Introduction to the Proceedings of the 2017 NATO Workshop on Cyber Resilience

The papers in these Proceedings were presented at the 2017 NATO Workshop IST-153 on Cyber Resilience. The workshop was held in Munich, Germany, on 23 - 25 October 2017, at the University of Bundeswehr.

This Workshop was unclassified and open to NATO nations, Partner for Peace nations, Mediterranean Dialogue, ICI nations and Global Partners.

The workshop co-chairpersons were Dr. Alexander KOTT, U.S Army Research Laboratory, United States, and Prof. Dr. Gabi DREO RODOSEK, research institute CODE, University of Bundeswehr Munich, Germany.

Committee members were:

Bob MADAHAR
Defence Science and Technology Laboratory
Cyber and Information Systems Division
United Kingdom

Emin Emrah ÖZSAVAŞ
Turkish Army Cyber Defence
Turkey

Alfred MØLLER
DALO
Denmark

Harald SCHMIDT
Fraunhofer-FKIE
Germany

Dennis McCALLAM
Northrop Grumman
United States

Peeter LORENTS
Estonian IT College
Estonia

Mark RAUGAS
Organization PNNL
United States

In organizing this workshop, the committee stressed that NATO Nations—citizens, businesses and governments -- increasingly rely on cyber infrastructure. This puts national security at considerable risk to unforeseen and unknown cyber threats. The high level of interconnectivity found in modern society has opened many avenues for cyber-attacks, including internal and external threats, and vulnerabilities within supply chain networks. Despite continual progress in managing risks in the cyber domain, it is clear that anticipation and prevention of all possible attacks and malfunctions are not feasible for current or future systems comprising the cyber infrastructure. Therefore, interest in cyber resilience (as opposed to merely risk-based approaches) is increasing rapidly, in literature and in practice with many nations expressing it in their cyber strategies. For example, the President of the United States released a presidential policy directive (Presidential Policy Directive 21 2013) and executive order (Executive Order 13636 2013), focusing national attention on cyber-infrastructure resilience. Similarly, NATO 2020 report states – “Responding to the rising danger of cyber-attacks: NATO must accelerate efforts to respond to the danger of cyber-attacks … helping Allies to improve their ability to prevent and recover from attacks.” Indeed, resilience is defined in dictionaries as the ability to recover from or easily adjust to misfortune or change. It is characterized by four abilities: to plan/prepare, absorb, recover from, and adapt to known and unknown threats. Unlike concepts of risks or robustness – which are often and incorrectly conflated with resilience -- resiliency refers to the system’s ability to recover or regenerate its performance to a sufficient level after an unexpected impact produces a degradation of its performance. However, the exact relation between resilience, risk and robustness has not been well articulated technically. This includes the appropriateness and use of metrics, the correspondence to the engineering and architectural approaches, and role of resilience-by-design in assuring effective recovery and continuity of operations. All these issues remain poorly researched and understood.

For all these reasons, the workshop aimed to explore how the directions of current and future science and technology may impact and define potential breakthroughs in this field. The presentations and discussions at the workshop yielded a report as well as proceedings of the workshop detailing certain aspects of the current state of research, projections into the future, with special focus on capabilities, architectures and anticipated technical milestones for achieving higher resilience of cyber infrastructures.

The co-chairpersons express their gratitude to Mr. Julius Zahn from the research institute CODE for his outstanding help in organizing and executing the workshop, and to Mr. John B. MacLeod for his critical role in organizing the workshop and preparing the proceedings.