Introduction to the Proceedings of the 2017 Workshop on Intelligent Autonomous Agents for Cyber Defence and Resilience

The papers in these Proceedings were presented at the workshop on Intelligent Autonomous Agents for Cyber Defence and Resilience organized by NATO research group IST-152-RTG. The workshop was held in Prague, Czech Republic, on 18-20 October 2017, at the premises of the Czech Technical University in Prague.

The Workshop was unclassified, releasable to public, and open to representatives of NATO Partnership for Peace (PfP/EAPC) Nations.

This workshop explored opportunities in the area of future intelligent autonomous agents in cyber operations. Such agents may potentially serve as fundamental game-changers in the way the cyber defence and offense are conducted. Their autonomous reasoning and cyber actions for prevention, detection and active response to cyber threats may become critical enablers for the field of cyber security. Cyber weapons (malware) rapidly grow in their sophistication, and in their ability to act autonomously and to adapt to specific conditions encountered in a friendly system/network. Current practices of cyber defense against advanced threats continue to be heavily reliant on largely manually driven analysis, detection and defeat of such malware. There is a growing recognition that the future cyber defense should involve extensive use of partially autonomous agents that actively patrol the friendly network, and detect and react to hostile activities rapidly (far faster than human reaction time), before the hostile malware is able to inflict major damage, or evade the friendly agents, or destroy the friendly agent. This requires cyber defense agents with a significant degree of intelligence, autonomy, self-learning and adaptability. Autonomy, however, comes with difficult challenges of trust and control by humans.

The workshop investigated 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 produced a report as well as proceedings of the workshop detailing the current state of research, projections into the future, with special focus on capabilities, architectures and anticipated technical milestones for achieving strongly intelligent autonomous behaviors of intelligent agents in cyber operations.

The workshop brought together approximately 30 cyber security researchers, technologists, and practitioners. The workshop provided an excellent opportunity to increase participants' insight in intelligent autonomous agents in general, and their use in cybersecurity in particular, and to influence the future research in intelligent autonomous agents, especially as it relates to cyber defence and resilience. The workshop comprised a series of topical sessions. Each session included several presentations of papers – some of which were full technical papers and others will be shorter position papers or product papers – and a discussion open to all participants. The Programme Committee utilize the oral discussions at the workshop to formulate the final report of the workshop, including a set of recommendations. The final report is a separate publication not to be confused with these proceedings.

The workshop was chaired by Programme Co-Chairs Prof. Michal Pechoucek, Czech Technical University in Prague, Czech Republic, and Dr. Alexander Kott, U.S. Army Research Laboratory, USA.

The committee of the workshop included the following members:

Benoit LEBLANC Ecole Nationale Supérieure de Cognitique France	Hervé LE GUYADER Ecole Nationale Supérieure de Cognitique France
Luigi MANCINI Sapienza Universita di Roma Italy	Heiko GUENTHER Fraunhofer FKIE Germany
Krzysztof RZADCA University of Warsaw Poland	Pavel CELEDA Masaryk University Czech Republic
Mauno PIHELGAS CCDCOE Estonia	Nazife BAYKAL Middle East Technical University (ODTU) Turkey
Paul THERON Thales France	Nikolai STOIANOV Defence Institute “Prof. Ts. Lazarov” Bulgaria
Martin DRASAR Masaryk University Czech Republic	Mauro CONTI University of Padua Italy
Frédéric CUPPENS Telecom Bretagne France	

The co-chairpersons express their gratitude to Ms. Katarina Takusova for her 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.