# Technical Evaluation Report

of the

**IST-190 - SYMPOSIUM**

on

# "Artificial Intelligence, Machine Learning and Big Data for Hybrid Military Operations"

**Dr. Roy Streit**
Metron, Inc.
UNITED STATES OF AMERICA

r.streit@ieee.org - streit@metsci.com

**Virtual Meeting - Webex**
**5-6 October 2021**

## EXECUTIVE SUMMARY

The IST-190 symposium provided a forum for invited and contributed papers that work "towards a common roadmap for future technologies, addressing the identified knowledge gaps, while recognizing the opportunities offered by available techniques related to emerging technologies in the areas of Artificial Intelligence (AI), Machine Learning (ML) and Big Data (BD) for hybrid military operations." Of necessity, it was a virtual symposium held via Webex, but it was nonetheless a very successful symposium thanks to the efforts of the Co-Chairs, Dr. Michael Wunder and Maj. Gen. Michael Faerber, and others in the organizing committee. Three Keynote addresses were given by highly distinguished speakers, and 34 papers contributed papers were given by subject matter specialists. The papers were split into seven topic-related groups that were presented in parallel sessions over two days. There were two such sessions at any given time, and the attendees could choose between them. The contributed papers are diverse and they report on a wealth of experience. They were all well-written, and the presenters were all excellent. The Best Paper Award and the Early Career Scientist Best Paper Award were announced at the end of the symposium. All 34 papers and presentation slides are available.

The technologies of AI and ML are evolving at a rapid pace, and they are exploiting the availability of Big Data, which has its own specialized set of techniques. There is currently a bewildering variety of existing methods and applications that are enabled by some combination of these technologies, and more are being proposed and explored every day. Some capabilities are extensions of what we know; some are reasonably predictable based on what is known; and some cannot be anticipated and will be surprisingly effective. The IST-190 symposium sought to identify and explore the potential of these emerging technologies for hybrid military operations. The emphasis of the papers was on defense and preparedness.

The papers presented at IST-190 showed that the threat of these combined technologies is real, and that AI/ML practitioners are gaining experience in applying them to military operations. The papers also show, collectively and in diverse ways, that defending against the threat requires the development of new and improved tools to deal with the technical challenges. The need for solutions is growing.

New tools are needed and welcome, of course, but new developments take time. Greatly improving the capabilities of existing tools will address many immediate needs. These include:

- Compensate for the lack of data for “infrequent” events with few available exemplars
  - Generative and adversarial methods can augment available data sets
- Explain AI/ML derived decisions and recommendations
  - Black box directives can mislead and undermine confidence
- Give accurate self-assessment of the reliability of AI/ML recommendations, and of the correctness of aggregated (fused) heterogeneous data sets
  - Make robust decisions in a fog of uncertainty
- Use natural language processing (NLP) for HUMINT
  - Often critical in AI/ML systems that exploit hard-soft information fusion
- Methods for real time adaptation to evolving threats
  - Perfect assessments that come too late are of limited value
- Support building trust in the system
  - Data provenance / drill down
  - Built-in sanity checks for the human in the loop

Many innovations will inevitably be developed by the private sector. For success, innovations that are successful in the private sector must be transitioned to meet demanding military operational needs that will severely stress the capabilities of commercial AI/ML methods. Case studies presented in the symposium suggest that tools for hybrid military operations should be jointly developed by military operation specialists and subject matter specialists to ensure that the focus is on the real and evolving need, and to build trust in the system.

## SUMMARY OF IST-190 SYMPOSIUM

### Plenary Sessions

**First Plenary: Day 1.**

- Opening the Symposium, by Dr. Michael WUNDER, Symposium C-Chair, Fraunhofer-FKIE, Germany, opened the Symposium.
- Welcoming participants, by Major General Michael FAERBER, Symposium Co-Chair, Commander Bundeswehr CIS Command, Germany.
- **Keynote speech 1.** Lt. General Alfons MAIS, Chief of the German Army, Germany.

**Second Plenary: Day 2. Welcome back**

- Welcome back, Dr. Michael WUNDER, Symposium C-Chair, Fraunhofer-FKIE, Germany
- **Keynote speech 2.** Prof. Wojciech MAZURCZYK, Warsaw University of Technology, Poland

**Third Plenary: Day 2**

- **Keynote speech 3.** Mr. John-Mikal STØRDAL, CSO Director, Norway

**Fourth Plenary: Day 2**

- Best paper award was presented by Prof. Bhopinder MADAHAR, DSTL, United Kingdom
- Technical Evaluation Report summary by Dr. Roy STREIT, Metron, United States
- Closing Ceremony
  - Dr. Michael WUNDER, Symposium C-Chair, Fraunhofer-FKIE, Germany
  - Major General Michael FAERBER, Symposium Co-Chair, Commander Bundeswehr CIS Command, Germany

**BEST PAPER AWARD**

# Robustness of Artificial Intelligence for Hybrid Warfare

by

**Metin Aktaş**
ASELSAN
Defence Systems Technologies Division
TURKEY
maktas@aselsan.com.tr

**James Sharp John Melrose Bob Madahar**
Defence Science and Technology Laboratory
UNITED KINGDOM
{jsharp1,jmelrose, bkmadahar} @dstl.gov.uk

**Niki Martinel**
University of Udine
Dept. of Mathematics, Computer Science and Physics
ITALY
niki.martinel@uniud.it

**Eilif Solberg**
Norwegian Defense Research Establishment
NORWAY
eilif.solberg@ffi.no

**Julian de Marchi**
Royal Netherlands Aerospace Centre
THE NETHERLANDS
Julian.de.Marchi@nlr.org

**Douglas S. Lange**
Naval Information Warfare Systems Center Pacific
UNITED STATES OF AMERICA
dlange@niwc.navy.mil

**Frank Kurth**
Fraunhofer FKIE
GERMANY
frank.kurth@fkie.fraunhofer.de

**Guven Orkun Tanik**
Turkish Aerospace Industries
TURKEY
guvenorkun.tanik@tai.com.tr

**Linus Luotsinen**
Swedish Defence Research Agency (FOI)
SWEDEN
linus.luotsinen@foi.se

## *ABSTRACT*

*In his 2016 address to the Association for the Advancement of Artificial Intelligence (AI), then President of the association called for AI that sacrificed some optimality for the sake of robustness [1]. For AI, robustness describes the ability of a system to maintain its level of performance under a variety of circumstances [5]. Developing and verifying high quality models through machine learning faces particular challenges. Generally recognised conditions that most AI might need to be robust to include:*

*Uncertainty in training and operational data;*

*Inputs that are different from the training set, yet consistent with the training population statistically or semantically;*

*Inputs that are outside the training population;*

*Learning with limited data;*

*Novel situations, different from how learned policies and classifiers were developed; and*

*Adversarial action.*

*Further, for human AI teaming, the human must appropriately trust the AI system; thus, transparency can also be considered a robustness issue. Hybrid warfare brings additional challenges for the robustness of AI. The varied nature of the decisions and necessary decision support widens the range of models required. The combined use of models developed under different conditions affects the statistical claims that can be made about the quality of the composite system.*

*If we are to require robustness, we must consider its measurement. A survey of research on robustness relative to the conditions above provides a range of possible measures. Hybrid warfare practiced by a coalition requires an understanding of the robustness of the capabilities being employed. In this paper we survey the landscape of robustness metrics from current literature. In doing so, we facilitate understanding the combination of a diverse set of models and software from within the alliance.*

## EARLY CAREER SCIENTIST - BEST PAPER AWARD

# Towards Authority-Dependent Risk Identification and Analysis in Online Networks

by

**Frederik S. BÄUMER and Sergej DENISOV**
Bielefeld University of Applied Sciences
GERMANY

**Yeong Su LEE and Michaela GEIERHOS**
Research Institute CODE, Bundeswehr University Munich
GERMANY

## *ABSTRACT*

*Interaction, discussion, and the exchange of diverse information make the Web the place it is today. Texts, images, videos, and even information such as geospatial and health data are shared at an unprecedented scale. This exchange of information on the Web generates an extensive, freely accessible data source for a variety of data-driven applications – with multiple opportunities, but also risks. In this paper, we present the overall idea of the research project ADRIAN – "Authority-Dependent Risk Identification and Analysis in online Networks" which is dedicated to the research and development of AI-based methods for detecting potential threats to individuals and institutions based on heterogeneous, online data sets. We will first monitor selected social sports apps and analyze the collected geospatial data. In a second step, the user profiles of sports apps and social media platforms will be correlated to be able to form a cluster of individuals and enable the identification of potential threats. Since a so-called "digital twin" can be reconstructed in this way, sensitive data is generated. If this data can also be correlated with other confidential data, it is possible to estimate the plausibility of the threat to individuals, groups or locations.*

# SYMPOSIUM PAPERS

## I. Concepts and Scenarios – 3 papers – DAY 1 (Tuesday, 5 October 2021)

Paper 1. "Detecting Adversarial Inputs and Robust Learning Using Data Manifolds" by Mr. Hervé P. LE GUYADER (P Nationale Supérieure de Cognitique (ENSC), France

- This is a very readable paper. Historical perspectives are carefully presented. It is a thoughtful essay that advocates strongly for adding a sixth new domain "Human" to the land/sea/sea/space/cyber paradigm. The topic merits further discussion in the wider community.

Paper 2. "Connecting the Dots – Enhancing the Information Processing Chain for the Detection of Hybrid Threats for Host Nation Support and Territorial Operation" by Mr. Arne SCHWARZE (Presenter), Dr. Michael GERZ and Mr. Hans-Peter STUCH, Fraunhofer-FKIE, Germany.

- This paper surveys the problems and the needs of hybrid threats, stressing the need for tools to support the analysis of a diversity of data sources. It reports the findings of a project that studied two realistic urban scenarios. The discussion emphasizes the importance and need of integrating AI and big data.

Paper 3. "The Role of Joint Intelligence Preparation of the Operating Environment to Multi-domain Operations" by Major Radovan VASICEK (Presenter) and LTC. Petr HLAVIZNA, University of Defence, Czech Republic.

- The paper examines the role and significance of Joint Intelligence Preparation of the Operating Environment (JIPOE). The relevance of AI/ML is oblique, not being overtly discussed, but is nonetheless real.

## II: Planning and Decision Making – 6 papers – DAY 1 (Tuesday, 5 October 2021)

Paper 4. "Knowledge Representation and Reasoning for Defense" by Dr. Paul CRIPPS (Presenter), Prof. Bhopinder MADAHAR and Dr. David BARBER, DSTL (Defence Science and Technology Laboratory), United Kingdom

- A high level survey of graph based methods for knowledge representation and reasoning for joint decision making by humans and machines. Socio-technical, information system, and S&T issues are outlined.

Paper 5. "Coalition Situational Understanding Via Adaptive, Trusted and Resilient Distributed Artificial Intelligence Analytics" by Prof. Alun PREECE (Presenter), Cardiff University, United Kingdom, Mr. Dave BRAINES, IBM Research Europe, United Kingdom, Dr. Federico CERUTTI, University of Brescia, Italy, Mr. Gavin PEARSON, DSTL, United Kingdom and Dr. Lance KAPLAN, U.S. DEVCOM Army Research Laboratory, United States.

- US/UK report on DAIS = adaptable, trusted, resilient AI. The paper is a high level overview of several important facets of the Demo. It is an interesting read. The introduction mentions the importance of recognizing patterns of activity in complex dense data streams without generating false alarms/detections, but this important topic is not discussed further.

Paper 6. " A Periodic System of Artificial Intelligence as an Effective Means of Communication between Machine Learning Experts and Military Operators" by Dr. Marlon MYLO (Presenter), Mr. Detlef SCHOEPE and Mr. Paul DYKTA, Bundeswehr, Germany

- A lively discussion of an interesting notion of depicting levels of AI abstraction as a kind of "periodic table". It seems a useful icon-style display, but it is not widely discussed in the literature.

Paper 7. "U.S. Army Artificial Intelligence Opportunities for International Partners" by Dr. Kelly RISKO (Presenter), Mr. Nathan ANDERSON, Dr. Jonathon BRAME and Dr. Tien PHAM, U.S. DEVCOM Army Research Laboratory, United States

- Reviews and discusses international partnering opportunities with the US Army. Such collaborations are valuable in many ways.

Paper 8. "Efficient and Resilient Edge Intelligence for the Internet of Battlefield Things" by Dr. Maggie WIGNESS (Presenter), Dr. Tien PHAM, Dr. Stephen RUSSELL, U.S. DEVCOM Army Research Laboratory, and Prof. Tarek ABDELZAHER, University of Illinois at Urbana Champaign, United States

- Discusses need for an AI/ML focused on efficiency, efficacy, and integrity of the IoBT itself. References recent advances in theory of Cyber-Physical System security to meet these needs. Effectively advocates for "a new breed of AI solutions […] that can be projected rapidly to the point of need, where they can survive the austere environment of field operations, as opposed to restricting AI to solutions that run at data centers of higher echelons."

Paper 9. "Benefits and challenges of AI/ML in support of intelligence and targeting in hybrid military operations" by Dr. Anne-Claire BOURY-BRISSET (Presenter) and Mr. Jean BERGER, Defence Research Development Canada (DRDC), Canada

- New decision support solutions for multi-objective optimization are explored in conjunction with AI/ML methods for IST, ATR, and multimodality data fusions. A good read.

## IV: Model Based Approaches – 3 papers – DAY 1 (Tuesday, 5 October 2021)

Paper 10. "Transition from Rule-based Behaviour Models to Learning-based Behaviour Models in Tactical Simulation Environments: A Case Study" by Dr. Arif Furkan MENDI (Presenter), Mrs. Fatiha Nur BUYUKOFLAZ, Mr. Tolga EROL, Mrs. Dilara DOGAN, Mr. Turan TOPALOGLU, Mr. Şenol Lokman ALDANMAZ Mr. Mehmet KOZAN, HAVELSAN, Mr. Muhammed Esat KALFAOGLU and Dr. Hüseyin Oktay ALTUN (Co-Presenter), AutoDidactic Technologies, Turkey

- Uses techniques from reinforcement learning for tactical training of pilots (air-to-air and air to ground flight simulators) and shows significant improvement over rule based behavior models. Novel, and with very practical and important implications.

Paper 11. "Playing Games to Learn Robustly from Adversarial Expert Demonstrations" by Dr. Prithviraj (Raj) DASGUPTA (Presenter), U.S. Naval Research Laboratory, United States

- Discusses how a reinforcement learning method called LfD (learning from demonstration) can be

exploited by its enemies to make LfG fail. A game-playing system between adversary and learner is presented that avoids degraded learning performance. Needs further work.

Paper 12. “Towards a Hybrid Model of Trust and Technology Acceptance for Hybrid Warfare Applications” by Dr. David J.Y. COMBS (Presenter), Knexus Research Corporation, and Dr. E.S. VORM, U.S. Naval Research Laboratory, United States

- Identifies a serious problem and establishes the very real need to solve it. The paper provided insufficient empirical evidence for a solution. Three references to the broad behavioral literature are a good start, but does not point to the larger base of literature currently exists.

## V: Managing Risks and Uncertainty – 7 papers – DAY 1 (Tuesday, 5 October 2021)

Paper 13. “Dealing with uncertainty in Hybrid conflict: A novel approach and model for uncertainty quantification in intelligence analysis” by Dr. Thomas POWELL (Presenter), Dr. Serena OGGERO, Mr. Joris WESTERVELD and Mrs. Emma SCHOOK, TNO (Netherlands Organisation for Applied Scientific Research), the Netherlands

- Proposes a method for uncertainty quantification that is closely related to statistical inference of categorical variables by working directly with the intel reports, not human analyst judgment. Discusses the need for automation using AI and ML.

Paper 14. “Risk Assessment for the Age of Algorithms” by Mr. Steven ROEMERMAN (Presenter), John VOLPI, Randall ALLEN, Lone Star Analysis (LSA), United States

- Excellent analysis of executive risk assessment. AI appears for the first time on page 10 as a "later extension" of their early work, giving a sense of less in-depth analysis. Nonetheless, this does not discredit the work. Risk assessment is a requirement for AI/ML in defense applications. Training executives and officers to use the tools is critical to success in fielded systems.

Paper 15. “Role of Big Data in Resilience Assessment in Military Context” by Mr. Charalampos SARANTOPOULOS (Presenter), Mrs. Ivana ILIC MESTRIC, Dr. Michael STREET, Mr. Riccardo D’ERCOLE and Mr. Giavid VALIYEV, NCIA, the Netherlands

- The paper is written in an IEEE format. To quote from the Abstract: "demonstrate the potential of open source data, coupled with big data analytics and data visualization, to indicate levels of resiliency […]". Emphasis on multiple interrelated interactive dashboard visualizations.

Paper 16. “Explainable AI for Strategic Hybrid Operations” by Dr. Felix GOVAERS (Presenter), Fraunhofer-FKIE, Germany

- Early study of XAI using the LIME (Local Interpretable Model-Agnostic Explanations) method. LIME was not referenced. An interesting application to “explaining” chess moves was presented as a surrogate for military operations. Seems a good approach but needs more evidentiary support.

Paper 17. “Robustness of Artificial Intelligence for Hybrid Warfare” by Dr. James SHARP (Presenter), Prof. Bhopinder MADAHAR, Mr. John MELROSE, DSTL (Defence Science and Technology Laboratory), United Kingdom, Dr. Metin AKTAS, ASELSAN, Turkey, Mr. Eilif SOLBERG, Norwegian Defense Research Establishment (FFI), Norway, Dr. Julian DE MARCHI, NLR (Royal Netherlands Aerospace Centre) Aerospace Vehicles Collaborative Engineering, the Netherlands, Mr. Guven Orkun TANIK, Turkish Aerospace Industries, Turkey, Dr. Niki MARTINEL, University of Udine, Italy, , Mr. Linus LUOTSINEN, Swedish Defence Research Agency (FOI), Sweden, Prof. Dr. Frank KURTH, Fraunhofer-FKIE, Germany, and Dr. Douglas S. LANGE, Naval Information Warfare Systems Center Pacific, United States

- An excellent wide-ranging summary and critical review of the state of the art of several facets of robustness in AI. The coverage of topics is especially valuable. New methods are not presented, but it is very clearly written, and the review and perspective will be helpful for many readers.
- **IST-190 Best Paper Award**

Paper 18. “Opposed Artificial Intelligence: Developing Robustness to Adversarial Attacks in Attacker-Defender Games via AI-based Strategic Game-Playing” by Dr. Prithviraj (Raj) DASGUPTA (Presenter), Dr. Phillippa SPENCER, Dr. Adam JEFFERY, DSTL (Defence Science and Technology Laboratory), United Kingdom, Dr. Michael MCCARRICK, Dr. Signe REDFIELD, Dr. Ranjeev MITTU, U.S. Naval Research Laboratory, United States, Dr. Michael NOVITZKY, Dr. John JAMES, United States Military Academy, United States, Dr. David HUBCZENKO, Defence Science and Technology Group, Australia

- Opposed AI is about the conflict between two or more AI systems that are in conflict due to noisy/bad data and/or mismodeling. It is studied using reinforcement learning in a multiplayer "capture the flag" game. A competition was organized.

Paper 19. “Deep Self-optimizing Artificial Intelligence for Tactical Analysis, Training and Optimization” by Dr. Matthias SOMMER (Co-Presenter), Dr. Michael RUEEGSEGGER, armasuisse Science and Technology, Federal Department of Defence, Civil Protection and Sport, Switzerland, and Dr. Oleg SZEHR (Co-Presenter), Mr. Giacomo DEL RIO, Dalle Molle Institute for Artificial Intelligence (IDSIA), Switzerland

- Feasibility study of using reinforcement learning with a Neural-Network-based Monte Carlo Tree Search algorithm for strategic planning and training in air-defense scenarios. Proof of concept study for a simple scenario.

## END OF DAY 1

## III. Socio-Technical Aspects – 7 papers – DAY 2 (Wednesday, 6 October 2021)

Paper 20. “Assessment of whole-of-society hybrid conflict: Fusion of activity signals and analyst insight” by Mr. Bas KEIJSER (Presenter), Dr. Thomas POWELL, Mr. Joris WESTERVELD and Mr. Peter VAN SCHEEPSTAL, TNO (Netherlands Organisation for Applied Scientific Research), the Netherlands

- A design method for the analysis of hybrid societal conflict was presented. The method was evaluated on a case study. The challenges to assessing hybrid conflict are clearly delineated.

Paper 21. “Provenance Tracking of Hybrid Decision Making” by Dr. Douglas S. LANGE (Presenter), Mr. Crisrael LUCERO and Mr. Braulio CORONADO, Naval Information Warfare Systems Center (NIWC) Pacific, United States

- Proposes provenance graphs within and across a system of systems for forensic analysis needed for decision making.

Paper 22. “On Digital Ethics for Artificial Intelligence in Hybrid Military Operations” by Prof. Dr. Wolfgang KOCH (Presenter), Fraunhofer-FKIE, Germany

- An exposition of the need to implement for ethical behavior in fielded systems to support and guide decision making. The legal consequences of poor decisions were discussed.

Paper 23. “Narrative Coherence and the Detection of Enemy Activity in Social Media Data: Case Study from the 2020 Azerbaijan / Armenia conflict” by Dr. Hezekiah Akiva BACOVCIN (Presenter), Mr. Maxime MARTINEAU, Nexalogy Environics, Inc., and Mr. Zach DEVEREAUX, Datametrex Inc., Canada

- Very interesting case study of ML methods to distinguish messages from different narratives. It is formulated as an unsupervised clustering problem.

Paper 24. “Towards Authority-Dependent Risk Identification and Analysis in Online Networks” by Dr. Frederik S. BAEUMER (Presenter), Mr. Sergej DENISOV, Bielefeld University of Applied Sciences, Dr. Yeong Su LEE and Prof. Dr. Michaela GEIERHOS, Research Institute CODE, Bundeswehr University Munich, Germany

- Studies the extent to which an individual’s anonymity is compromised by combining multiple social media platforms. This paper will help readers appreciate the importance of the problem in both civilian and military operations.
- IST-190 Early Career Scientist - Best Paper Award

Paper 25. “Detecting Generated Media: A Case Study on Twitter Data” by Mr. Harald STIFF (Presenter) and Mr. Johan SABEL, Swedish Defence Research Agency (FOI), Sweden

- Advances in generative NNs are evaluated for performance in detecting deep Twitter fakes. Interesting application.

Paper 26. “Conflict Monitoring” by Mrs. Theresa KRUMBIEGEL (Presenter), Mrs. Samantha KENT, Mr. Albert PRITZKAU, Dr. Hans-Christian SCHMITZ, Fraunhofer-FKIE, Germany

- Applies and adapts methods for Latent Dirichlet Allocation (LDA) to media event extraction and Open Source Intelligence (OSInt). The fusion of OSInt (media space) and events in the physical world is challenging. They write, “Linking the physical domain to the information space is not a trivial task.”

## VI: Cyber Security – 5 papers – DAY 2 (Wednesday, 6 October 2021)

Paper 27. “New Defenses for the Hybrid Battlefield” by Dr. Paul Maxwell (Presenter), Army Cyber Institute, West Point, United States

- The paper identifies and discusses eight "threats of the hybrid battlefield and makes recommendations on how to update our tactics to protect against them." Very well written. The recommendations need more in-depth study.

Paper 28. “Adversarial Machine Learning and the Future Hybrid Battlespace” by Dr. Christopher RATTO (Presenter), Dr. Michael PEKALA, Mr. Neil FENDLEY, Mr. Nathan DRENKOW, Dr. Kiran KARRA, Mr. Chace ASHCRAFT, Mr. Cash COSTELLO, Dr. Philippe BURLINA, Dr. I-Jeng WANG and Dr. Michael WOLMETZ, The Johns Hopkins University Applied Physics Laboratory, United States

- Summarizes recent ML research at their institution related to hybrid warfare: physical adversarial attacks on imaging systems, data poisoning attacks, and design of robust AI systems.

Paper 29. “Sensitive or not? How to attack and defend document security classification models” by Dr. Konrad WRONA (Presenter), NATO Cyber Security Centre, the Netherlands, Prof. Maria Carla CALZAROSSA, Mrs. Sara PIZZIMENTI and Mr. Alessandro OBERTI, University of Pavia, Italy

- Demonstrates that adversarial attacks are not limited to images but can also be directed at text classification and NLP/Natural Language Processing. Examples of "adversarial text" are given. Countermeasures are discussed.

Paper 30. “From Plain Text to CTI – A Technological Solution for Gathering Cyber Threat Intelligence using Natural Language Processing” by Mr. Robert MUELLER (Presenter) and Prof. Dr. Elmar PADILLA, Fraunhofer-FKIE, Germany

- Develops a model for extracting cyber-threat intel (CBI) from free-form natural language text. Implemented the method on publically available data on malware threats. Interesting selection of real data. Hard and important problem.

Paper 31. “Tracking Cyber Threat Actors through Semi-automatic OSINT Analysis” by Mrs. Hanna LILJA (Presenter) and Mr. Lukas LUNDMARK, Swedish Defence Research Agency (FOI), Sweden

- Leverage recent developments in NLP and ML to identify threat actors in Open Source (OS) text. The effectiveness of the method is studied in two examples. Difficult but important problem. Need better data.

## VII: EM Environment & Communication – 3 papers – DAY 2 (Wednesday, 6 October 2021)

Paper 32. “Application of AI/ML technology to address congestion, quality, and security of private military network deployments” by Dr. M. Patryk DEBICKI (Presenter), Thales UK Limited, United Kingdom, and Mr. Gonzalo ARECHAGA, Thales Programas de Electrónica y Comunicaciones S.A.U., Spain

- AI/ML is used to "augment" performance management of LTE networks and to detect anomalies across multiple network domains.

Paper 33. “Reinforcement Learning Environment for Tactical Networks: Multi-Agent based Scenario Generation” by Mr. Thies MOEHLENHOF (Presenter), Mr. Norman JANSEN and Mrs. Wiam RACHID, Fraunhofer-FKIE, Germany

- Reports on the use of reinforcement learning to generate dynamically changing tactical network scenarios to enable the training of a tactical system to improve performance in DIL networks (Disconnected, Intermittent, Limited). Training data augmentation is important in many AI/ML problems.

Paper 34. “Towards Drone Recognition and Localization from Flying UAVs through Processing of Multi-Channel Acoustic and Radio Frequency Signals a Deep Learning Approach” by Dr. Andrea TOMA (Presenter), Dr. Niccolò CECCHINATO, Prof. Carlo DRIOLI, Dr. Giovanni FERRIN and Prof. Gian Luca FORESTI, University of Udine, Italy

- A method for recognition and localization of unidentified aerial acoustic source with RF-assisted is presented and implemented as a four-stage CNN-based network architecture. Methods are relevant to ML and NNs.

**END OF DAY 2**