Funded by the European Commission
Seventh Framework Programme

# Cyber ROAD

Development of the Cybercrime and Cyber-terrorism Research Roadmap

Grant Agreement N. **607642**

# Social resilience

Author(s): Davide Andreoletti (SUPSI), Angelo Consoli (SUPSI), Clement Guitton (MELANI)

CC/CT LEG 2 –Absence of a trusted authority for communication with people at risk
CC/CT LEG 3–Identification of possible security and safety issues
CC/CT LEG 1and CC/CT LEG 2–Ensure redundancy of the trusted authority

**ABSTRACT**

Research on social resilience focuses on social responses to cybercrime and cyber terrorism. Leveraging on social resilience provides the basis of a potential programme of intervention that helps to both prevent cybercrimes from taking place and reducing the impact of cybercrime when it does take place. A key aspect of a social resilience system is the presence of a reliable mechanism that is able to spread awareness about some dangerous situation. The idea suggested here consists in the definition of a trusted authority that is in charge of communicating with the potential victims. Implications of the use of such a system are discussed (e.g., security and safety issues).

**RESEARCH ACTION #1**

*Absence of a trusted authority for communication with people at risk*

DISTANCE TO THE MARKET: **TRL 3**
COST OF THE TOPIC: **2 STREPs + 1 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **5**
TIME SPAN FOR ADDRESSING THE ACTION: **24 months**
ACTORS: **Institutional bodies, Security responsible actors, Police, Government, Law enforcement, Research bodies, Cybercrime forces, Police, Research bodies, Private industry**

Telecommunication infrastructures and services are used to communicate in time of crisis; this includes when a terrorist attack has taken place. Two main drawbacks of the current approach are distinguishable: first, people have to proactively tune in to hear about the dangerous situation; second, telecommunication systems only too rarely take into account the issues that could arise following a crisis (e.g., lines jammed because their capacity becomes saturated, routes down lowering this very capacity).
Thus, a mechanism that delivers timely and effective alerts to all the people that are at risk is required. Such a system should be based on a trusted authority (e.g., police/intelligence organization) that is able to certify the presence of a genuine danger. Then, the notification system has to be location-based, i.e., it has to deliver alerts messages to all the people that stay within an area that is considered at risk. For example, all the people within the cellular cell where a terrorist attack occurred could be notified by SMS, or by an automatic call.

It is needed to understand how the trusted authority receives information about the dangerous situation that is happening. In light of the following, we present two options:

1) the first one is that a "trusted authority" which handles the dangerous situation is also responsible of informing the broader public. An illustrative scenario could be: a water plant gathers data collected by its sensors that monitor the quality of water in the supply networks. If the quality of the water is under a threshold, the authority acts as a "trusted authority" and sends alert messages to all the people that reside within the involved areas.
2) the second one is about situations that are more chaotic and difficult to predict (e.g. terrorist attacks). Here it is needed that the "trusted authority" understands that something dangerous is happening, and is in measure to verify that the danger is real. False alarm must be put aside. This can be done with the help of the victims. Research must be done in order to find an easy way to communicate the danger, and then to verify that this is indeed not a false alarm.

The goal is to develop services that help people in danger to find solutions. For example, map of the safe areas can be distributed (e.g., via e-mail) to those who are in the crisis area.

**RESEARCH ACTION #2**

*Identification of possible security and safety issues*

DISTANCE TO THE MARKET: TRL **3**
COST OF THE TOPIC: **2 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **12 months**
ACTORS: **law enforcement agencies and their crisis centre, telecommunication providers, research institutes**

The system has to be reliable and secure. For example, it must be able to disambiguate true from false alarms (including when people genuinely mistakenly over-react thinking a crisis is about to burst when it is not) and it must prevent manipulation activities. One possible malicious activity is described: the attacker could impersonate the trusted authority and provide people with a fake map of safe areas, thus urging people to go to a place where something dangerous would then be happening.

If messages coming from a fake authority are a concern that must be taken into account, the reverse is also true. In fact, the trusted authority should understand where some dangerous situation is really happening, and should do it in a timely manner. To do this, the trusted authority can for instance rely on messages received by people who feel they are at risk (e.g., because gunfire is taking place somewhere). Before sending alarm messages to any involved victims, the authority must be sure that this was a true danger and not, for example, a bad joke.

In order to evaluate the effectiveness of the alerting system, suitable metrics should be properly defined. For example, the time needed to notify potential victims of the occurring danger must be below a given threshold. Also the implication of any security compromise of such a system on human safety has to be quantitatively assessed.

**RESEARCH ACTION #3**

*Ensure redundancy of the trusted authority*

DISTANCE TO THE MARKET: TRL **3**
COST OF THE TOPIC: **2 STREPs + 0 IP**
AVAILABILITY OF COMPETENCE IN EUROPE: **4**
TIME SPAN FOR ADDRESSING THE ACTION: **12 months**
ACTORS: **law enforcement agencies and their crisis centre, telecommunication providers, research institutes**

When a crisis emerges, it may be difficult for authorities to ensure their message reach out to the victims. Telecommunication providers plan for a "normal" usage of their lines; a crisis event is however all but "normal". People's usage pattern changes. Traffic becomes saturated. On top of that, as in the case of a terrorist attack, an explosion may have very well physically damaged part of the telecommunication infrastructure. People within the crisis situation may not have signal. And as a consequence, the information may not reach its target audience in time.

To remedy such a situation, the trusted authority will need to be creative on how to reach out to people. This does not have to be via technological innovation. It will need to ensure that different telecommunication providers have agreements in place to jump in to support each other when such unlikely-but-with-high-safety-risk emerges. It will also need to ensure that it relies on a diverse strategy, using several mediums at the same time. Technology and creativity should allow to replace what otherwise was very effective albeit less convenient to deploy: good old analogous loudspeakers.

An example of such a creative solution could be with the use of drones. If part of the telecommunication infrastructure is down, a few drones could be dispatched to the crisis area, spread out and flown stationary: they could in so doing act as relay to other still-operating telecommunication towers, or transmit information via satellite link. Facebook is famously working on such a system to extend internet offers to developing countries, notably in Africa. Drones could furthermore act as a modern but easier-to-deploy version of the analogous loudspeaker.

Lastly, once such a system has been well-thought, tested and implemented, it should be set as a standard for cities and countries. This implies that the goal is naturally to be able to deploy the system as widely as possible: such a system would ideally be cheap, easy to implement, and not be culture-sensitive. This newly developed system will also need to be mapped to economic models, thus be scalable and adequate for different societal models.