Collaborative Modeling of Awareness in Critical Infrastructure Protection
Josune Hernantes¹, Ana Laugé¹, Leire Labaka¹, Elliot Rich¹,², Finn Olav Sveen³, Jose Mari Sarriegi¹, Ignacio J. Martinez-Moyano⁴,⁶, Jose J Gonzalez³,⁵

¹TECNUN – University of Navarra (jhernantes, alauge, llabaka, jmsarriegi@tecnun.es).
²University at Albany, SUNY, (e.rich@albany.edu) ³Gjøvik University College (finn.sveen@hig.no), ⁴Argonne National Laboratory (imartinez@anl.gov), ⁵University of Agder (josejg@uia.no), ⁶University of Chicago

Abstract
While awareness is acknowledged as a key factor in crisis management, much is vague as to the meaning of the awareness concept, its measurement, how awareness impacts the lifecycle of a crisis and how awareness can be promoted. This vagueness, we hypothesize, potentially reflects the immaturity of crisis management theory. This in turn obscures the landscape of leading crisis indicators, which then leaves crucial clues for the development of crisis management approaches in the attention shadow. In the absence of codified knowledge, the collaborative approach known as Group Model Building employing system dynamics, where modeling experts elicit and unify fragmented, tacit knowledge from domain experts, is worth exploring. We have done so in the context a European project on crisis management of large-scale power cut crises. We describe our preliminary results and propose a concept model relating awareness, leading indicators, and policies for crisis prevention and mitigation.

1. Introduction – definition of needs

While it has been recognized long ago that manifest crises are preceded by a long process of incubation [1-5], most studies of crisis management deal with management of exceptions [6]. Exceptions attract most attention, the most prominent attention given to the “triggering event”, which unleashes the disaster. Rather than thinking in terms of a crisis triggering event some authors [1, 6] favor the term “precipitating event”. The term “precipitating event” recognizes the existence of a process and associated dynamics preceding the manifest crisis.

Once dynamic aspects of crisis lifecycles are recognized, somewhat blurred concepts such as “awareness” and “precursors” and their potential role in crisis prevention, response, and mitigation may become clearer. To illustrate this we summarize insights from a thorough study of accidents in the petrochemical industry [7], based on data recorded in the Dutch accident database FACTS: First, no one of the analyzed accidents were “unforeseen” – all were preceded by significant disruptions (precursor conditions). Second, the cause of the majority (> 60%) of these accidents was management’s failure to adapt to reoccurring disruptions – not being able to change their mental model of the real world. The necessary double-loop learning process, as described by Argyris [8], was severely impaired. Third, most accidents could be linked to changes (technical, organizational, staff) in the company. Sonnemanns et al. [7, p. 193] remark: “A seemingly innocent change in the procedures, in parts, in staffing or in whatever was, almost without exception, the alteration that initiated the propagation and the escalation of the disruption.” The authors conclude “… the double-loop learning cycle should be the focus of safety improvement programmes” [7, p. 194].

We have chosen a study from the petrochemical industry because its completeness and thoroughness.

Figure 1 The awareness ladder (adapted from Shaw et al. [9])
For brevity, we do not discuss studies in other industrial sectors supporting the generic hypothesis
that a feedback learning model must be at the core of safety (and security) improvement processes – a process of organizational learning. We proceed swiftly and remark that in such a feedback context of organizational learning, the concept of awareness – often quite elusive – assumes meaning through levels in a ladder of increasing richness of learning, viz. perception, comprehension and projection [9] – Fig 1.

In this context, “indicators” are “leading indicators” or “precursors” for a potential crisis. Perception of leading indicators requires the ability to distinguish significant information from noise. Leading indicators can be technical or organizational, they can be “hard”, e.g. some loss of control, or ‘soft’, e.g. outcomes of risk analysis [7]. Thus, perception already presupposes that users have an appropriate mental model of the system. Comprehension implies a more advanced mental model, and projection requires an even more advanced, “dynamic” mental model. The transition from perception to projection, via comprehension is a process of organizational learning, whereby a shared understanding is developed of what is not normal and unexpected [10], moving to high reliability by enlarging what people monitor, expect and fear [11].

We are far from having a good theory of crisis management, one that is anchored in organizational science [6]. Awareness is a much quoted concept in the area of information security. But even there, awareness is still understudied, with few empirical studies available [12]. All in all, knowledge required for a generic theory of crisis management is mostly tacit, it is spread in the minds of many experts, that is, it exists only as fragmented knowledge.

In particular, the observation that awareness relates to organizational learning, with an increasing richness in detection, comprehension and use of precursors to anticipate crisis conditions and act in timely manner cannot be considered more than a hypothesis, still based on observations from different crisis sectors, mingling safety with security aspects, and not yet embedded in a generic theory of crisis management.

2. A methodological approach to awareness and precursors

To take a step on that direction (theory building) we remark that a collaborative methodology, known as Group Model Building (GMB) in combination with system dynamics (SD) modeling [13-18] has been employed to elicit fragmented domain expert knowledge, to unify it in terms of dynamic theories expressed by SD models, and to generate theories [18]. In recent years the methodology has been applied successfully to safety and security problems, including critical infrastructure protection (CIP) [19-25] Accordingly, we consider a GMB/SD approach to the awareness/precursors issue a promising one and the purpose of this paper is to report our observations and lessons learned within the framework of the SEMPOC project.

SEMPOC stands for Simulation Exercise to Manage POwer cut Crises, which will lead the alert reader to wonder as to whether the eclectic approach of combining clues from multiple sectors of safety, security and CIP is a methodological sound one. This caveat is legitimate. Notice, however, that the preliminary validity of our study is restricted to our having targeted and achieved a consensus within a representative group of interdisciplinary panel of domain experts (cf. Table 1) and being able to represent this consensus in a qualitative SD model (to be discussed below). Thus, this paper is work in progress, seeking fruitful discussion and criticism.

SEMPOC examines potential pan-European effects of a multi-national power outage. We develop SD simulation models that consider the effects of outages with varying severity. The purpose is to test and recommend policies to prepare for and mitigate damage, and improve recovery times in future crises. We hypothesize that reaching a satisfactory and effective preparation, mitigation, and response is dependent upon the perspective of the observer. Additionally, response planning must include the realities of political and social effects on the process and outcomes.

The SEMPOC project perspective goes beyond power engineering, in that a severely damaged grid strains other critical infrastructures, taxes social support, and disrupts public and private activities. We include explicit representation of soft variables, such as the coordination needed among organizations, as a means to understand the direct technical and sociopolitical aspects (e.g., pressure of media, public anxiety) on crisis perception, response and recovery.

This wide scope creates several challenges. First, the problem has overlapping action timeframes. Power companies react very quickly to an outage, attempting to restore power within hours or days of an outage. Building the organizational and technical capacity to detect and repair a multinational crisis may take years, however, as myriads of legal and engineering tasks are required in a region without standardization.

Second, this holistic view requires multi-disciplinary and international knowledge. Domain experts from European countries were invited to participate, bringing diverse different cultures, expertise and mental models to bear on the problem. Table 1 demonstrates the diversity of institutions and skills, including first responders, civil protection,
health care and critical infrastructure experts, along with power generation and distribution authorities.

Third, and as remarked in the introductory section, much of the experiential information about the causes and reactions to crises remains tacit and fragmented.

Table 1: Participating Organizations.

<table>
<thead>
<tr>
<th>Organization</th>
<th>Country</th>
</tr>
</thead>
<tbody>
<tr>
<td>National Operations Centre</td>
<td>Holland</td>
</tr>
<tr>
<td>Sjöland &amp; Thyselius (Energy consultants)</td>
<td>Sweden</td>
</tr>
<tr>
<td>Swedish Civil Contingencies Agency</td>
<td>Sweden</td>
</tr>
<tr>
<td>Red Eléctrica Española (REE) (Spanish Energy Company)</td>
<td>Spain</td>
</tr>
<tr>
<td>Gas Natural Fenosa (Spanish Energy Company)</td>
<td>Spain</td>
</tr>
<tr>
<td>Faculty of Criminal Justice and Security</td>
<td>Slovenia</td>
</tr>
<tr>
<td>Gjøvik University College</td>
<td>Norway</td>
</tr>
<tr>
<td>CNPIC (National Critical Infrastructure Protection Center)</td>
<td>Spain</td>
</tr>
<tr>
<td>Argonne National Laboratory</td>
<td>USA</td>
</tr>
<tr>
<td>Directorate for Civil Protection and Emergency Planning</td>
<td>Norway</td>
</tr>
<tr>
<td>Danish Emergency Management Agency (DEMA)</td>
<td>Denmark</td>
</tr>
<tr>
<td>SAMUR (Emergency and Rescue Service)</td>
<td>Spain</td>
</tr>
<tr>
<td>Eles (Slovenian Electric Company)</td>
<td>Slovenia</td>
</tr>
<tr>
<td>EPES (Public Emergency Health Organization)</td>
<td>Spain</td>
</tr>
</tbody>
</table>

The project design faced these challenges by adopting an iterative protocol which shifted the problem domain from regional to international concerns, and from short-term to long-term, by organizing three workshops over a period of 13 months following the methodology of GMB/SD. This paper reports about the observations and lesson learned during the third workshop – mainly from the point of view of the adequacy of the method to capture key insights about the awareness/precursors issue.

The SEMPOC project has been using a workshop structure that combines exercises for knowledge elicitation with hypothetical causal structure. During three two day GMB workshops, modelers work on the problem jointly with multidisciplinary domain experts. The modeling team’s main objective is to gather information needed to develop the simulation models ensuring that all sectors and mental models are considered. The workshop agenda includes several specific exercises that facilitate efficient information discussion and cooperation.

In between GMB workshops the data gathered, including the SD model sketches, are refined and expressed in terms of preliminary calibrated models that are further calibrated and validated using interviews with the same experts who contributed with their presence and activities during the GMB workshops. As to the content of this paper, we again remark that the observations and lesson learned are preliminary. The further elaboration with domain expert validation in the remainder of the SEMPOC project (finishing 1 April 2011) is still ahead. The constructive criticism that we hope this paper will elicit – from reviewers and, hopefully, from this conference’s participants – will be a valuable addition to the internal validation process.

3. Model building methodology: exercises to obtain dynamic insight

This section describes the collaborative exercises that we used during the third workshop to address the awareness/precursors issue. The inspiration for the exercises came from the sources described in section 1 “Introduction – Definition of needs”.

Each exercise has a similar pattern. Small group work within expert – modeler teams alternates with plenary discussion. When convergence on a subset of alternatives is desirable, a voting exercise or similar technique reduces the range of alternatives. In case of disagreement, the facilitator allots time for the necessary time to achieve consensus. (In rare cases, where disagreement remains, notes are made of the unresolved issue in order to gather additional insights in the post workshop phase, for so to resolve the issue.) In other cases, the contrast among the work of the teams is used to stimulate identification of patterns and areas of divergence. Modelers and experts periodically reflect on the system structure that emerges from the discussion. The exercises and results obtained are described in the following subsections.

3.1. Stakeholder analysis

One of the first activities in the workshop protocol is the identification of different stakeholders which are those agents affected or influenced by the problem. Experts identify the stakeholders, and then rank them by relative interest (motivation to solve the problem) and influence (the stakeholder’s impact on the problem or solution), while the "Interest" represented their motivation to solve the problem. When there are many agents to consider, the analytic focus rests on those who have both high interest and high impact.

Our experts identified a relatively large number of stakeholders (Fig. 2). The high-interest, high-influence are grouped into four sectors: power system, government, civil protection and first responders (Fig. 3). In some later exercises work teams were grouped according to their background and expertise in terms of these four sectors. In others, participant expertise was distributed to ensure that there was a rich flow of information among sector representatives.
Figure 3 Stakeholder map

Power System
- Energy companies
- Power plants
- Grid operators

Civil Protection
- Regional Civil Protection
- National Civil Protection
- International Civil Protection

Government
- Local government
- National government
- EU Government

First Responders
- Military
- Emergency services
- Police (law enforcement)
- First Responders (police, ambulances, fire brigades.)

Interest

Influence

Organized crime, terrorist, 3rd country attack, malicious agents

Media & Broadcast companies

Business sector

NGO, Climate activist

Utilities

Politicians and parties

Power plants and grids operators

Energy companies

National and local government

EU Government

Police (law enforcement)

Military

Citizens

Manufacturing Industry

Children, vulnerable group

Hospitals

Figure 2: Main sectors
Critical Infrastructure Protection requires crisis managers to understand the system vulnerabilities, the interaction among directly or indirectly involved sectors and how the decisions taken under stress situations may influence the length of a crisis. Regarding the power sector, current complexity of interconnected grids and cross border trade makes this sector particularly vulnerable to cascading outages due to terrorist attacks or technical failures. This fact, in addition to the severe consequences that a power outage might have on Society, forces crisis managers to develop proactive strategies that enhance the crisis managers’ awareness to predict that a crisis is going to occur.

Based on the awareness definition (Fig. 1), the goal of this exercise is to identify the most important leading indicators that may help to predict crises in the government, civil protection, first responders and power system sectors. It is also required to explain how these indicators may be perceived, comprehended and projected to anticipate the crisis.

For the power system sector, the experts agreed on two crisis leading indicators as most important. First: the redundant power load capacity of the power system. Power load (demand) and power production must be kept in equilibrium or there will be severe frequency and voltage disruptions which ultimately cause blackouts. Redundant capacity allows substituting equipment if it is unexpectedly brought off line. A lower degree of redundancy reduces the power system’s ability to handle unexpected occurrences which may cause outages. Second: the environmental conditions detected by weather forecasts, so that consequences can be diminished by defining preventive measures.

The indicators proposed by the government sector were the number of engineering students and trust in the government. The first indicator detected by statistics would influence the future number of power engineers. Therefore it is necessary to motivate students using awards to increase the enrolment. The trust in government can be measured by media reports, complains and interviews with focus groups. It is necessary that the governments not only base their decision on the technical details of an incident but also on the soft factors, such as social resilience.

The civil protection group also identified the weather conditions as a leading indicator. The second proposed leading indicator was the type of threat detected and interpreted by intelligence agencies, which impact can be diminished by contingency plans.

For the first-responders sector, the media coverage of certain incident was considered a reliable indicator, measured by the number of received phone calls. The season of the year is also important since in some periods the demand of these services increases considerably. In both cases, it is necessary to develop a plan in advance, in order to anticipate the crisis.

3.3. Identification of awareness barriers

The crisis manager’s awareness may influence the severity of future crises. For instance a high level of awareness can make managers act proactively in order to diminish the impact of an outage. However, the ignorance of incidents in the system can lead to high severity consequences.

In this exercise the experts were asked to identify the barriers that limit awareness levels and may influence crisis management.

Some of the barriers that the civil protection group detected were divergent information interpretation and lack of economical funding. The first one was referred to the different information obtained through different information sources; thus the managers need to interpret the information and decide which one is relevant. The second depended on available resources for crisis managers to develop planning and exercises.

The power sector’s barriers have much to do with the quality and quantity of the information they have and the lack of experts in this area.

The government sector identified their barriers with competing interests that politicians can have when deciding where deploy their resources, and with long time delays that occur between the decision makers and outcomes.

Incorrect managing of the information and news and the lack of resources and skills were the most important limitations for the first-responder’s group.

3.4. Identification of dynamic stories

In the next exercise domain experts were divided in three groups, mixing people from different sectors. They were asked, based on their experience and intuition, to think of dynamic stories about detecting events relating to leading crisis indicators and how over time different levels of awareness affect the system. A very long time horizon was presupposed.

As the ability to detect precursors could prevent or lessen the occurrence of a crisis, what would happen if we do not have the ability to detect those precursors well? What about if we detect them but we are not able to act very well? And, what if we detect them and have the ability to act?

In order to analyze these alternatives three different scenarios over a 20 year long period were presented (Fig. 4). The first scenario was called “No detection”
and it represented a situation where many events were taking place but none of them were detected, so that as a consequence two crises occurred. The second scenario named “Poor detection & limited resolution” showed that some of the occurred events were detected, so that crisis managers acted upon them consequently and one of the two crises was avoided. In the third scenario, “Detection & resolution”, most of the events were detected and managers acted upon them, preventing both crises to occur.

In addition, the number of events happening was reduced in the last two scenarios compared to the events occurred in the first one. When events are detected and managers act upon them in order to improve system resilience, some future events can be prevented.

In addition, the number of events happening was reduced in the last two scenarios compared to the events occurred in the first one. When events are detected and managers act upon them in order to improve system resilience, some future events can be prevented.

Then, experts proposed some indicators that could be consolidated between the stories to analyze the different measures that influence the system’s behavior. To decide which of the identified measures were more relevant a voting exercise was carried out. Each of the three expert groups could allocate a total of four votes. The voted measures were quality of crisis management, number of detected incidents, quality of infrastructures design, level of regulation, perception of risk, and budget for crisis management.

The most voted set of indicators (excluding budget for crisis management, which on reflection was deemed being less significant) were used as inputs for this exercise, which consisted of drawing their evolution over time. Experts relied on their experience and intuition in the three mentioned scenarios, considering also relevant units to measure the indicators.

Fig. 6 depicts an example of a behavior over time graph. The experts evaluated the level of crisis management on the quality of planning conducted. The dotted line correspond to the “no detection” scenario, the solid line corresponds to the “poor detection and limited resolution” scenario, and the dashed line corresponds to the “detection and resolution” scenario.

The information gathered during this exercise is a key input for the simulation model development, as the model should reproduce these behavior modes.

### 3.6. Identification of policies

The second day of the workshop considered which managerial policies might be available to help move away from outage-driven change and become more aware of the potential for failure.

The first group proposed to form a workgroup in cooperation with public and private companies to carry out formal strategic meetings. This policy was focused on preparedness, safety and security before the crisis, identifying responsibilities and different goals. The consequences derived from this approach in the long term had much to do with the financial agreements and consensus in operations between private and public organizations whereas in the short term political agreements, information exchange and sector’s efficiency improvement were the detected ones.

National action plan for civil emergency management was the policy identified by the second group. The barriers that can limit the good operation were funding needed, lack of experts in this area and shortage of resources. Risk and vulnerabilities analysis, improvement in the planning, regulatory
issues and international coordination exercises would be the long-term consequences. In the short-term more funding to finance the plans and more commitment in the education around those topics would be achieved.

The last group proposed improving the planning and crisis exercises to get a better response when an outage occurs. Not only public organizations but also private organizations should bear the cost of responding to outages. This policy was expected to lead to a better response, less critical situations and higher awareness.

This information is very useful for the modeling team in order to know how the final simulation model should behave when implementing some policies.

4. Qualitative modeling

This section describes model sketches that were derived during the workshop.

4.1. System weaknesses and indicators

Power outages do not happen out of the blue (although it can seem so for those affected). They are caused by the presence of weaknesses (technical and organizational) in the power grid, some known, and some unknown. If the system is not robust enough, these weaknesses may trigger outages. In Fig. 7 we have modeled lack of system robustness as a stock of system weaknesses. A weakness can be insufficient attention to maintenance of equipment or ignoring the use of weather forecasts to predict how resources should be prepositioned when a thunderstorm approaches.

Weaknesses in the system may be addressed, given the resources and skills to interpret the current state and anticipate possible problems. An outage can be investigated to detect system conditions that need to be avoided. We call these signs of system conditions indicators. Thus, if one is able to detect relevant indicators, understand what they mean for the system’s behavior and use them to anticipate future consequences, weaknesses can be mitigated or removed entirely from the system as one knows the specific weaknesses that caused the outage. In the figure this is represented as the balancing loop B1a–
number of remaining weaknesses, reducing the probability of a future outage.

Although the first two stages of the awareness ladder likely cause some reduction in vulnerability, attainment of the final stage, projection, is needed for full effect. Projection means that an indicator is actively used to manage the system, thus constituting a form of double loop learning, as the governing values of how the system should be managed has changed by the adoption of the indicator and process of understanding its meaning. Single loop learning occurs within the context of change in an indicator, which prompts adjustment to compensate, but the meaning of the indicator is not challenged.

Fortunately, multi-national outages are relatively infrequent, but not unknown, viz. the 2003 power outage that struck Italy but started outside its borders [26]. The consequence is that one must wait a long time to learn about potential weaknesses in the system from outages alone, and it is problematic that such learning happens after the fact. Ideally, weaknesses should be identified and removed before they can cause outages. The industrial accident literature describes many kinds of events that precede true accidents, and we wish to draw a parallel from these works to the power grid. Events are often caused by the same conditions as accidents, but because not all the right conditions for an accident were there, instead became less serious happenings. Thus, events and accidents are both signs of the same underlying system weakness. Applying this concept to the power grid, analysis of the Italian outage in 2003 indicates that the same is likely to be the case for power outages. There were events that preceded the outage but were not seen as indicators of problems. If one could detect these events one could potentially remove the weaknesses before they cause serious outages with high costs to Society and the individual company. This is represented in the model as the balancing loop B1b – Event mitigation.

Ideally, one would be able to analyze the system in advance and remove weaknesses before they even cause precursor events. This is indicated in the model by the loop B1c – Latent Weakness Mitigation. However, it is very hard to detect dangerous conditions in a complex system in advance. It presumably requires considerable experience, analytical capability and resources, all of which are in short supply.

We assume that disruptions (events) happen more often than real outages and the weaknesses are always there until they are removed. The loops B1b and B1c will thus give feedback about the state of the system more rapidly than the B1a loop. Power grid activity work with events and, we hope, proactive problem detection will clear system weaknesses without the cost of outages. The task of improving robustness is moving the system from B1a to B1b, and to B1c.

We have an a priori belief that experience with using indicators will improve the ability of the power grid to detect and apply them. Each detected, understood and adopted indicator adds to the organization’s experience base, which helps improve detection, understanding and adaptation of indicators to manage system weaknesses. This is represented by the three loops R1a, R1b and R1c.

Learning to improve is important, owing to the significant amount of noise that must be filtered out. Modern power systems are extremely complex because of the large scale of these systems, their technical variety and large amount of organizations that are involved. Information overload is likely to be a factor which contributes to reduce the rate at which indicators are detected, understood and adopted for management of the system. This is represented in the model by the three variables complexity to detect, complexity to understand and complexity to adopt.

4.2. Policies

![Figure 8 Model sketch linking policies to indicators and system weaknesses](image)

Fig. 8 links policies (such as described in section 3.6) to the weaknesses and indicators of the previous figure. Outages (and to some extent events) draw attention from decision makers. This shift of attention, while competing with other demands, will likely increase resources for the grid. One common policy after a serious outage is to deploy resources to reduce weaknesses (B2). If resources are applied to improving the capacity to evaluate, new indicators may be found which can be used to detect and work with events (B3 – Identifying needed indicators). The lessons learned loop (R2) improves our use of indicators, as the
experience and the capacity we develop to evaluate indicators improving our ability to use them.

Relying on outages alone to trigger resources and attention at a pan-European level is a risky venture, as the level of the outage would need to be quite severe. Our assembled experts believed that an additional set of policies that addressed the institutional barriers faced in managing large-scale crises would greatly affect the robustness of the system without waiting for a crisis to occur. Institutional cooperation improves the relationship among organizations which allows for a better response and to reduce system weaknesses (loop R4). This cooperation would not be possible without information sharing, which necessarily involves reciprocal trust (loop R3). A failure to develop such trust could also create a trust trap, where a lack of shared information makes future sharing even more difficult.

5. Observations and lessons learned

The exercises for the GMB workshop synthesized materials eclectically from the areas of safety, security and CIP. The domain experts could through discussions, participation in exercises, and constructive criticism modify, or even eliminate, concepts and constructs. The first observation is that this did not happen: Domain experts adopted the framework of the awareness ladder, which has been proposed in the context of information security [27]. Also, they did not challenge the main conclusion from the study of accidents in the Dutch petrochemical industry [7] that crises always develop along observable and observed disruptions (precursors that would serve as leading indicators).

The outcome of the exercises – as expressed in model sketches – are consistent with processes of double loop learning, where feedback from perceived, comprehended and “projected” leading indicators act to eliminate system weaknesses, that is, to prevent or mitigate crises. However, it is not a given that double loop learning occurs. An outage which is followed by an investigation, recommendations for improvement, and their subsequent implementation only leads to double loop learning if governing values are examined and questioned. In this case there are two possibilities for double loop learning: The first is if detection and examination of an indicator reveals fundamental deficiencies in the way the system is governed. The second is critically examining the method that is used to improve awareness, i.e., the detection, understanding and projection processes.

As stated previously, “awareness” and “precursors” are concepts that can be defined and understood in different ways. The GMB workshop arguably provided a sharper definition and understanding of these concepts, as explicit levels and metrics were agreed upon. Workshop participants achieved consensus that the stakeholders can have different values for their awareness concerning large pan-European crises, and that the value of each stakeholder’s awareness can influence other stakeholders’ awareness.

There is a close relation between awareness and precursors. Awareness determines not only the capacity of stakeholders to detect precursors but also the probability of a precursor taking place, as awareness improves prevention. This means that the evolution of awareness can behave through different patterns depending on several parameters, such as, the influence of precursors’ detection on awareness increase, the influence of awareness on precursors' detection capacity or the influence of awareness on prevention and precursor’s amount.

Our paper is work in progress. We look forward to a discussion of our observations and lessons learnt that promotes engagement and constructive criticism.

Acknowledgment

We are grateful to the European Programme of Critical Infrastructure Protection (EPCIP) and the European Commission, Directorate-General Justice, Freedom and Security for funding the SEMPOC project.

This manuscript has been created in part by UChicago Argonne, LLC, Operator of Argonne National Laboratory (“Argonne”). Argonne, a U.S. Department of Energy Office of Science laboratory, is operated under Contract No. DE-AC02-06CH11357. The U.S. Government retains for itself, and others acting on its behalf, a paid-up nonexclusive, irrevocable worldwide license in said article to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the Government.

10. References


12. Puhakainen, P., *A design theory for information security awareness*, in Faculty of science, department of information processing science. 2006, University of Oulu: Oulu, Finland.


