Synopsis of my talks on Adaptive Risk Management at RMIT

Mihaela Ulieru
Canada Research Chair

My lectures will build on the radical shift in 'the Internet of the Future' from how we know it today (a mere communication highway) into a vast *hybrid network* seamlessly integrating physical (mobile or static) devices with distributed sensing and actuation, communications, storage and computation mechanisms to power, control or operate virtually any device, appliance or system/infrastructure. In such *networked embedded control systems* manipulation of the physical world occurs locally but control and observability are enabled safely and securely across a virtual network.

Tremendous progress in the emerging area of ubiquitous, pervasive and tangible computing enables hardware and software to be integrated to a degree that makes possible a technological revolution in which ICT systems merged with physical infrastructure will be transformed together into a vast intelligence network, called an 'eNetwork'. eNetworks are the 'nervous system' of interdependent critical infrastructures and as such are the 'the weakest link'. I will introduce a novel approach to building resilient critical supply networks of any kind (electricity, water, gas, finances, materials and products, etc).

In this context I will focus on the design integration and implementation of networked embedded control systems regarded as a "ubiquitous computing" system of ever-evolving networks of computers and mobile devices that are needed to support and provide the monitoring and control of critical infrastructure. I will present a generic methodology of design for resilience of critical infrastructures in which the eNetwork middleware will continuously self-organize to adapt the resilience of the infrastructure accordingly as vulnerabilities and threats emerge. I build on previous experience in developing adaptive information infrastructures and adaptive risk management strategies following three streams of research briefly described below.

- **Stream 1: Network self-organization to preserve/increase resilience.** I will present self-healing and reconfiguration methodologies integrated into a framework in which services flowing through eNetworks are able to organize themselves (and the eNetwork) in a resilient system without requiring any manual intervention by performing short-term adaptations to the environment as well as long-term evolution of new self-healing functionalities.

- **Stream 2: Risk Mitigation via eNetworks.** The goal is to endow eNetworks with the ability to quickly evaluate system vulnerability with respect to potential threats / undesirable events. I will present a methodology of *design for anticipation* in networked intelligent surveillance systems for the security of critical infrastructures.

- **Stream 3: Impact of Interdependencies**. The goal is to develop a strategy for resources allocation (such as sensor networks and mobile devices) to discover vulnerabilities in distinct components of the eNetworked infrastructure. Sensors and mobile devices will be allocated to enable appropriate collection of information considering the interdependent topology and structural vulnerability of the network of networks, to anticipate an attack on the supported infrastructure.

I will show how sensor networks have to be distributed to monitor critical hubs such as to enhance situational awareness while providing an integrated view of high quality contextual information to support decision making by combining relevant information from multiple disparate sources. For this I integrate latest advances in the evolution of complex networks topology with findings in infrastructure interdependencies to model the complex dynamics of critical hubs emergence under various threats. Such dynamics are encapsulated in control algorithms that will act on critical hubs as they evolve towards criticality before the catastrophic effects occur. Through proactive monitoring strategies, every critical hub in the eNetwork is alerted at the first sign of an eventual malicious intent, triggering fighter agents that specialize in eliminating attackers similar to how antibodies fight viruses in biological systems. As such, the eNetwork will behave like a *cyberorganism* that reacts to attacks in the same way as the immune system reacts to protect biological organisms. The drawback of false alarms is tackled via a thorough risk assessment threshold mechanism.

The approach introduced will make a radical shift from the current stream by looking at the security of eNetworked critical infrastructures from an ***anticipative*** perspective. To induce immunity into the eNetwork I propose the following ‘vaccine’: A hybrid mixture of static and mobile (physical and software) agents with an underlining *holonic self-organization mechanism* will be injected into the eNetwork to continuously monitor the status of the critical nodes (hubs). This approach is original in that it combines the latest trends in context-aware supply networks with the latest ideas in modeling self-organizing communication networks and the holonic paradigm. In this view a resilient eNetworked infrastructure consists of holons navigating the supply network (via the eNetwork) to monitor and detect any suspicious changes that could lead to an undesirable effect. The eNetwork would self-organize in appropriate resilience patterns using novel a context-awareness mechanism envisioned to tune the autonomy across the holarchic levels according to the detected/anticipated intent of eventual malicious holons.

This will result into a generic methodology to build resilient networked infrastructures encompassing an adaptive risk management mechanism of self defense (including potential to intercept malicious intent and annihilate attackers before they act). Using such a mechanism, eNetworks will reconfigure the infrastructure system into new adaptive structures and architectural patterns, resilient to both accidental failures and malicious attacks.