Towards Holistic Security Ecosystems
- Invited Keynote Paper-

Mihaela Ulieru
Canada Research Chair
http://www.cs.unb.ca/~ulieru/

***Abstract*-We introduce the concept of Holistic Security Ecosystem as an overarching operational layer enabling the deployment of dynamic, short living emergency response organizations capable of reacting quickly to emerging crisis situations. Based on a trusted overall operational picture shared via a reliable communications backbone, across a *holistic security ecosystem* harmonious inter-organizational coordination achieves a total effect greater than the sum of the individual parts. The realization is rooted in our Adaptive Risk Management platform for the analysis of interdependent systems and organisations via an operational picture of correlated collective dynamics - supporting strategic thinking and organisational leadership in a wide range of complex operations that go beyond the emergency response into trend analysis in global markets and enterprise dynamics for business operations.**

Keywords. Adaptive risk management, multi-agent systems, complex adaptive systems, inter-organizational coordination, emergency response operations, disaster resilience

I. Introduction – The Research Problem

To be able to effectively respond to the emerging threat environment first responders must develop better integration, cooperation and coordination mechanisms in order to work more effectively with other governmental and non-governmental actors. Management of the interactions between these organizations has to undertake multifaceted challenges (cultural, professional, coopetition, trust in a new temporary authority, etc). It is generally the intent of each partnering organization to retain their autonomy while "joining forces" to achieve shared goals. The resulting tensions between autonomy and partnering lead to ambiguity and complexity in the meta-organizational (i.e. the collective set of entity organizations and interrelationships) structure or form. These tensions must be reconciled in order to achieve both individual and shared objectives. Participants are pushed into activities that are beyond traditional areas of competence and they are stressed when encouraged simultaneously to build inter-organizational linkages and to protect organizational autonomy. In these instances, both cooperative and competitive behaviour will likely be observed.

The persistence of coordination as a problem in operations indicates a deeper issue than merely the need to coordinate tasks, which relates to the nature of the relationships amongst entities within a meta-organization and whether or not the set of relationships and consequent meta-organizational form promotes or hinders collective decision-making. Response shall encompass harmonious inter-organizational coordination that will enable the meta-organization responding to the crisis to achieve a total effect greater than the sum of the individual parts. This calls for a more holistic approach to IT-enabled emergency response operations, in which IT (information technology) encompasses the physical artefacts as well as the social relations emerging around those artefacts which connect first responders and citizens involved during response to crises.

To address this we propose an integrated security framework supporting the timely creation of cross-organizational operational units in addressing emerging threats through improving communications capabilities, and enhancing threat awareness and intelligence assessment capabilities (Ulieru 2008). We call this framework a holistic security ecosystem (Ulieru 2007a).

II. A Holistic Approach To Emergency Response Operations

The approach expands our previous work on the holonic enterprise and emergency response holarchy concepts and implementation experience (Ulieru and Unland 2004a), (Tognalli and Ulieru 2005) to bring together psycho-social, cultural and professional factors into a unified robustly networked security meta-organization model. Holistic security ecosystems (HSE) are rooted in the concept of emergency response holarchy, Fig. 1 as a meta-organizational structure deployed 'on the fly' from dispersed resources to address a dynamically evolving unexpected situation. In an emergency response holarchy, the C2 backbone, Fig. 2, mobilizes and deploys units of first responders around specific tasks as they dynamically emerge in the chaos of crisis (Ulieru 2008).

Based on latest communication and networking technologies we proposed and implemented (Tognalli and Ulieru 2005) a multi-agent based implementation for the C2 backbone of an emergency response holarchy – which uses FIPA (Foundation for Intelligent Physical Agents) standards, Fig. 3 to define the interoperation of the holons at various levels of resolution. We further developed an adaptive risk management approach to emergency response operations (Ulieru and Worthington 2005) – which enables threat anticipation and co-evolution of the emergency response holarchy with the evolving crisis at hand. To capture the emergent behavior induced by the hybrid nature of the information exchange and psycho-social cultural and professional factors across a holonic meta-organization, we recently proposed a complex systems approach to the deployment of HSEs (Ulieru 2007a) as mechanism capturing the cross-organizational dynamics while balancing autonomy of individual entities with the drive towards cooperation to achieve common goals. Organizations in an HSE are characterized by:

- the participants' ability to negotiate between autonomy and cooperation in a drive (attractor) towards a common goal
- a coordinated workflow process that triggers the formation of high-level organizational structure (patterns of collaborative clusters) through low-level interactions between participants
- a capacity to organize over spatial and functional scale to maintain resilience against attack.

To seamlessly deploy the first responder meta-organization (aka the HSE) as a 'crisis controller' (Fig. 4) we recently proposed an original implementation of the emergent engineering paradigm (Ulieru and Doursat 2008). The idea (Ulieru 2008) is to capture the collective behavior resulted when simple individuals (at the atomic holon level – Fig 1) are interacting locally with one another and with their environment without centralized control. Such systems can be modeled using the Agent-Based Modeling and Simulation

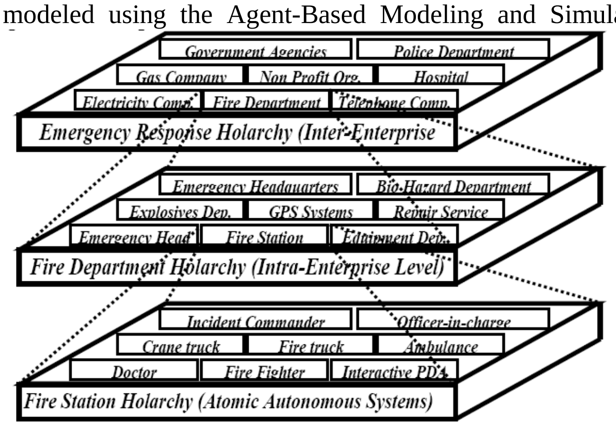

Fig. 1. Emergency Response Holarchy

(ABMS) paradigm (North and Macal 2007) with each individual modeled as an agent and their interactions modeled as links. Such a simulation model for a first responder meta-organization deployed to contain an evolving crisis (Fig. 1) equates a network of agents, Fig. 2, interacting intensely with each-other in generating a collective behavior that co-evolves with the environmental dynamics of the crisis at hand. The collective behavior emerging from the 'bottom-up' individual interactions is elastically constrained by the C2 backbone coordinating 'top-down' the holonic structure (Fig. 1) The C2 backbone (Fig. 2) constrains the overall network of first responder agents – to follow the higher strategy, a high-level policy crafted by the command centre enabling the undertaking of concrete action plans.

The SOS Network paradigm (Ulieru 2008) aims to enable the flexible adaptation of the top-down (mostly rigid) policies to the crisis dynamics to accommodate the 'bottom-up' emergence of groupings of hybrid resources (individuals from various organizations working together and their tools) to respond to the unexpected dynamics occurring 'in the field'. The high-level policies of the HSE meta-organization (termed in our approach overall rules of the network) will thus materialize into flexible concrete action plans that are

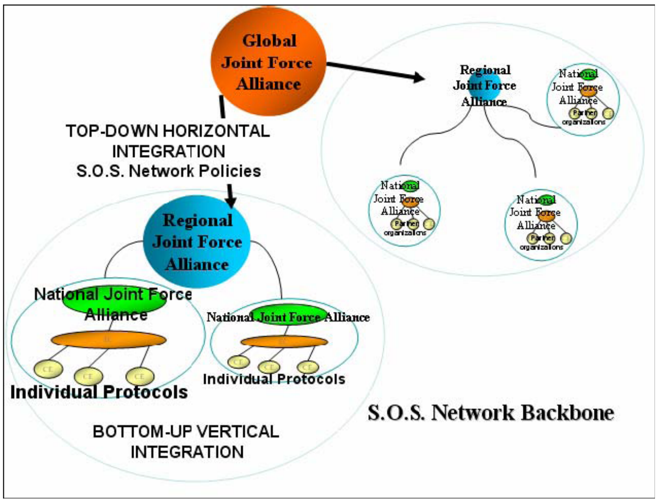

Fig. 2. C2 backbone of an ERH

broadcast on the fly and distributed ('compiled') top-down into local rules (individual protocols) transmitted to the agents involved in addressing the particular complex situation. The individual-to-collective dynamics (how the agents create the collective behavior through the way they interact/influence each-other) in such a network depends on the particular action plan most suitable to addresses the situation at hand.

III. Approach To Modeling Holistic Security Ecosystems

A. *Balancing top-down organizational policies with bottom-up individual protocols*

The biggest challenge in undertaking such a holistic approach to security systems dynamics is the need to balance these two opposites - 'top down' command and control with the 'bottom-up' emergent collective behavior - which ultimately translates into balancing the autonomy of subordinates with the excessive power of commanders. Our approach aims to implement HSE meta-organizations as holarchies (Fig. 1) with a highly adaptive Command and Control (C2) backbone Fig. 2. The solution we propose exploits the latest advances in communication networks and services to enable cross-border (organizational, political, national and geographical) productive collaboration in dealing with acute and developing crisis situations. The overall holonic meta-organization policy is implemented

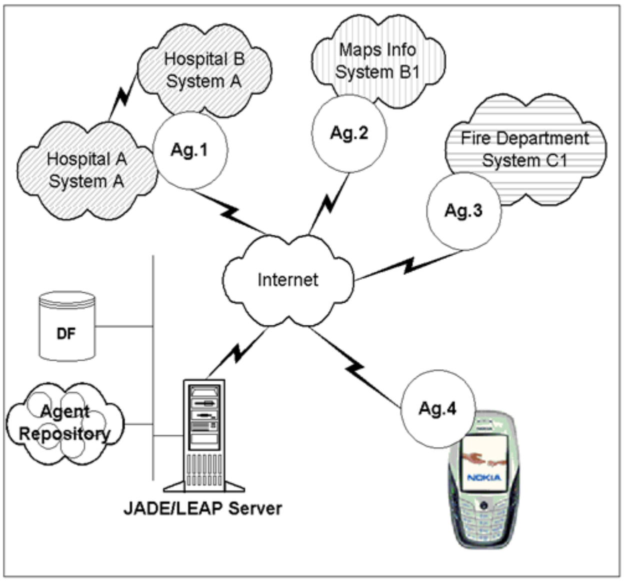

Fig. 3. FIPA-enabled C2 Structure

using a multi-agent software middleware platform that enables the coordination of inter-organizational interactions via remote process execution and management. The C2 coordination mechanism separates process from execution, acting in the background according to the governance rules of the meta-organization – while the individuals coming together from their specific military and civilian units are following their own specific protocols in a goal-seeking self-organizing swarm. It is the balance between the rules at the microscopic level of the agents (their individual protocols) and the overall macroscopic behavior of the collectivity (the dynamic meta-organization mediating the top-down policies across all organizations that are hosts for the deployed individual agents to create action plans appropriate for managing the particular situation) that guides the emergence of appropriate action plans for dealing with the crisis most effectively. Relatively complex behavior can therefore result from balancing the individual protocols – the simple agent-based rules that encode positive feedback - with the overall rules of the system that result in the adaptive action plans - by adjusting the individual behavior to the overall goal of the network of agents via negative feedback. This equates with balancing autonomy of the individual agents with the need to cooperate to achieve the overall goal of the system, in a holonic enterprise (Ulieru and Unland 2004b).

The HSE meta-organization approach is about how first responders use communication networks and information to conduct and to support operations, in the most effective

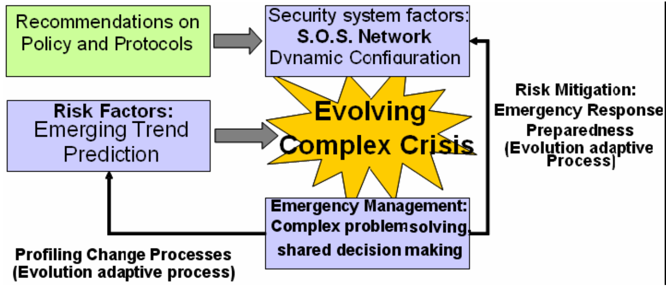

Fig. 4. HSE as Crisis Controller

manner. Given the nature of complex issues with the centrality of human factors, the problem has significant multidisciplinary dimensions. The HSE concept spans across four domains: information, cognitive, social and physical. The information domain is where knowledge becomes codified, manipulated and shared. The cognitive domain is internal to people and is where perceptions, awareness, beliefs and values reside. It is also where mental models (Dietrich et al 2008) are created and decisions are made as the result of internal processes. The social domain is where individuals interact with others. Finally, the physical domain is where operations take place across different environments during the crisis situation.

The HSE Framework is envisioned to run on a Testbed, Fig 5 that encompasses all these domains. The physical domain is encapsulated as geographical capacity while the information, cognitive and social domains are merged into intellectual capacity. The geographical and intellectual capacities represent the organization and its partners as a network.

B. Bottom-up clustering of resources via emergent engineering

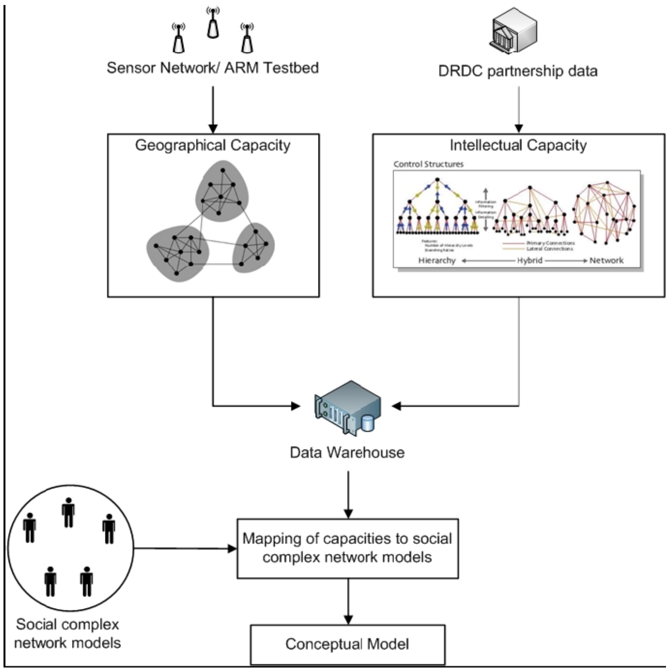

Fig. 5. HSE Simulation Testbed

The **geographical capacity** of the meta-organization addresses *which* resources ("partners") are located *where* at any given time. On our testbed the geographical placement of organizational partners is realized through a Wireless Sensor Network, where every sensor represents the location of a collaborative partner. In a spatially explicit environment, the agents have a location in geometric space. To illustrate how we plan to investigate the geographical capacity and the emergent behavior through 'bottom-up' clustering of resources within the meta-organization consider the example of a stadium in which a terrorist attack unfolds (Ulieru 2008). For this example, Fig. 6, an important part of the network of agents is essentially spatial, and most of the intervention efforts must be focused on *placing* people, units, vehicles, equipment where they are needed to form effective *functional patterns*. During the evacuation of a stadium, space could be partitioned e.g. into different sectors organized around the nearest exits and the center of the field to direct the flow of the crowd most effectively. Military or law-enforcement personnel could form human chains and security cordons in complex but targeted branching structures serving multiple purposes: encircling the scene of a threat or accident, guiding people toward the exits, transporting victims to emergency vehicles, and building specific local formations such as enclosed areas containing equipment or medical field units (rectangle in Figure 6) (Doursat and Ulieru 2008).

The emergent engineering capability of our testbed can grow barriers to attacks that co-evolve with the crisis dynamics as per Fig. 7, where e.g. a cordon of first responders evolved to isolate a threat while two chains of first responders emerged to surround and isolate the suspects as well as to guide the crowds to safety.

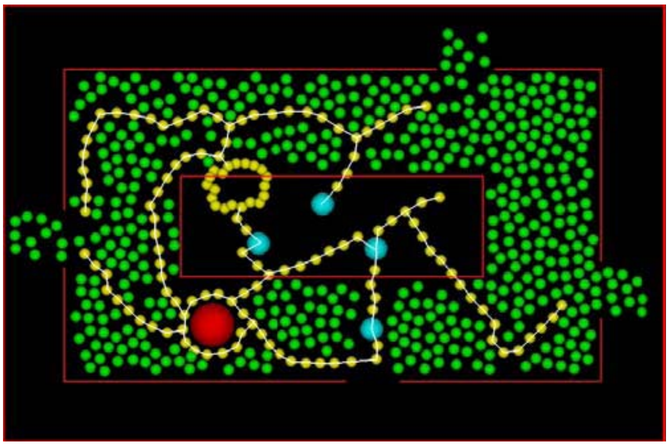

Fig. 6. Schematic view (not a simulation) of a possible SOS scenario within the space of a stadium, that would combine programmed networking and dynamic interaction with the environment. Growing cordons of security agents (orange) encircle the threat (red), guide the crowd (green) toward the exits, carry victims to emergency vehicles (blue, driving in and out through gates under the bleachers), and create special enclosed spaces on the field (cycle).

The emergent engineering capability enables specification of the meta-organization functionality to be relaxed to the point of being able to cope with 'surprise attacks' by harvesting the most appropriate <meta-organization structure> / <type of crisis to control> pairs from a free-range "menagerie" of <protocols>/<action plans> configurations. Dynamical adaptation to an evolving crisis basically happens at two levels: (a) quick adaptation to local circumstances at the level of the human agents (collision avoidance, common sense reactions, etc.) *under the same rules of deployment*, and (b) major changes of strategy at the command level that *change the rules of deployment*. High-level C2 action plans would set only the global course of the action, based on symbolic codenames ("raid", "evacuation", "withdrawal", etc.), while the low-level implementation details are carried out by individual agent protocols (real-time positioning). Action plans are compiled into local rules for joining the meta-organization and broadcast to all agents. Thus, the network can adapt to new incidents and episodes of an evolving crisis by reprogramming the agents on the fly to create new formations (Doursat and Ulieru 2008).

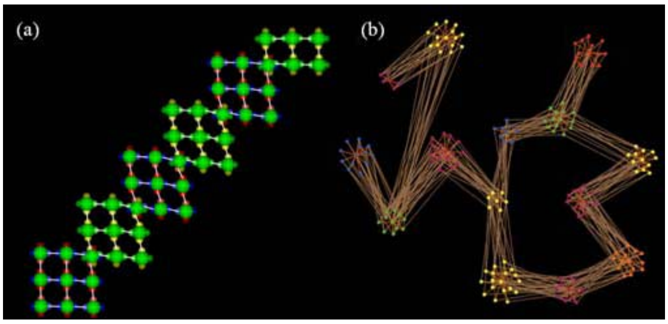

Fig. 7. Growing Barriers to Attacks Via Emergent Engineering

C. *Top-down coordination of response by mediating inter-organizational policies*

The **intellectual capacity** of the organization consists of the specialized skills available through different partners in the organization coming together into a collective response. In a spatially implicit environment, the location of agents is irrelevant, yet retrieving timely the appropriate information and knowledge is of the essence. To create the intellectual capacity of the meta-organization we are using complex network models ranging from statistical physics to natural web foods and social networks (Grobbelaar and Ulieru 2007) (Doursat and Ulieru 2008). To illustrate our capacity to simulate the intellectual capacity, consider the top-down coordination of response during a state of emergency which involves many agencies within all levels of government and first responder organizations (firefighters, police, ambulance service, hospitals). Consider a chemical fire taking place on a foreign vessel anchored in e.g. a Canadian harbor. In this case, additional agencies such as; Transport Canada and PSEPC (Public Safety and Emergency Preparedness Canada) are likely to get involved. Data from multiple national sources such as; fire, EOC, RCMP, Transport Canada is mined and integrated into an online dynamic knowledge repository (the 'data warehouse' in Fig. 5). Assume for example that the fire is on-board a vessel which has hazardous chemicals in its cargo and the situation escalates after an explosion occurs resulting in a plume drifting towards a densely populated area. In this case the firefighting and police response will need to adjust/adapt accordingly. The Testbed provides a decision support capability which can monitor the events unfolding on the ship-borne fire to predict necessary response for firefighters and police assets. Through simulations, data from existing social and other complex networks are being matched with the HSE model to investigate the strengths and resilience of various meta-organizational configurations, thus determining their suitability to address various crisis models. This enables us to map various HSE configurations to various crisis types for which the particular meta-organizational structure works best. Validation of resulted HSE configuration on 'in-vivo' simulation exercises for various instantiations of scenarios provides essential feedback for the model improvement.

IV. Implementation

A. *Overview of the simulation environment*

Using the facilities available in the Adaptive Risk Management (ARM) Lab (Ulieru et al 2006), which target the command and control operational backbone of emergency response operations we have created a simulation environment for an overarching HSE Framework to enable experimentation and understanding of the high-level effects at the meta-organizational level as they emerge from local interactions among participants within and across organizations. The generic methodology is rooted in our (ARM) research platform, Fig. 8 (Ulieru and Grobbelaar 2007) for the analysis of interdependent systems and organizations via an operational picture of correlated collective dynamics, which involves:

- gathering of application-specific resource data (in our case data about the particular disaster and how it was addressed by the respective collaborative meta-organization);
- developing models and solutions for the management and engineering of complex situations using inspiration from Complex Adaptive Systems (Holland 1998);
- making sense of the data by processing it on the ARM testbed using our models (as described in the next section).

The ARM Lab hosts an integrated research platform (Fig. 8) consisting of distributed static and mobile computing devices integrated into a hybrid opportunistic communication network (part C of Fig. 8) which includes: Local Area Network of various desktops and laptops, Wireless Mesh Network based on Avaya-AP7 Routers, mobile devices (PDA and cellular phones of various makes to push the interoperability issue beyond existing boundary solutions), and wireless sensor networks with 25 nodes (Crossbow). This powerful communication infrastructure is animated by a secure intelligent middleware solution (part D of Fig. 8) on which various complex adaptive systems models (Part F in Fig. 8) are matched with real-life applications (Part E of Fig. 8) to enable the analysis of interdependent systems and organizations via an operational picture of correlated collective dynamics.

The Modeling and Simulations Module of the ARM

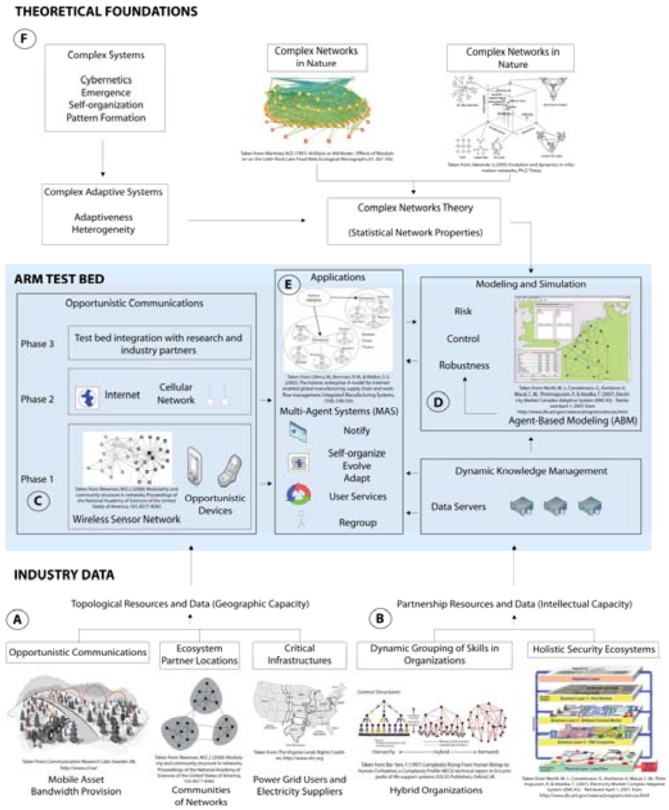

Fig. 8. Adaptive Risk Management Research Platform

research platform (marked D in Fig. 8) embraces the top-down command and control level and the bottom-up atomic holon interaction level of a holonic enterprise via powerful software which supports the implementation of the Multi-Agent Systems (MAS) paradigm (for the top-down modeling of extended enterprises and their interdependencies) together with software which supports the modeling and simulation of peer production and emergent clustering at the atomic holon level, based on the Agent-Based Modeling (ABM) paradigm (as described in the previous section). The ability to simulate individual actions of diverse agents and measure the resulting system behavior provides us with a unique tool for studying the effects on processes that operate on multiple operational scales and organizational levels. To implement the MAS paradigm we follow the FIPA standards and infrastructures (www.fipa.org) and use Java Agent Development Environment (JADE) (Bellifemine 2001), based on its performance, robustness and number of existing applications, which include CoMMA (Gandon et al 2002), a JADE implementation for managing organizations by facilitating the creation, transmission and reuse of knowledge in the organization intranet. This gives our applications the ready-made pieces of functionality and abstract interfaces for application-dependent tasks.

From the perspective of emergency response operations (Ulieru et al 2006) the ARM platform supports capabilities that enhance the Command & Control of a coordinated response during a catastrophic event such as: collaborative planning, directing, coordinating, and controlling of inter-agency operations on the ground. Across an emergency response holarchy, the ARM platform acts as a secure, intelligent middleware enabling an information centric operations approach which allows for tremendous horizontal and vertical scaling. Two powerful software platforms support the top-down operational level of the ARM platform: ARTIS M3Data (www.artisnet.com), which is deployed as the secure, intelligent middle-ware solution and RightsEnforcer (www.rightsmarket.com) deployed as the "every time, everywhere" document and email security solution. The M3Data software enhances situational awareness within an emergency operations environment by providing contextually based access to information from multiple disparate data sources. Information is shared securely between multiple agency repositories and combined into a common knowledge warehouse as foundation for the display of an Integrated Intelligence Picture (Fig. 9) as a decision aid during consequence management activities with capability for displaying entities within a given area of interest. For example, the location of 911 callers, hospitals, sensors (e.g. tracking field personnel and/or resources) etc. can be displayed. Users can then drill-down into these items of interest to access related knowledge which has been correlated across multiple repository types. M3Data enables compliance for strict inter-agency information sharing agreements shaped by privacy and security needs. These disparate information sources are combined and related using various M3Data libraries. The RightsEnforcer product suite works in conjunction with M3Data security model to provide enhanced "every time, everywhere" protection. It can grant and revoke access even after the information has been distributed and used by legitimate users. RightsEnforcer integrates seamlessly with standard email tools (such as Microsoft Outlook and Lotus Notes) to provide persistent email and attachments protection with minimal impact on user workflow.

For the implementation of the emergent engineering paradigm the ARM platform is supported by Fluidix - a particle-based physics simulation package distributed by OneZero Software (www.onezero.ca) which is typically used to model large scale particle interaction in complex systems such as fluid dynamics as well as emergence mesoscale phenomena in biological systems pertaining to the holonic paradigm http://www.onezero.ca/fpm_apps.htm) (Ulieru and Doursat 2009). The mock-up scenario (Fig. 6) and the real simulation presented in Fig. 7 were realized using this software. To the best of our knowledge, the parallel processing platform on which Fluidix runs is the fastest available platform for modeling large numbers of locally-interacting entities within a dynamic 3D physical environment - thus it perfectly serves our purpose of modeling large scale interactions among the participants in a meta-organization at the lowest (atomic) level, where the various entities (holons, which can be any kind of resource: people, devices, tools, machines, etc) from each participating organization come together to address the particular need (crisis at hand).

B. *Unique capability offered by our ARM lab*

Above all – what makes the ARM platform unique is its ability to blend the top-down modeling of organizational structures (institutions) as holarchies with the bottom up emergence of agent coalitions (clustering around a common purpose / task at hand) within the dynamic meta-organization created to address the evolving crisis. The combination of ARTIS and Fluidix brings unique abilities in modeling the complex interdependent dynamics arising from the (clashing)

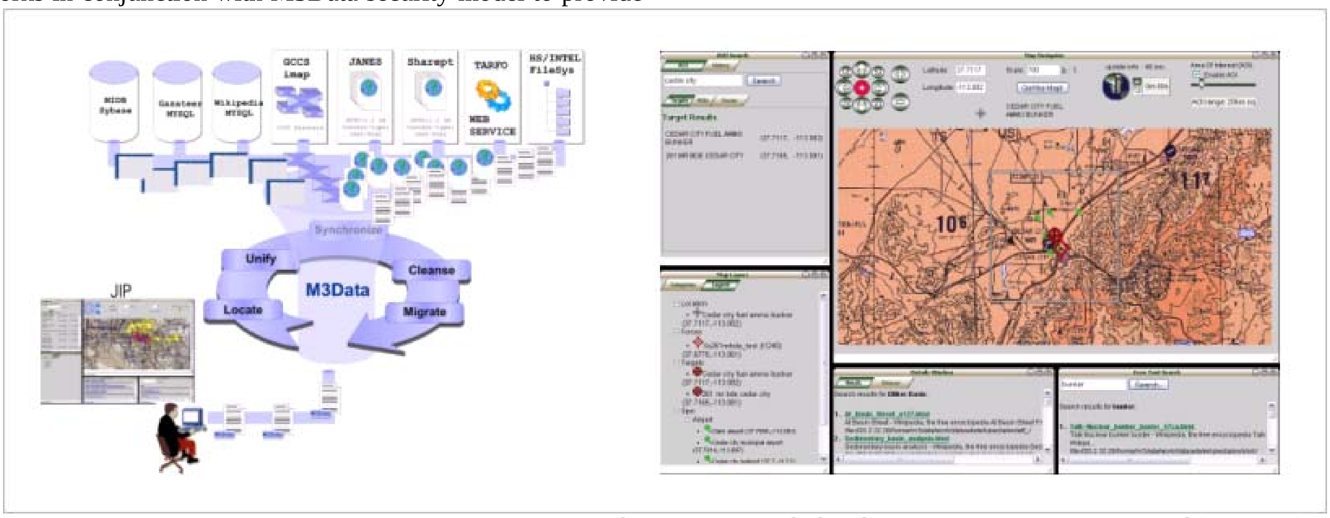

Fig. 9. Integrated Intelligence Picture Capability of the ARM Lab

inter-organizational policies and individual agent protocols coming together in hybrid teams. The ARM platform makes the modeling of interactions between large and small holons at the inter- and intra- organizational levels of a holarchy be as seamless and consistent as possible. The main capabilities that single out the ARM platform in implementing emergent engineering applications are:

- Ability to encapsulate generic individual attributes and protocols of any kind of atomic resource while seamlessly connecting into the scaling at higher levels of the meta-organization dynamically brought together to address the problem.

- Capability for modeling and synchronizing interactions and communication between a large number of agents within a parallel processing software environment.

- Capability to emulate how humans take actions via a bionic decision making process based on our research on emulating the mind (Dietrich et al 2008).

- Capability to balance the degree of realism required with efficient computational techniques to accommodate the thousands of agents simultaneously within the simulation.

- Enhanced Situational Awareness – providing an integrated view of high quality, contextual information to support decision making by combining relevant information from multiple disparate sources into an integrated picture.

- Information Sharing / Dissemination – supporting intra/inter agency information sharing and service composition through secure access to relevant information that is stored in multiple disparate repositories.

- Decision Support Capabilities – applying advanced knowledge management techniques to analyze a diverse set of data to predict outcomes, make recommendations, provide notifications / warnings or automatically take certain actions.

- Logistics Management - applying dynamic knowledge management techniques to analyze a diverse set of data to optimize the utilization and distribution of assets.

- Persistently secure documents and email messages – enable protection, control of access operations, and tracking, wherever the document or email goes, every time someone attempts to use it, thus endlessly extending the domain of secure information dissemination and collection.

Blending the modeling and implementation requirements of sophisticated high level agency as per the MAS paradigm in parallel with the simple agency involved in the modeling of complex adaptive systems characteristic of the ABMS paradigm is a unique capability – not currently offered by any platforms - which the ARM platform supports. Thus the ARM platform can simulate both the coordination backbone vertically within a holonic organization as well as the peer-to-peer interactions at the atomic holon level as essential pillars for the deployment of HSEs.

V. Risks And Challenges

A. *Coping with the problem magnitude*

It is practically impossible to offer a complete (and presumably correct) solution to a problem of this magnitude - mirroring the full, detailed dynamics of highly interactive human society while considering psycho-social, cultural and professional factors that are extremely subjective, intangible and difficult to express. We rely on our unique and leading expertise with interdisciplinary research problems of this kind through our work on emulating the mind which brings together psychoanalysts and engineers to develop computer models encapsulating subjective human experience. In spite of our efforts to make our models as accurate and realistic as possible we are aware of the limitations of current state of the art. In such emergency logistics problems, where the scope of possible organizations/tasks/skills is not restricted and/or predefined it is difficult to express and code enough real world semantics to permit a goal-driven and effective communication between the various organizations involved as well as between the levels of each organization. We recognize the difficulty in defining semantic standards and ontologies via which information can be expressed in a manner that is uniform.

While we expect that we can produce a number of generic guidelines about "how" (in which way) one may act in particular kind of crises, and predict/compare outcomes based on chosen decisions and actions, we acknowledge our possible inability to state "what" exactly to do (the best course of action) in a particular case/instance. In spite of the highest end technologies available in the ARM lab, any state of the art computer simulation of such real-life complex techno-social system is still a rough imitation of real processes. To date there is no unanimously recognized solution or theory that addresses with high fidelity real-life problems of this magnitude. We take this challenge as an opportunity to test our leading theories and models against the extremely demanding HSE requirements, knowing that if we are successful we will get an even higher competitive advantage as leaders in the field.

B. *Encapsulating inter-agency collaboration*

Another major challenge concerns the intrinsic (and difficult to grasp) values (‘culture’) that society and individuals place on secrecy and obfuscation both for personal and institutional advantage. In modeling inter- and intra- organizational coordination we need to consider how individual values clash with the values that the meta-organization places on sharing of sensitive information within and between the participating organizations. The volatility of issues such as the human wish to share and not share information is extremely difficult to encode in computer models. It is a proven fact that sharing of information with other government departments, critical infrastructure organizations including private corporations, and other nations is imperative but does not happen because of perceived advantage of restricted information in any societal environment. This mirrors the organization flow in large corporations where the reward system frequently discourages the sharing of information and, due to competition for power in the organization, by omission rewards the restriction rather than sharing of information - invariably to the detriment of the whole organization. To deal with this challenge we use our expertise with developing co-opetition models (Ulieru and Grobbelaar 2006) as well as our emulating the mind work (Dietrich et al 2008).

VI. Conclusions And Future Work

As an overarching simulation modelling capability the proposed HSE framework is capable to capture social, cognitive and information conceptual factors into a complex systems approach to security systems dynamics for the purpose of assessing meta-organizational decision-making structures, practices and processes. The ARM Lab simulation testbed will enable to assess the effectiveness of HSE deployment technologies and mechanisms through:

- experimentation and understanding of the high-level effects (resultant collective behaviour) at the meta-organizational level as they emerge from local interactions among individual participants within and across the partnering organizations;
- the design of exercise scenarios involving various organizational structures, for training and evaluation purposes;
- evaluation of the integration extent required to work effectively in a meta-organization team and the extent to which personnel can be educated into thinking and behaving cooperatively and collaboratively within and between mixed teams.

The simulation testbed enables a deep analysis of the effect that each key factor (cultural, professional, trust-related, etc.), has on the overall security ecosystem. By identifying interdependencies amongst the various factors, the eventual cascading effects will point to the weakest points while potential counteracting measures will be highlighted. The results of these analyses will contribute to a change of inter- and intra- organizational policies to ease the way toward teaming first responders into joint response alliances which could easily plug into international response efforts to optimize the counteracting effects in case of a major event. This will further enable future answers to some major research questions that are still open such as:

- What are the important trade-offs that must be analyzed and decided upon when choosing to transition from single organization operation to collaborative endeavor?
- What are the key enablers and what is the expected benefit of a holistic approach to operations?
- How to capture the coordination logic over an HSE to implement this overarching operational layer?
- What are the characteristics of HSE and how can they improve status quo in emergency response operations?

The HSE simulation tool can deliver a picture of the dynamics of emerging trends that will enable decision makers to anticipate the evolution of emerging crises and evaluate the effectiveness of different inter-agency configurations coming together in addressing it. This will result in a timely reduction of the vulnerability of our defense systems, thus increasing the social resilience through better effort coordination in first responders operations. Integrating the simulations results into a strategic thinking process will further enable a change of culture in the deployment of emergency operations by mobilizing and effectively using the most suitable resources and keeping the operational flow unobstructed through the chaos of crisis. The HSE simulation tool will enable analyses supporting the development of standards and practices for disaster resilience applicable beyond Canadian borders, which are much needed to strengthen our society.

Network-enabled operations have a very wide area of applications that go beyond first responder collaboration into production and enterprise operations. Our future work will focus on expanding the HSE simulation modeling into a generic emerging trends prediction tool supporting business, market and political analysts. In the long run we envision that this work will provide a platform for the analysis of interdependent systems and organizations via an operational picture of correlated collective dynamics, supporting strategic thinking and organizational leadership in a wide range of complex operations that go beyond the emergency response into trend analysis in global markets and enterprise dynamics for business operations. Further this research will open the door to new inventions enabling the development of solutions crucial for the orderly functioning of eSociety and economy (Ulieru and Verdon 2008). Examples can be found in the resilient deployment of interdependent critical infrastructures (Ulieru and Worthington 2006) (Ulieru 2007b) with applications such as blackout-free optimized power grid (Grobbelaar and Ulieru 2006) network-enabled operations

(Ulieru, 2008), hazard free transportation, environmental monitoring and pandemic mitigation.

REFERENCES

(Akyildiz 2005) F. Akyildiz, X. D. Wang, and W. L. Wang, "Wireless mesh networks: A survey," The International Journal of Computer and Telecommunications Networking: Computer Networks, vol. 47, pp. 445-487, 2005.

(Alberts and Hayes 2007) Albert, D. and Hayes, R. Power to the Edge: Command & Control in the Information Age, CCRP Publication Series 2003

(Boardman and Sauser 2008) Boardman J. and Sauser B. Systems Thinking: Coping with 21st Century Problems, CRC Press 2008 ISBN 13:978-1-4200-5491-0

(Crowell 2002) Crowell, Gary: Government Keynote at the Continuity from Chaos: Managing Resources and Logistics Information for Federal Enter-prises, FEMA Administration and Resource Planning Directorate, Washington DC, March 19, 2002.

(Dietrich et al 2008) Dietmar Dietrich, Mihaela Ulieru, Dietmar Bruckner, and Georg Fodor, The Mental Apparatus for Complex Automation Systems A Combined Computer Scientific and Neuropsychoanalytical Approach, Emulatig the Mind - A psychoanalytical approach to computer engineering, Dietrich et. a. (Eds), Springer 2008

(DND 2007) http://www.dnd.ca/site/reports/dps/index_e.asp

(Doursat and Ulieru 2008) Rene Doursat and Mihaela Ulieru (2008a), Emergent Engineering for the Management of Complex Situations, Keynote Paper appearing first (as vision paper) in the Proceedings of Autonomics 2008, Second ACM International Conference on Autonomic Computing and Communication Systems, Turin, Italy, September 23-25, 2008

(Enemo, G. 2007) Analysis of Command and Control (C2) in Network Enabled Operations (NEOps), The Norwegian Defense Research Establishment, Kjeller, Norway. http://www.ima.org.uk/conflict/papers/Enemo.pdf

(Gandon 2002) F. Gandon, A. Poggi, G. Rimassa, and P. Turci, "Multi-agent corporate memory management system," Applied Artificial Intelligence, vol. 16, pp. 699-720, 2002.

(Gerow 2002) Gerow, Bob: Emergency Management Software Solutions, Presentation at the Disaster Forum 2002 – Cooperating in Emergency Preparedness, Sept. 29-Oct 2, 2002, Calgary. AB, Canada.

(Gibson, Lemyre et al 2007) Terrorism Threats and Preparedness in Canada: The Perspective of the Canadian Public, Biosecurity and Bioterrorism, 5,2, 133-134.

(Grobbelaar and Ulieru 2006) Stefan Grobbelaar and Mihaela Ulieru, Self-Organizing Cyber-Systems as Infrastructure for Optimizing Power Distribution Networks, SAICSIT 2006, October 9-11, 2006, Capewinelands, South Africa

(Grobbelaar and Ulieru 2007) Stefan Grobbelaar and Mihaela Ulieru, Complex Networks as Control Paradigm for Complex Systems, Position Paper at the 1st IEEE International Workshop on eNetworks Cyberengineering, IEEE Systems Man and Cybernetics Conference, October 7-10, 2007, Montreal, Canada.

(Holland 1998) Holland J, Emergence: From Chaos to Order, Perseus Books F. Bellifemine, A. Poggi, and G. Rimassa, "Developing multi-agent systems with a FIPA-compliant agent framework," Software-Practice & Experience, vol. 31, pp. 103-128, 2001.

(Mentrup 2002) Mentrup, C., O. Fuhrer: e-Motion: e-Mobile Testbed for Interopera-bility of Networks in e-Logistics,; Session on Innovative Sectorial Applications, Proc. 1st Int. Conf. on Mobile Business - Evolution Scenarios for Emerging Mobile Commerce Services, July 8-9, 2002 Athens, Greece.

Moreri K.K, Mioc D., Anton F., Nickerson B., McGillivray E., Morton A., Ulieru M. and Tang. P., Web based Geographic Information Systems for a Flood Emergency Evacuation, Joint ISCRAM China and Gi4DM Conference on Information Systems for Crisis Management, August 4-6, 2008, Harbin, China

(North and Macal 2007) North, M J and C M Macal, Managing Business Complexity: Discovering Strategic Solutions with Agent-Based Modelling and Simulation, Oxford University Press, Inc. 2007, New York, NY.

(S&T 2007) Mobilizing Science and Technology to Canada's Advantage (http://www.ic.gc.ca/epic/site/ic1.nsf/en/h_00231e.html)

(Sen and Airiau 2007) S. Sen and Airiau S.: Emergence of Norms through Social Learning, in Proceedings of the IJCAI-07 pp. 1507-1512

(Tognalli and Ulieru 2005) Enrique M. Tognalli and Mihaela Ulieru, Pervasive Information Infrastructures for Industrial Informatics: An Application to Emergency Response Management, 3rd International Conference on Industrial Informatics, INDIN 2005, Perth, Australia, August 2005

(Ulieru 2007a) Mihaela Ulieru, A Complex Systems Approach to the Design and Evaluation of Holistic Security Ecosystems, International Conference on Complex Systems, Boston, MA, October 28-November 2, 2007

(Ulieru 2007b) Mihaela Ulieru (2007b), e-Networks in an Increasingly Volatile World: Design for Resilience of Networked Critical Infrastructures, The Inaugural IEEE International Conference on Digital Ecosystems and Technologies - IEEE-DEST 2007 - Cairns, Australia, 21-23 February 2007, 540-545.

(Ulieru 2008) Mihaela Ulieru, Enabling the SOS (Self-Organizing Security) Network, Proceedings of the IEEE SMC 2008 Conference, October 12-15, Singapore

(Ulieru and Doursat 2009) Mihaela Ulieru and Rene Doursat, Emergent Engineering: A Radical Paradigm Shift, Int. J. Autonomous and Adaptive Communications Systems 2009

(Ulieru and Grobbelaar 2006) Mihaela Ulieru and Stefan Grobbelaar, Holonic Stigmergy as a Mechanism for Engineering Self-Organizing Applications, Proceedings of ICINCO 2006 – 3rd International Conference of Informatics in Control, Automation and Robotics, August 1-5, 2006, Setubal, Portugal, pp. 5-10.

(Ulieru and Grobbelaar 2007) Mihaela Ulieru and Stefan Grobbelaar, Engineering Industrial Ecosystems in a Networked World, Keynote Paper at the 5th IEEE International Conference on Industrial Informatics, July 23-29, 2007, Vienna, Austria

(Ulieru and Unland 2004a) Mihaela Ulieru and Rainer Unland, Emergent e-Logistics Infrastructure for Timely Emergency Response Management, in Engineering Self-Organizing Systems: Nature Inspired Approaches to Software Engineering, Di Marzo Serugendo et.al. (Eds.) Springer Verlag, Berlin 2004, ISBN 3-540-21201-9, pp. 139-156.

(Ulieru and Unland 2004b) Mihaela Ulieru and Rainer Unland (2004a), "Enabling Technologies for the Creation and Restructuring Process of Emergent Enterprise Alliances", International Journal of Information Technology and Decision Making, Vol. 3, Issue 1, March 2004, pp. 33-60.

(Ulieru and Verdon 2008) Mihaela Ulieru and John Verdon "IT Revolutions in the Industry: From the Command Economy to the eNetworked Industrial Ecosystem" - Position Paper appearing first (as vision paper) in the Proceedings of the 1st International Workshop on Industrial Ecosystems, IEEE International Conference on Industrial Informatics, Daejoen, Korea, July 13-17 2008.

(Ulieru and Worthington 2005) Mihaela Ulieru and Paul Worthington, "Adaptive Risk Management System (ARMS) for Critical Infrastructure Protection", Integrated Computer-Aided Engineering, Special Issue on Autonomic Computing in Engineering in Integrated Computer-Aided Engineering; ISSN: 1069-2509; IOS Press; expected publication volume: 12:2 (January 2006), pp. 63-80.

(Ulieru et al 2006) Mihaela Ulieru, Paul Relf and Merv Matson, ARM – An Adaptive Risk Management Platform for Emergency Response Operations, IEEE- IECON 2006, November 8-10, 2006, Paris, France.

(Vasconcelos 2004) W. W. Vasconcelos. Norm verification and analysis of electronic institutions. In Declarative Agent Languages and Technologies (DALT) AAMAS'04 Workshop, New York City, New York, USA, 2004

(Vicente 2007) J. Vicente, S. Rungta, G. Ding, D. Krishnaswamy, W. Chan, and K. Miao, "OverMesh: Network-centric computing," in IEEE Communications Magazine, vol. 45, 2007, pp. 126-133.

(Werther 2000) Werther, G., Profiling 'Change Processes' as a Strategic Analysis Tool, Competitive Intelligence Magazine, January-March, 2000