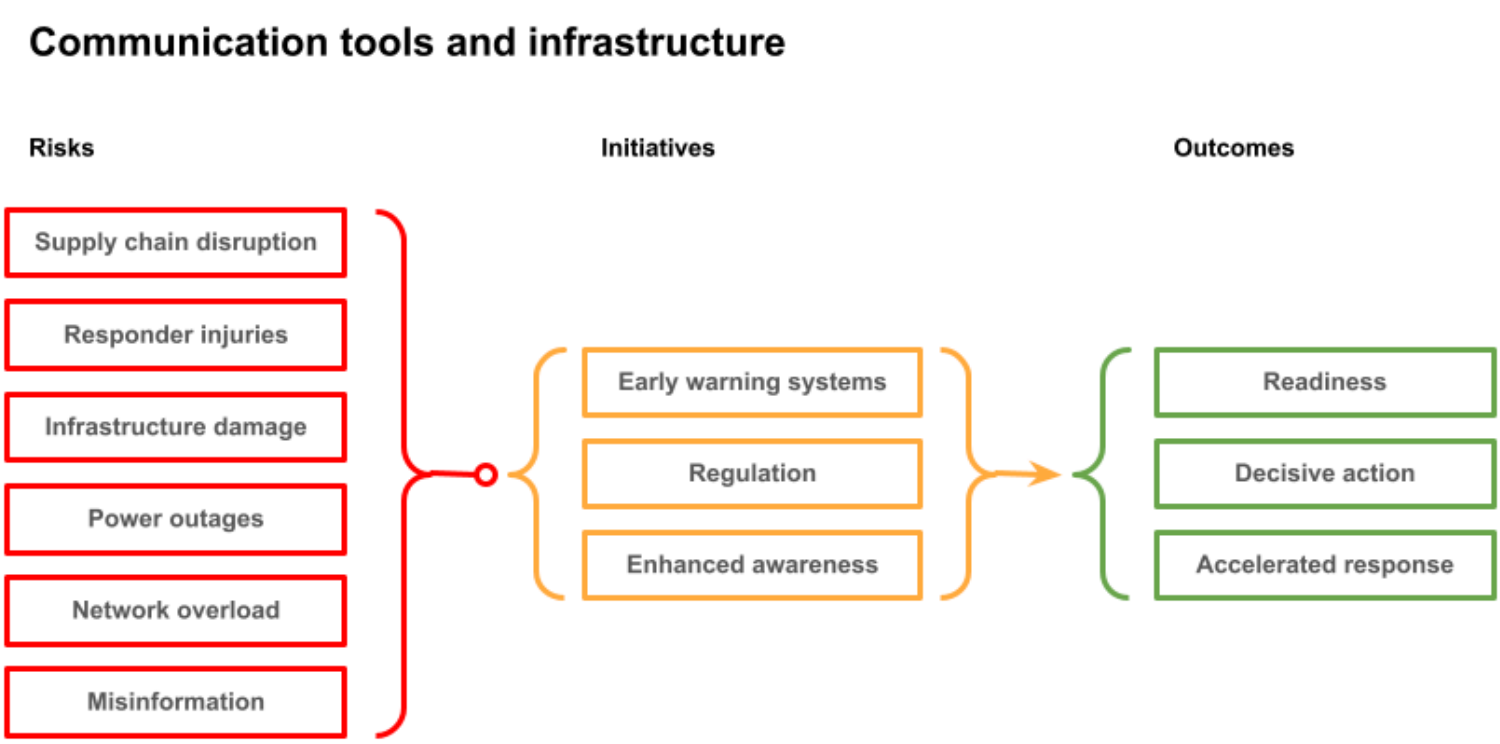
# SUMMARY

In June 2024, we held a collaborative session as part of the PSCE Spring Conference. The session was a novel thought experiment aimed at exploring the nature of technology risks in the field. The workshop was intended to unearth how cybersecurity, and public safety risks manifest in disaster scenarios.
Around 60 participants were grouped in random teams where they were asked to select a disaster scenario and chose strategies to maintain effective communication and save the day. As the workshop progressed, the facilitators introduced threats and challenges to their solutions to see how they impacted the scenario outcomes. The aim was to elicit tacit information from the teams about their involvement real world scenarios.

# RESULTS & THEMES


## Outreach and public awareness promotes effective response

The role of the public in disasters was very thoroughly explored in the workshop. Concepts of leadership and public outreach were prevalent, but the teams also recognised the counterpoint of large-scale misinformation leading to civil unrest and riot. The danger of unsubstantiated rumours was highlighted, emphasising the need for fact checking during a crisis. Our delegates recognised the variety of roles played by the public as; victims of disaster, volunteers aiding in the response, and possible unintentional catalysts for worsening the situation. They also explored the complexity of public safety communications at scale but saw the huge benefit of engaging constructively with communities to source invaluable trusted local knowledge to cope with the emergency.




## Enhanced awareness, alerts and regulation promotes accelerated response

Shared situation awareness is a topic which we have seen arise in previous workshops.

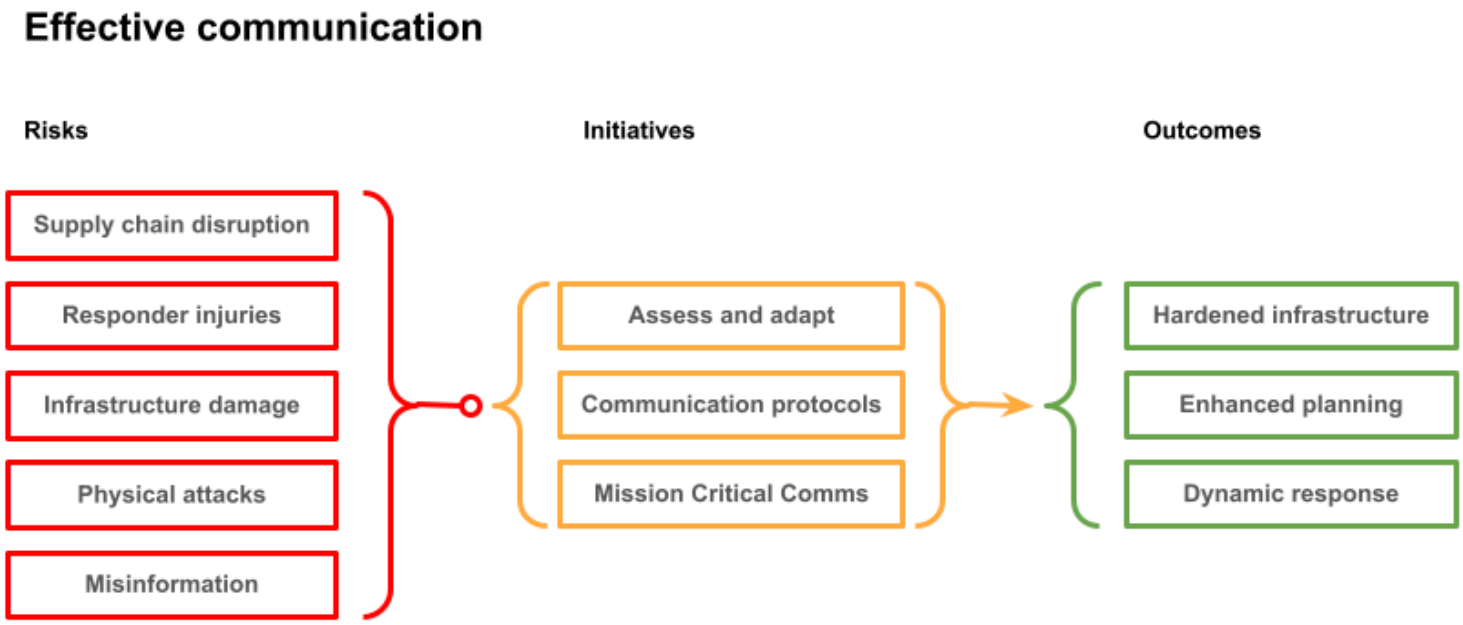
At the summer conference, the teams focused upon what components comprise these systems, and the future technology first responders may have at their disposal.

Our multi-disciplinary teams saw great utility in the promise of drones, artificial intelligence and satellite communications. Respectively, these advanced technologies enhance responder capability, increase the speed of situation analysis and provide robust communication media to disseminate critical information.

However, they also highlighted the need for basic reliable tools which remain useful without a power supply, and the risks that come with overreliance on technology.

The delegate community seemed united in the need for tools which enhance collaboration, and allow quick understanding of the situation, with the aim of having clearer paths to critical decisions.

They also saw the need for proactive enhanced regulation to protect responders and the communication systems they rely on to save lives.




## Well understood and versatile critical communication systems promote a dynamic response

Cyber-attacks pose a significant threat to communication systems.

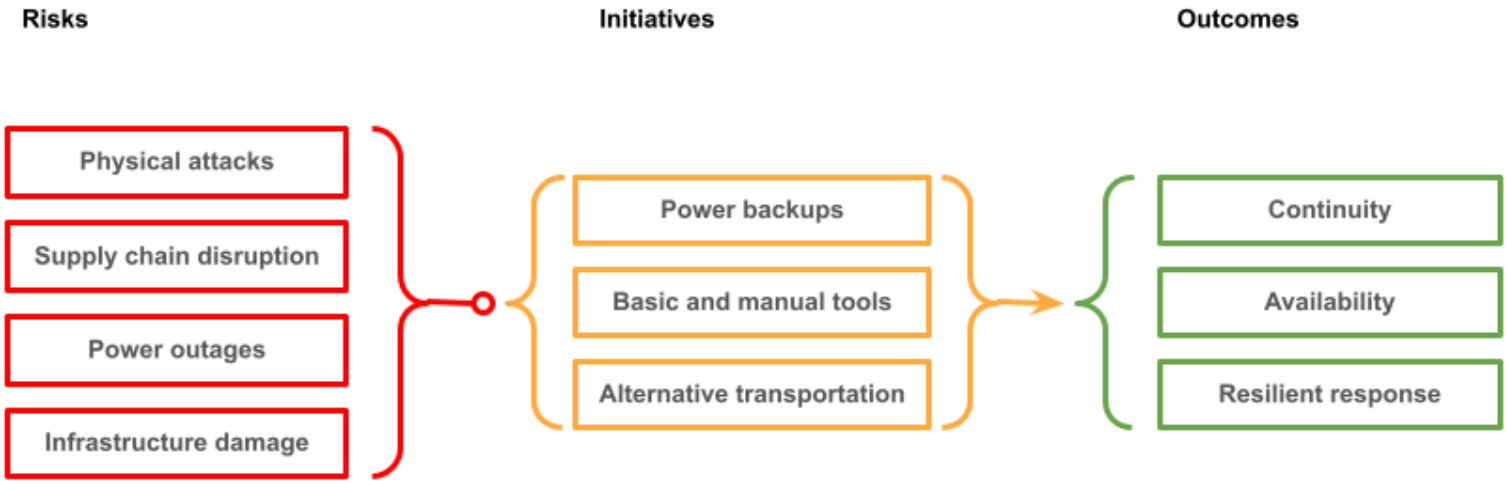
The teams highlighted the risks of interrupted communications and the consequent negative outcomes, as well as the need for preparation.

The discussion centred on the importance of a well understood reliable mission critical communication systems.

Within this discussion they also emphasised the need assess and adapt to scenarios, using pre-planned alternative communication systems when the need arises.

The discussion considered the risks of our growing reliance on technology and the looming threat of well-funded foreign threat actors sowing fear, uncertainty and doubt to exacerbate response challenges.

## Power and Logistics




# Continuity of power and logistics supply promotes resilient response

Within the analysis of logistics, the delegates were quick to highlight the central role of electricity and fuel.

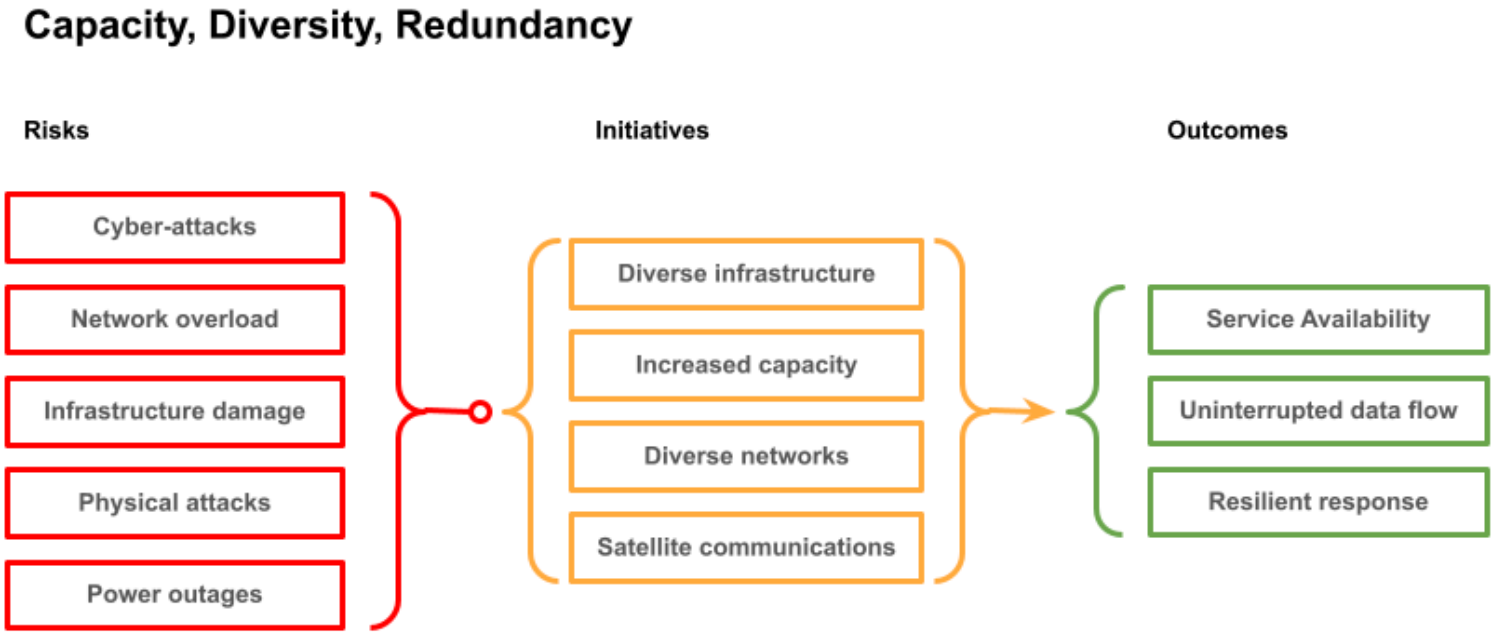
They proposed smart grids, battery backups, and sustainable energy to combat emergencies.

Within this debate the teams also acknowledged the risks of handling fuel in large quantities, and possible kinetic attacks during a crisis.

During the workshop, the conversation explored the heightened risk of unrest during periods of resource shortage.

The focus was on ensuring transport for critical aid and services, even in the event of infrastructure failure.

Additionally, they recognised the competing demands for energy between industry and the recovery effort.



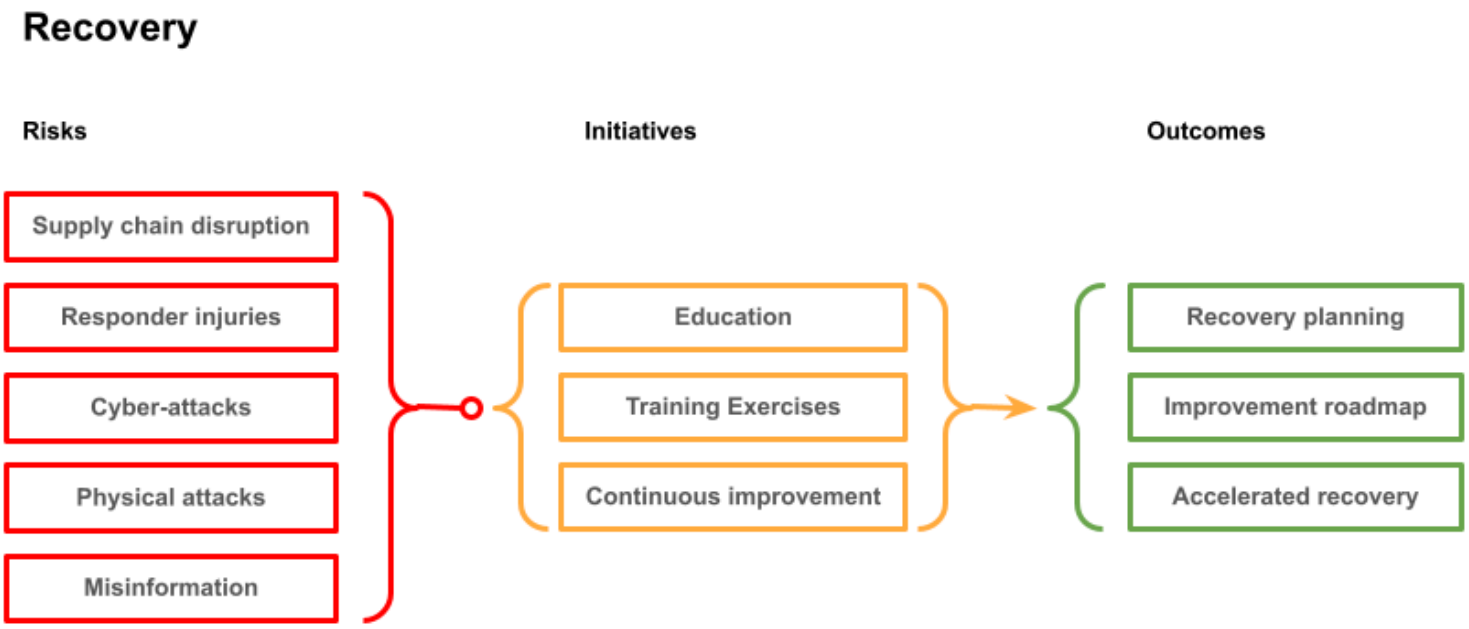

## Continuity of communication and information flow promotes resilient response

Concepts around capacity and high availability surfaced frequently in the workshop.

Our multi-disciplinary teams thought it was paramount to maintain the ability of first responders to communicate seamlessly to reduce delays in the response, which could be lifesaving.

Critical information for first responders must flow unimpeded for the best outcomes.

Designing communication systems with various resilient media would mitigate failure through accidental or deliberate destruction, or sustained denial of service.




## Training, education and continuous improvement accelerate recovery

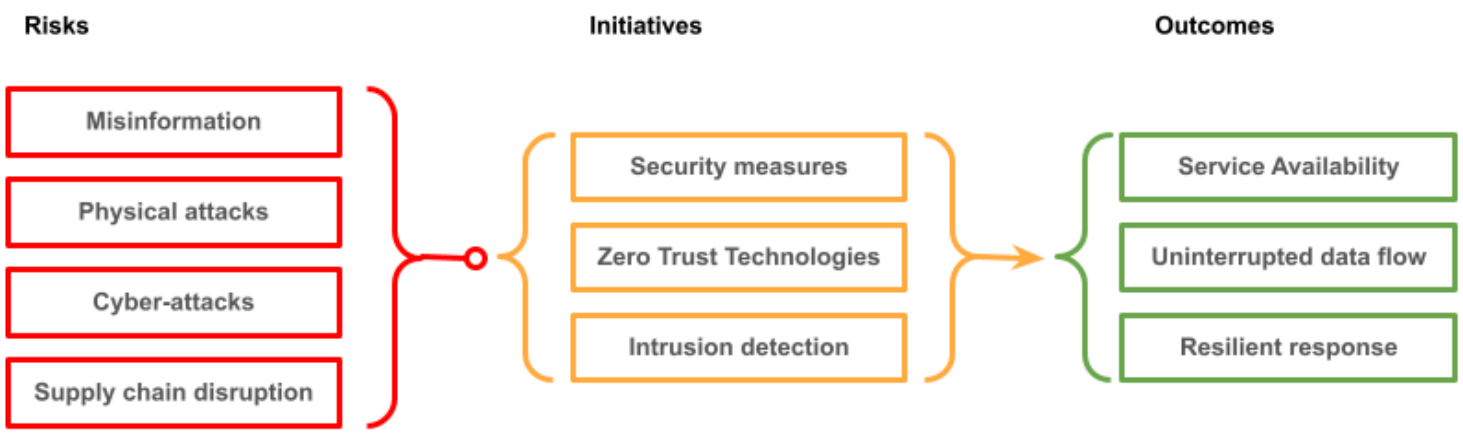
Workshop discussions touched on important concepts concerning the long term and often re-enforcing effects of disasters.

Enabling communities to bounce back from adverse scenarios was foremost in the minds of the teams.

They saw the clear need for planning, guided by past experiences, to optimise strategies for response. Not only this, but they foresaw general approaches to averting emergencies in the first place using effective information management.

Again, the role of information security to protect these efforts from misdirection was a major part of the discussion.

The teams recognised that it was important to project these lessons into the political collective consciousness around resource and resilience planning, to enable faster recovery.




## Continuity of services and data promotes resilient response

Throughout the discussion there was broad acknowledgement that political disruption and misdirection of resources was already a common challenge.

While some sources of misdirection were domestic, there were times in the discussion where the thoughts of our delegates turned to ideologically motivated groups or foreign powers acting in bad faith.

To increase resilience, the discussion frequently turned to security features, like “zero trust” for confidentiality and “priority” for increased availability to key personnel.

Our delegate group saw a need to use enhanced security measures to protect European values, especially democracy and the rule of law.

## CONCLUSION

Our conclusion to the workshop output is that preparation is paramount. Facets of the solution include:

- Communication Tools and Advance Shared Situation Awareness
- Logistics planning, with particular attention to energy and transport
- Effective cyber security awareness, during periods of emergency and public confusion
- Collaboration, coordination and training
- Resilience and Recovery planning

Notably, our growing dependence on technology means that we must plan for scenarios where advanced information technology becomes unavailable or is compromised.