European Intelligence & Security Informatics Conference

The Premier European Conference on Counterterrorism and Criminology

Dekelia Air Base, Dekelia, Greece, September 11-13, 2017

http://www.eisic.org

EISIC 2017

Conference Program

EISIC 2017

Conference Organizer and Sponsor

Academic Sponsors

FOI

KTH VETENSKAP OCH KONST

Panel Sponsors

VALCRI

VISUAL ANALYTICS FOR SENSE-MAKING IN CRIMINAL INTELLIGENCE ANALYSIS

Technical co-sponsorship

IEEE

IEEE computer society

Conference Secretariat

Conference registration takes place at the Conference Secretariat located at the lobby of the Conference Center of Hellenic Air Force Academy, during the following days and hours:

Monday	8:30 – 17:00
Tuesday	8:30 – 17:00
Wednesday	8:30 – 14:00

The registration fee includes:

- One lunch and two coffee breaks per conference day
- One ticket for the Conference Reception held on Monday 11th September, 2017 at 20:00
- One ticket for the Gala Dinner held on Tuesday 12th of September, 2017 at the Hellenic Armed Forces Officers Club.
- Conference bag with the conference program, proceedings, conference gifts, etc.
- Free access to transfer service from hotels to the conference venue and back.

Table of Contents

EISIC 2017 – Conference Organization

Honorary General Chair

Anastasios Zagorianos,

Hellenic Air Force Academy, Greece

General Chair

Panagiotis Karampelas,

Hellenic Air Force Academy, Greece

Program Chair

Joel Brynielsson,

KTH Royal Institute of Technology, Sweden

Track Chairs

Martin Boldt,

Blekinge Institute of Technology, Sweden

Anton Borg,

Blekinge Institute of Technology, Sweden

Lisa Kaati,

Uppsala University, Sweden

Neesha Kodagoda,

Middlesex University London, UK

Margit Pohl,

TU Wien, Austria

B. L. William Wong,

Middlesex University, UK

Publicity Chair

Thirimachos Bourlai,

West Virginia University, USA

Publication Chair

Christos Pavlatos,

Hellenic Air Force Academy, Greece

Local Arrangement Chairs

Ioanna Lekea,

Hellenic Air Force Academy, Greece

EISIC 2017 – Program Committee

Mohd Helmy Abd Wahab
Universiti Tun Hussein Onn Malaysia, Malaysia

Carlo Aliprandi
Integris Srl, Italy

Mohamed Faouzi Atig
Uppsala University, Sweden

Fernando Berzal
University of Granada, Spain

Martin Boldt
Blekinge Institute of Technology, Sweden

Anton Borg
Blekinge Institute of Technology, Sweden

Hervé Borrion
University College London, United Kingdom

Egon L. van den Broek
Utrecht University, Netherlands

Gerhard Budin
University of Vienna, Austria

José Luís Calvo Rolle
University of A Coruña, Spain

David Camacho
Universidad Autónoma de Madrid, Spain

Michał Choraś
ITTI Sp. z o.o., Poland

Christophe Fagot
Intactile Design, France

Shamal Faily
Bournemouth University, United Kingdom

Göran Falkman
University of Skövde, Sweden

Ulrik Franke
RISE SICS Swedish Institute of Computer Science, Sweden

Zeno Geradts
Netherlands Forensic Institute, Netherlands

Helen Gibson
Sheffield Hallam University, United Kingdom

Bénédicte Goujon
Thales Research & Technology, France

Gunther P. Grasemann
Fraunhofer IOSB, Germany

Mohammad Hammoudeh
Manchester Metropolitan University, United Kingdom

Chris Hankin
Imperial College London, United Kingdom

Johan de Heer
Thales Research & Technology, Netherlands

Thomas J. Holt
Michigan State University, USA

Nils Jensen
Ostfalia University of Applied Sciences, Germany

Borka Jerman Blažič
Jožef Stefan Institute, Slovenia

Fredrik Johansson
Swedish Police Authority, Sweden

Jason Jung
Chung-Ang University, Republic of Korea

EISIC 2017 – Program Committee

Lisa Kaati

Uppsala University, Sweden

Sergii Kavun

University of Banking, Kharkiv Educational and Scientific Institute, Ukraine

Jeroen Keppens

King's College London, United Kingdom

Neesha Kodagoda

Middlesex University London, United Kingdom

Ana Kovacevic

University of Belgrade, Serbia

Luca Mazzola

German Research Center for Artificial Intelligence, Germany

Alessandro Moschitti

Qatar Computing Research Institute, HBKU, Qatar

Antonis Mouhtaropoulos

University of Warwick, United Kingdom

Azzam Mourad

Lebanese American University, Lebanon

Federico Neri

Integris Srl, Italy

Arne Norlander

Swedish Armed Forces Headquarters, Sweden

Jakub Piskorski

European Commission Joint Research Centre, Italy

Margit Pohl

TU Wien, Austria

Awais Rashid

Lancaster University, United Kingdom

Christian Reuter

University of Siegen, Germany

Galina Rogova

State University of New York at Buffalo, USA

Günter Schumacher

European Commission Joint Research Centre, Italy

Gerardo I. Simari

Universidad Nacional del Sur, Argentina

David Skillicorn

Queen's University, Canada

Dominik Ślęzak

University of Warsaw, Poland

Ulrik Spak

Swedish Defence University, Sweden

Yannis Stamatiou

University of Patras, Greece

Jerzy Surma

Warsaw School of Economics, Poland

Muhammad Adnan Tariq

KTH Royal Institute of Technology, Sweden

I-Hsien Ting

National University of Kaohsiung, Taiwan

Edward Tjörnhammar

KTH Royal Institute of Technology, Sweden

Róbyn Török

Edith Cowan University, Australia

Theodora Tsikrika

Information Technologies Institute, CERTH, Greece

Stefan Varga

KTH Royal Institute of Technology, Sweden

Cor Veenman

Netherlands Forensic Institute, Netherlands

Jozef Vyskoč

VaF s.r.o., Slovak Republic

Leon Wang

National University of Kaohsiung, Taiwan

Susanne Wetzel

Stevens Institute of Technology, USA

Uffe Kock Wiil

University of Southern Denmark, Denmark

B. L. William Wong

Middlesex University London, United Kingdom

Fatos Xhafa

Technical University of Catalonia, Spain

Moi Hoon Yap

Manchester Metropolitan University, United Kingdom

Lina Zhou

University of Maryland, Baltimore County, USA

EISIC 2017 – Message from the General Chair

We are very pleased to host the European Intelligence and Security Informatics Conference (EISIC) once again in Greece after the Athens conference in 2011 when EISIC first started to be organized annually in various cities across Europe. Until now, EISIC has hosted the research and scientific work of several researchers not only from Europe but also from overseas, becoming a premium venue for research relevant to counterterrorism and criminology. We hope that this tradition will continue this year and that the works to be presented by all the participants will be innovative and interesting.

Regarding the keynotes, this year we have invited a diverse group of speakers from academia, police, and army, emphasizing that the new challenges in the geopolitical scene require close collaboration between these three entities to produce novel dual use technologies. In this respect, the Director of the Cyber Crime Center of the Hellenic Police, Greece, Mr. George Papaprodromou, and the Director of the Cyber Defence Directorate, Hellenic National Defence General Staff, Greece, Mr. Spyros Papageorgiou, will refer to the modus operandi of their groups and the challenges they face every day, while on behalf of the research community novel techniques for contemporary challenges will be presented by Prof. Christos Douligeris (University of Piraeus, Greece) and the recently awarded Dr. Vishal M. Patel (Rutgers University, USA). A novel feature in the conference this year is the organization of a very interesting and controversial panel titled “Ethical Dilemmas in Intelligence

Analysis: Implications for Systems and Operations” with prominent speakers from academia and governmental agencies chaired by Prof. B. L. William Wong (Middlesex University London, United Kingdom) and Dr. Ioanna Lekea (Hellenic Air Force Academy, Greece) with Prof. Stelios Virvidakis (University of Athens, Greece), Dr. Ioanna Lekea (Hellenic Air Force Academy, Greece), Mr. Demosthenis P. Bakopoulos (Ministry of Maritime Affairs, Greece), Dr. Don Gotterbarn (East Tennessee State University, USA), Ms. Samantha Todd (West Midlands Police, United Kingdom) and Prof. Kai Kimppa (University of Turku, Finland) as invited speakers, and financial support from the VALCRI project. Following the panel, a tutorial titled “Ethical Dilemmas in Intel Analysis and Operations and Implications for Systems Design and Development: Individual Rights vs. Security of Society” will take place for the participants who are interested in the topic.

Another particular feature regarding the organization this year is the nature of the conference organizer. EISIC 2017 is organized by the Hellenic Air Force Academy, a military institute of Higher Education which provides education to Hellenic Air Force officers. As a military institute, it is located inside the Dekelia Air Base which was a challenge for the organization of the conference. However, with the support of Air Vice-Marshal Thomas Chatzieuthimiou, the previous Commander of the Hellenic Air Force Academy and now Commander of the Air Training Command, as well as the support of the current Commander of the Hellenic Air Force Academy, Air Vice-Marshal Ioannis Gkontikoulis, who both embraced the idea of organizing an international research and scientific conference in the premises of the Academy, the organization of this conference was rendered feasible. Special reference also needs to be made to the previous commander of the Hellenic Air Force, Air Chief Marshal Christos Vaitsis, and the current commander of the Hellenic Air Force, Air Chief Marshal Christos Christodoulou, who both approved the organization of the conference and provided their full support concerning whatever resource was required for the endeavor. Without their support the organization of the conference would not be possible. Special thanks also need to be attributed to the previous Academic Dean of the Hellenic Air Force Academy, Prof. Petros Kotsiopoulos, and the new Academic Dean, Prof. Anastasios Zagorianos, for their guidance regarding the interaction with the administration services, as well as to Group Captain Mr. Apostolos Moschos who undertook the communication with all the military personnel involved in the organization and to Flight Lieutenant Mr. Athanasios Ntellas for his support regarding the financial services of the conference, Dr. Christos Pavlatos for attending the preparation of the conference program, Dr. Ioanna Lekea for the local organization of the conference and all the Hellenic Air Force Academy personnel who supported this conference.

Last but not least, the scientific committee of the conference needs to be thanked and especially the Program Chair of EISIC 2017, Joel Brynielsson (KTH Royal Institute of Technology, Sweden), who coordinated the scientific work and the communication with the program committee with the assistance of the track chairs who contributed to the scientific preparation of the conference: Martin Boldt (Blekinge Institute of Technology, Sweden), Anton Borg (Blekinge Institute of Technology, Sweden), Lisa Kaati (Uppsala University, Sweden), Neesha Kodagoda (Middlesex University London, United Kingdom), Margit Pohl (TU Wien, Austria) and B. L. William Wong (Middlesex University London, United Kingdom). We are also grateful to our publicity chair Thirimachos Bourlai (West Virginia University, USA) who helped disseminate the call for papers in both Europe and the United States.

Once again, we cordially welcome you to our premises in Dekelia Air Base and we hope that you will enjoy EISIC 2017 and your stay in Athens, Greece.

Panagiotis Karampelas, Hellenic Air Force Academy, Greece

EISIC 2017 – Message from the Program Chair

Intelligence and Security Informatics (ISI) is an interdisciplinary field of research that focuses on the development, use, and evaluation of advanced information technologies, including methodologies, models and algorithms, systems, and tools, for local, national, and international security related applications. Over the past decade, the European ISI research community has matured and delivered an impressive array of research results that are both technically innovative and practically relevant.

Academic conferences have been an important mechanism for building and strengthening the ISI community. The series of international IEEE ISI conferences have been held annually since 2003, and have been followed by regional ISI conferences such as the Pacific Asia ISI (PAISI) workshop series and the European ISI Conference (EISIC) series. These conferences have provided stimulating forums for gathering people from previously disparate communities including those from academia, government, and industry. Participants have included academic researchers (especially in the fields of information technologies, computer science, public policy, and social and behavioral studies), law enforcement and intelligence experts, as well as information technology company representatives, industry consultants and practitioners within the relevant fields.

The 2017 European Intelligence and Security Informatics Conference (EISIC 2017) is the seventh EISIC meeting to be organized by the European ISI community. During 2011–2016 the EISIC meetings have been held annually in Athens, Greece; Odense, Denmark; Uppsala, Sweden; The Hague, the Netherlands; Manchester, United Kingdom; and Uppsala, Sweden. EISIC 2017 is organized by the Hellenic Air Force Academy, and is scientifically sponsored by the Royal Institute of Technology, Sweden and the Swedish Defence Research Agency, and has also received technical co-sponsorship from the IEEE Computer Society and its Technical Committee on Intelligent Informatics (IEEE CS TCII).

We would like to express our sincere gratitude to these sponsors.

EISIC 2017 received 51 submissions in total, and accepted 31% of the papers. For comparison, EuroISI 2008 received 48 submissions and accepted 52% of the papers, EISIC 2011 received 111 submissions and accepted 27% of the papers, EISIC 2012 received 70 submissions and accepted 40% of the papers, EISIC 2013 received 87 submissions and accepted 31% of the papers, IEEE JISIC 2014 received 98 submissions and accepted 28% of the papers, EISIC 2015 received 78 submissions and accepted 35% of the papers, and EISIC 2016 received 64 submissions and accepted 24% of the papers.

The three-day conference program includes presentations by prominent keynote speakers, paper presentation sessions, and poster sessions. We are very pleased with the technical quality of the accepted submissions, and would like to express our sincere gratitude to all authors for contributing their work.

To distinguish between the submitted papers and guide the acceptance decisions, all papers have been carefully read and analyzed by at least three independent experts. Representing all the different flavors of the broad ISI field and coming from 24 different countries, the 66 program committee members generously provided 174 high-quality review reports. We are most grateful to the program committee members for their time spent sharing their valuable expertise with the paper authors.

Joel Brynielsson, KTH Royal Institute of Technology, Sweden

EISIC 2017 – Program at a Glance

Monday, September 11, 2017

08:15-08:30	Bus from Semiramis Hotel to Conference Venue	
08:30-09:00	Registration	
09:00-09:30	**Opening: Welcome Session**	Room: **Auditorium**
09:30-10:30	**Keynote: Active user authentication on mobile devices** Speaker: Vishal M. Patel	Room: **Auditorium**
10:30-11:00	Coffee Break / Poster Session	Foyer
11:00-13:00	**Session: Tools and Techniques for Analyzing Data I**	Room: **Seminar Room 1**
	Session: Criminal Intelligence Analysis	Room: **Seminar Room 2**
13:00-14:00	Lunch Break	Officers' Club
14:00-15:00	**Keynote: Hunting the cyber threats: Intelligence driven Incident response** Speaker: Spyros Papageorgiou	Room: **Auditorium**
15:00-15:30	Coffee Break / Poster Session	Foyer
15:30-17:00	**Session: Tools and Techniques for Analyzing Data II**	Room: **Seminar Room 1**
17:00-17:15	Bus from Conference Venue to Semiramis Hotel	
19:15-19:30	Bus from Semiramis Hotel to Hellenic Air Force Museum and Hellenic Officer's Club	
19:30-22:15	**Social Event**: Hellenic Air Force Museum Visit, Reception at Officer's Club, Dekelia Air Base	
22:15-22:30	Bus from Officers' Club to Semiramis Hotel	

Tuesday, September 12, 2017

08:15-08:30	Bus from Semiramis Hotel to Conference Venue	
08:30-09:00	Registration	
09:00-10:30	**Panel: Ethical Dilemmas in Intelligence Analysis: Implications for Systems and Operations** Chairs: B.L. William Wong & Ioanna Lekea	Room: **Auditorium**
10:30-11:00	Coffee Break	Foyer
11:30-13:00	**Tutorial: Ethical Dilemmas in intel analysis and operations and implications for systems design and development: individual rights vs. security of society**	Room: **Seminar Room 1**
	Session: Criminal Analysis & Detection I	Room: **Seminar Room 2**
13:00-14:00	Lunch Break	Officers' Club
14:00-15:00	**Keynote: Effective Prevention and Investigation of Cybercrime** Speaker: Georgios Papaprodromou	Room: **Auditorium**
15:00-15:30	Coffee Break	Foyer
15:30-16:30	**Session: Tools and Techniques for Analyzing Data III**	Room: **Seminar Room 1**
	Session: Criminal Analysis & Detection II	Room: **Seminar Room 2**
16:30-16:45	Bus from Conference Venue to Semiramis Hotel	
18:15-19:30	Kifisia Metro Station to Evangelismos Metro Station (Detailed instructions in Full Conference Program)	
19:30-21:30	**Social Event**: Gala Dinner at Hellenic Armed Forces Officers Club (Rigillis 1 & Vasilissis Sofias (Pavlos Melas Square), Athens 10675)	

Wednesday, September 13, 2017

08:15-08:30	Bus from Semiramis Hotel to Conference Venue	
08:30-09:00	Registration	
09:00-10:00	**Keynote: Modelling of Supply Chain Service Systems' Security** Speaker: Christos Douligeris	Room: **Auditorium**
10:00-10:30	Coffee Break	Foyer
10:30-12:30	**Session: Models and Tools for Intelligent Decision Making**	Room: **Seminar Room 1**
	Session: Criminal Analysis & Detection III	Room: **Seminar Room 2**
12:30-13:30	Lunch Break	Officers' Club
13:45-14:00	Bus from Conference Venue to Semiramis Hotel	

Vishal M. Patel
Rutgers University, USA

09:30-10:30 Monday, 11 September 2017 Room: Auditorium Chair: Joel Brynielsson

"Active user authentication on mobile devices"

Abstract

Recent developments in sensing and communication technologies have led to an explosion in the use of mobile devices such as smartphones and tablets. With the increase in use of mobile devices, one has to constantly worry about the security and privacy, as the loss of a mobile device would compromise personal information of the user. To deal with this problem, active authentication (also known as continuous authentication) systems have been proposed in which users are continuously monitored after the initial access to the mobile device. This talk will provide an overview of different continuous authentication methods on mobile devices. We will discuss merits and drawbacks of available approaches and identify promising avenues of research in this rapidly evolving field.

Bio

Vishal M. Patel is an A. Walter Tyson Assistant Professor in the Department of Electrical and Computer Engineering at Rutgers University. Prior to joining Rutgers University, he was a member of the research faculty at the University of Maryland Institute for Advanced Computer Studies (UMIACS). He completed his Ph.D. in Electrical Engineering from the University of Maryland, College Park, MD, in 2010. His current research interests include signal processing, computer vision, and pattern recognition with applications in biometrics and imaging. He has received a number of awards including the 2016 Office of Naval Research (ONR) Young Investigator Award, the 2016 Jimmy Lin Award for Invention, A. Walter Tyson Assistant Professorship Award, the Best Paper Award at IEEE BTAS 2015, and Best Poster Awards at BTAS 2015 and 2016. He currently serves as a member of the Information Forensics and Security Technical Committee of the IEEE Signal Processing Society and Associate Editor of the IEEE Biometrics Compendium. He is a member of Eta Kappa Nu, Pi Mu Epsilon, and Phi Beta Kappa.

Spyros Papageorgiou

Cyber Defence Directorate, Hellenic National Defence General Staff, Greece

14:00-15:00 Monday, 11 September 2017 Room: Auditorium Chair: Antonios Andreatos

"Hunting the cyber threats: Intelligence driven Incident response"

Abstract

The adversaries are always steps ahead of us. They use unknown tools, tactics and procedures to compromise our systems and networks. Their goal is to steal our data. Our mission is to stop them completing their mission. In order to be close to them we must develop skills to defend actively our networks. Active defense is the reaction to an attack. It is not hack back. There is no security without detection and no protection without reaction. Active defense is the Intelligence driven incident response. Deploying Intelligence driven incident response, we can respond to an incident both proactively by hunting the unknown threats and also reactively when an incident alert occurs. Working both proactively and reactively we are closer to the attackers and we reduce the amount of time, necessary to detect and locate advanced persistent threats (unknown threats).

Bio

Navy Captain Spyridon Papageorgiou, MSc (Computer Science), present Assignment: Director of Cyber Defense Directorate. Navy Captain Papageorgiou has significant experience (more than 16 years) in information security and cyber defense research and implementations. He is responsible for organizing National Cyber Defense Exersice and Cyber Defense School. He is GIAC Certified Security Professional (Incident Handling, Reversing Malware, System and Network Penetration Tester, Forensics analyst). He teaches as an expert in the University of Piraeus, Windows Forensics and System Penetration testing.

Since 2013, he has been member of the red team in the Cyber Defense Exercise "LOCKED Shields", organized by the NATO Cooperative Cyber Defense Centre of Excellence. He is a regular speaker regarding cyber security and cyber defense presentations at Suprime Joint War College (ADISPO) and also at Hellenic National Defense College.

Georgios Papaprodromou
Cyber Crime Center of the Hellenic Police, Greece

14:00-15:00 Tuesday, 12 September 2017 Room: Auditorium Chair: Panagiotis Karampelas

"Effective Prevention and Investigation of Cybercrime"

Abstract

During the lecture, the lecturer will analyze the mission and the goals of the Hellenic Police HQ Cybercrime Division, will emphasize on the offenses committed in the Cyberspace and present relevant statistics. The lecture will also include issues of the existing legal framework concerning the cybercrime, what is happening in Greece and in Europe. Finally, the lecturer will present the development of preventive and raise awareness actions carried out by the Hellenic Police HQ Cybercrime Division.

Bio

Police Director PAPAPRODROMOU Georgios was born in 1965 at Giannitsa Pellas. He joined the Hellenic Police in 1984. He served as an officer in numerous but also special services mainly in Northern Greece. He is a graduate of the Law Faculty of the Aristotle University of Thessaloniki. He is an expert as Forensic Document Examiner, having served since 1999 in the Laboratory Department of the Forensic Division of the Hellenic Police Headquarters. At the same time, he was the founder (2002) of the Laboratory of Forensic Document Examination in Forensic Subdivision of Northern Greece, in which he served until 2011. From 20-08-2015 until 26-05-2016 he served as Director of the newly-established Cyber Crime Subdivision of Northern Greece. From 27-05-2016 until today he is the Director of the Cyber Crime Division of the Hellenic Police Headquarters.

He is a graduate of the Joint War College (12th Educational Series) as well as an e-student of the National Defense School (7th Educational Series). He has been trained, among other things, in Organization and Management and in new Information and Communication Technologies (ICT), on e-Government, Forensics, Radicalization, Civil Protection, Critical Infrastructure and anti-drug policies. He has taught courses in Public Institutes of Vocational Training and in various schools of the Police Academy. He speaks English and German. He is married, having two (2) children, students in the Department of Applied Informatics and in the Law Faculty, Aristotle University of Thessaloniki.

Christos Douligeris

University of Piraeus, Greece

09:00-10:00 Wednesday, 13 September 2017 Room: Auditorium Chair: B.L. William Wong

"Modelling of Supply Chain Service Systems' Security"

Abstract

A Supply Chain Service (SCS) is a complex network of interconnected business partners, including all the information, processes and assets required for the movement of goods and the performance of services. However, the smooth operation of an SCS could suffer from interruptions and delays due to a variety of reasons ranging from acknowledged business and financial factors (e.g. frequent changes in business partners' leadership and demand uncertainty) to the exploitation of physical threats (e.g. bombing of a storage room) and/or cyber threats (e.g. gaining unauthenticated access to an alarm system and changing the alarm settings). Cyber threat exploitation results from the lack of implemented security controls, making the assets vulnerable to these threats.

This lecture introduces a process-centric approach for modelling security concepts in order to improve Supply Chain sustainability. We focus on the Vehicle Transport Service (VTS) and we present a business-process oriented model. In order to show how security issues can be visualized we apply simulation techniques on the developed process models. The three model infrastructures are component materials of the MITIGATE EU project, which has a goal the development of a platform that provides risk assessment techniques in critical maritime cyber assets aiming to manage risks that could compromise the organization's information security.

Bio

Christos Douligeris, currently a professor at the department of Informatics, University of Piraeus, Greece held positions with the Department of Electrical and Computer Engineering at the University of Miami. He was an associate member of the Hellenic Authority for Information and Communication Assurance and Privacy and the President and CEO Hellenic Electronic Governance for Social Security SA. Dr. Douligeris has published extensively in the networking scientific literature and he has participated in many research and development projects. He is the co-editor of a book on ''Network Security'' published by IEEE Press/ John Wiley and he is on the editorial boards of several scientific journals as well as on the technical program committees of major international conferences. He has been involved extensively in curriculum development both in the USA and Greece. His latest work has focused on the use of big data and artificial intelligence techniques in several areas, mainly in Telecommunications Planning and Management and in Security Analysis of Port Information Systems. Moreover, he has been working in data analytic techniques in Learning and Education and Emergency Response Operations.

Panel			
09:00-10:30	Tuesday, 12 September 2017	Room: Auditorium	Chairs: *B.L. William Wong &* *Ioanna Lekea* Participants *Stelios Virvidakis* *Demosthenis P. Bakopoulos* *Don Gotterbarn* *Kai Kimppa*

"Ethical Dilemmas in Intelligence Analysis: Implications for Systems and Operations"

Overview

The field of ethics is concerned with the study of the concepts of right and wrong behaviour, and generally involves three broad subject areas: metaethics, normative ethics, and applied ethics. Metaethics investigates where our ethical principles come from, and what they mean; normative ethics refer to our study and determination of moral standards that regulate right and wrong conduct; while applied ethics involves the examination of specific controversial issues such as abortion, animal rights, environmental concerns. In this panel, we will identify and discuss ethics issues as they apply to a number of emergent challenges in the design and development of intelligence analysis systems, as well as during day-to-day operations of law enforcement and military officers. In many discussions on ethics, there is a tendency for the discussions to remain at a high level and surround the main principles of ethics, e.g. respect for autonomy, non-maleficence or do no harm, beneficence, and justice (Beauchamp & Childress, 2013). In this panel, we present some concrete problems that emerged through our research in projects such as the FP7 VALCRI, as we seek to respect the rights of European citizens to liberty and security. These problems include the mosaic effect, protection of personal data, potential mis-use and abuse during information exploitation and analysis activities encountered during intelligence and investigative analysis. How should we design to ensure computational and analytic transparency in the decision making processes? How we design systems and processes that are visible and open to inspection by colleagues and overseers? These are some issues that will be addressed by this Panel.

Participants

1. Ethical Issues in Intelligence Analysis and Surveillance for Defense Purposes: The Deontological vs the Consequentialist Approach (or When Principles are More Important than Consequences)

Stelios Virvidakis, University of Athens; and Ioanna K. Lekea, Hellenic Air Force Academy

Abstract

When making decisions, people usually adopt a consequentialist perspective, which means that they mainly focus on the outcomes of their actions (or inaction). The idea that there are certain moral principles or duties that prohibit specific forms of behavior (irrespectively of the individual's presumption concerning the probability of a bad outcome actually coming true) is usually a factor omitted or ignored in the equation. Also, people tend to be quite protective when their own individual rights are at stake or in question, while the same does not apply when they discuss other people's rights (especially when those others are considered as the enemy).

After the 9-11 attacks and over the last decade, in the wake of terrorist acts in various places around the world, a counter-terrorism debate has arisen on how to decide whether and when it is morally permissible to set aside the individual's right to privacy. The issue of Intel analysis and surveillance of specific individuals, usually deemed (or marked out due to ideological or religious beliefs) as suspects of planning or executing a dangerous act against the common good, has come into the foreground. For many people, under the terrorism threat, the infringement of the right to privacy could be justified; intruding into a suspect's life is considered/regarded as the morally right thing to do and a governmental duty of the utmost importance in order to prevent bad things from happening and, thus, to protect civilians from an unjust terrorist attack.

Obviously, the former approach is based on the assumption that it is morally acceptable (or even permissible) to go wrong against one person (: a suspect that equals to a potential terrorist) if the aim is to protect the majority of (innocent) people. So all people are not created equal with regard to the right of privacy. But how many should you expect to save in order to justify sacrificing one person's rights ? And are there really clear established criteria so as to detect a potential terrorist? Where should someone draw the line between the status of an innocent person and a suspect (who might not be innocent beyond reasonable doubt, but is not obviously guilty too)? And who is to decide on how to treat the suspect?

We will focus on consequentialist arguments to show that this approach might prove a dangerous slippery slope undermining the effort of our society to honor individuals rights and to discriminate between innocent/guilty, non-combatants/combatants. We will then try to discuss the right to privacy using the deontological approach, according to which the intrinsic characteristics of actions and rules are more important than their consequences, so even when in extremely critical situations one should hold true to his moral obligation to do what is right.

Bios

Stelios Virvidakis, Department of Philosophy and History of Science, University of Athens, is Professor of Philosophy at the Department of Philosophy and History of Science of the University of Athens. He studied philosophy at the University of Athens, at the University of Paris I and at Princeton University. His publications include books in metaethics, textbooks for the teaching of philosophy in Greek highschools and many articles in Greek, in French and in English, mainly in the areas of ethics, epistemology, metaphilosophy and the history of philosophy.

Ioanna K. Lekea, Department of Aeronautical Sciences, Hellenic Air Force Academy, holds a BA (Hons) in Classics from the University of Athens, a MSc in History and Philosophy of Science and Technology and a Ph.D. in Military Ethics awarded jointly by the University of Athens and the National Technical University of Athens. She currently works as a lecturer with the Hellenic Air Force Academy and teaches Military Ethics and Just War Theory. She also works as a researcher at the War Games Lab of the Hellenic Air Force Academy focusing on the development of simulation games and their application to teaching scientific areas such as: military ethics, crisis management, prediction and prevention of terrorism activities using computer-aided techniques. Her publications include books and papers related to Just War Theory, simulations and computer-based programs for educational and research purposes, the war against terrorism and human rights, military history.

2. The Right to Privacy within the Context of Space Technology Evolution

Demosthenis P. Bakopoulos, Ministry of Maritime Affairs, Greece

Abstract

The right to privacy or in other words the right to be left alone has been considered as a fundamental human right for more than 150 years. The evolution of technology challenged its validity, because law enforcement authorities used sensors and scaners placed on board aircrafts to combat criminality. Surprisingly enough, case-law never seriously complained for the new police capabilities for peripheral reconnaisance, even when the asylum residence could not be guaranteed and protected. Within the context of the controversial "war against terror", space reconnaisance data, i.e. data related to peoples everyday life, were used not only for the surveillance of suspected terrorists, but for their murder as well. The proposed presentation will analyze the legal rules of such space data use and challenge the ethics behind the rules.

Bio

Demosthenis P. Bakopoulos is a Lawyer registered in Athens Bar Association since 2001. After his postgraduate studies in International Air and Space Law, he worked for 15 years as a legal advisor of Hellenic Air Force and he continued his career at Hellenic Ministry of Defense as a legal advisor to the Minister of Defense until June 2012. He is a Scientific Expert of Hellenic Air Force Academy on International Aerospace Law and International Humanitarian Law. He is the author of the following books: (i) Introduction to Law of Air Warfare and International Space Law, 2010; (ii) Public Contracts on Defense and Security Sectors, 2013. Mr. Bakopoulos is the Commander of Ports Public Authority since April 2017.

3. Reducing Soft Errors

Don Gotterbarn, East Tennessee State University, USA

Abstract

Automated decision support systems like VALCRI help structure complex data to facilitate difficult decisions but unless explicitly addressed these automated systems can, in fact, facilitate and encourage ethical lapses; ethical lapses which are not intended nor recognized by the well-intentioned analyst.

To proactively identify and developing ethical safeguards the VALCRI project used an internal group to address social, privacy and legal issues and a group of computer ethics specialists in an independent ethics board. They asked if the product is ethically viable and does it mitigate known ethical problems. Thy identified modifications to the design and development which could be addressed by the system developers. This required ethical design beyond mere technological solutions. The built-in ethical safeguards needed to have the system both identify and either prevent or alert individuals to alter their decision strategies.

Amongst the difficulties identified are analyst overconfidence in the “computerized” results and visual thinking techniques encouraging rapid insightful analysis affecting the investigator’s obligation to produce 'communicable knowledge' which can be used by others.

The visual analytic techniques and thinking increase the analyst’s overconfidence requiring modifications like recording the competence level of the analysts. But this left open issues of information bias- a tendency to ignore disconfirming instances. A system needs to make clear when potential weak relationships

However, using skill level indicators does not resolve the overconfidence problem. Research shows that when a decision makers experience level is low that they base their decision on the empirical data (explicit information), whereas those with a high or medium experience level focus on their previous experiences (implicit information) and have a tendency to ignore disconfirming evidence. Using skill levels as criteria may encourage later analysts to suffer from overconfidence bias.

Techniques for addressing the obligation to produce 'communicable knowledge' which can be used by others helps to reduce overconfidence bias. Modifying the system so it supports transparently handling chains of reasoning- recording the reasons for decisions and connections made by the investigator- helps to develop communicable knowledge. This modification addresses overconfidence in the computerized decision. One of the trade-offs in requiring a recounting of the reasoning process is that the verbalization may be in tension with the creative rapid visual recognition thinking encouraged by a visual analytics.

The complexity of these systems is evident in the attempt to resolve one form of bias may introduce another. We are still addressing the interplay of the ethical issues and various technical solution to them.

Bio

Don Gotterbarn is Professor Emeritus at East Tennessee State University, the Director of the Software Engineering Ethics Research Institute, and visiting professor at the Centre for Computing and Social Responsibility, UK and works as an expert witness in computer cases. His work as a computer consultant includes international software projects for the U.S. Navy, the Saudi Arabian Navy, and the European Union. Projects included decision support systems, vote counting machines, and missile defense systems. He was a visiting scientist at Carnegie Mellon's Software Engineering Institute and did special training for the National Security Agency- USA and TATA Consultancy Services- India. He has been active as a researcher and participant promoting professional computer standards and ethics for over 25 years. He chaired the committee that wrote the Software Engineering Code of Ethics and Professional Practice.

4. Lost in Translation: Showing Trustworthiness of Computation

Kai Kimppa, Turku University, Finland

Abstract

In systems which take a large amount of data and present it visualised in a condensed format, it is necessary to carefully consider what might get lost in transition from one representation format to another and how to make sure the user does not over simplify the results they are shown. It is important to have a method for the user to see the level of trustworthiness of the end-result and that they can go back to a more detailed level and verify that the conclusions based on the visualisation are correct.

This is especially relevant if the system is used by persons either not aware of this or in a situation where they do not have time to check the relevant data for accuracy. This might happen if the users are not aware of all the necessary steps to verify their work or systems like this may be used in an environment where they were originally not meant for.

Due to these reasons it is of paramount importance that advanced decision support systems like VALCRI are not delivered to use without proper verification of the users' ability to use them, in environments to which the systems are not designed for.

Bios

Kai Kimppa has a PhD in the field of Information Technology Ethics and is working as a postdoctoral researcher at the University of Turku. His specific areas are IPRs, eGovernment and eHealth applications and Computer Games in relation to Ethics. He has worked in the industry (Nokia Mobile Phones) as a Design Engineer, and teaches Information Systems Science, Usability and User Interface Design on top of IT and Ethics.

B.L. William Wong PhD FNZCS FBCS is professor of Human Computer Interaction and head of the Interaction Design Centre, Middlesex University London. His research interest is in cognitive engineering and the representation design of user interfaces that enhance information uptake, sense-making, situation awareness, reasoning, and decision making in dynamic environments. His research has included studies in air traffic control, hydro-electricity dispatch, emergency ambulance control, and intelligence analysis. He has received over US$25.3 million in research grants. He is currently Project Coordinator for the 17-partner EU FP7 project VALCRI, Visual Analytics for sense-making in Criminal Intelligence Analysis. He has led other multi-partner projects including FP7 CRISIS, US-UK funded UKVAC, and Eurocontrol 3D-in-2D. He has published over 100 scientific peer reviewed articles with his students and colleagues.

Tutorial			
11:00-13:00	Tuesday, 12 September 2017	Room: Seminar Room 1	Chairs: *B.L. William Wong &* *Ioanna Lekea*

"Ethical Dilemmas in intel analysis and operations and implications for systems design and development: individual rights vs security of society"

Description

Part 1

Introduction to ethical principles and ethical issues in intelligence analysis and counter-terrorism - this will be based on a series of short lectures given by some members of the panel to introduce tutorial participants on how to recognise ethical issues and the dilemmas they present

Part 2

The participants will be divided into groups, they will be given one case study / simulation, with the aim to identify and explain the ethical issues. At the end of the session, all groups would come together to present their findings and what lessons they have learnt.

Monday, September 11, 2017

08:15-08:30		Bus from Semiramis Hotel to Conference Venue
08:30-09:00		Registration
09:00-09:30		**Opening: Welcome Session** Auditorium
09:30-10:30		**Keynote: Active user authentication on mobile devices** Speaker: Vishal M. Patel, Auditorium, Chair: Joel Brynielsson
10:30-11:00		Coffee Break / Poster Session
11:00-13:00		**Session: Tools and Techniques for Analyzing Data I**
	Seminar Room 1	Chair: David Camacho
		Cyberbullying System Detection and Analysis Yee Jang Foong and Mourad Oussalah
		Gender Classification with Data Independent Features in Multiple Languages Tim Isbister, Lisa Kaati, and Katie Cohen
		Author Profiling in the Wild Lisa Kaati, Elias Lundeqvist, Amendra Shrestha, and Maria Svensson
		Are We Really That Close Together? Tracing and Discussing Similarities and Differences between Greek Terrorist Groups Using Cluster Analysis Ioanna Lekea and Panagiotis Karampelas
11:00-13:00		**Session: Criminal Intelligence Analysis**
	Seminar Room 2	Chair: Theodora Tsikrika
		An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling Erik T. Zouave and Thomas Marquenie
		How Analysts Think: How Do Criminal Intelligence Analysts Recognise and Manage Significant Information? Celeste Groenewald, B. L. William Wong, Simon Attfield, Peter Passmore,and Neesha Kodagoda
		A Survey of Intelligence Analysts' Perceptions of Analytic Tools Mandeep K. Dhami
		Behavioural & Tempo-Spatial Knowledge Graph for Crime matching through Associative Questioning and Graph theory Nadeem Qazi and B. L. William Wong
		Behavioural Markers: Bridging the Gap Between Art of Analysis and Science of Analytics In Criminal Intelligence Junayed Islam and B. L. William Wong
13:00-14:00		Lunch Break Officers' Club
14:00-15:00		**Keynote: Hunting the cyber threats: Intelligence driven Incident response** Speaker: Spyros Papageorgiou, Auditorium, Chair: Antonios Andreatos
15:00-15:30		Coffee Break / Poster Session
15:30-17:00		**Session: Tools and Techniques for Analyzing Data II**
	Seminar Room 1	Chair: Lisa Kaati
		Adversarial Machine Learning in Malware Detection: Arms Race between Evasion Attack and Defense Lingwei Chen, Yanfang Ye, and Thirimachos Bourlai
		Text Mining in Unclean, Noisy or Scrambled Datasets for Digital Forensics Analytics Konstantinos Xylogiannopoulos, Panagiotis Karampelas, and Reda Alhajj
		Detecting Periodic Subsequences in Cyber Security Data Matthew Price-Williams, Nick Heard, and Melissa Turcotte
17:00-17:15		Bus from Conference Venue to Semiramis Hotel
19:15-19:30		Bus from Semiramis Hotel to Hellenic Air Force Museum and Hellenic Officer's Club
19:30-22:15		**Social Event**: Hellenic Air Force Museum Visit, Reception at Officer's Club, Dekelia Air Base
22:15-22:30		Bus from Officers' Club to Semiramis Hotel

Tuesday, September 12, 2017

08:15-08:30	Bus from Semiramis Hotel to Conference Venue
08:30-09:00	Registration
09:00-10:30	**Panel: Ethical Dilemmas in Intelligence Analaysis: Implications for Systems and Operations** Chairs: B.L. William Wong & Ioanna Lekea
10:30-11:00	Coffee Break
11:00-13:00	**Tutorial: Ethical Dilemmas in intel analysis and operations and implications for systems design and development: individual rights vs. security of society**
Seminar Room 1	Chair: B.L. William Wong & Ioanna Lekea
	Part I Introduction to ethical principles and ethical issues in intelligence analysis and counter-terrorism - this will be based on a series of short lectures given by some members of the panel to introduce tutorial participants on how to recognise ethical issues and the dilemmas they present
	Part II The participants will be divided into groups, they will be given one case study / simulation, with the aim to identify and explain the ethical issues. At the end of the session, all groups would come together to present their findings and what lessons they have learnt.
11:00-13:00	**Session: Criminal Analysis & Detection I**
Seminar Room 2	Chair: Thirimachos Bourlai
	Detecting Crime Series Based on Route Estimation and Behavioral Similarity Anton Borg, Martin Boldt, and Johan Eliasson
	An integrated framework for the timely detection of petty crimes Nikolaos Dimitriou, George Kioumourtzis, Anargyros Sideris, Georgios Stavropoulos, Evdoxia Taka, Nikolaos Zotos, George Leventakis, and Dimitrios Tzovaras
	A Statistical Method for Detecting Significant Temporal Hotspots Using LISA Statistics Martin Boldt and Anton Borg
13:00-14:00	Lunch Break Officers' Club
14:00-15:00	**Keynote: Effective Prevention and Investigation of Cybercrime** Speaker: Georgios Papaprodromou, Auditorium, Chair: Panagiotis Karampelas
15:00-15:30	Coffee Break
15:30-16:30	**Session: Tools and Techniques for Analyzing Data III**
Seminar Room 1	Chair: Neesha Kodagoda
	IoT Data Profiles: The Routines of Your Life Reveals Who You Are Johan Fernquist, Torbjörn Fängström, and Lisa Kaati
	Interpretable Probabilistic Divisive Clustering of Large Node-Attributed Networks Lisa Kaati and Adam Ruul
15:30-16:30	**Session: Criminal Analysis & Detection II**
Seminar Room 2	Chair: Anton Borg
	Towards a breakthrough speaker identification approach for law enforcement agencies Khaled Khelif, Yann Mombrun, Gerhard Backfried, Farhan Sahito, Luca Scarpato, Petr Motlicek, Srikanth Madikeri, Damien Kelly, Gideon Hazzani, and Emmanouil Chatzigavriil
	Period Analysis and Trend Forecast of Terrorism in SCO Region by Wavelet Transform Ze Li, Duoyong Sun, Bo Li, and Wei Ding
16:30-16:45	Bus from Conference Venue to Semiramis Hotel
18:15-19:30	Kifisia Metro Station to Evangelismos Metro Station (Detailed instructions in Full Conference Program)
19:30-22:00	**Social Event**: Gala Dinner at Hellenic Armed Forces Officers Club (Rigillis 1 & Vasilissis Sofias (Pavlos Melas Square), Athens 10675)

Wednesday, September 13, 2017	
08:15-08:30	Bus from Semiramis Hotel to Conference Venue
08:30-09:00	Registration
09:00-10:00	**Keynote: Modelling of Supply Chain Service Systems' Security** Speaker: Christos Douligeris, Auditorium, Chair: B.L. William Wong
10:00-10:30	Coffee Break
10:30-12:30	**Session: Models and Tools for Intelligent Decision Making**
Seminar Room 1	Chair: Panagiotis Karampelas
	Cyber Threat Intelligence Model: An Overview of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence Vasileios Mavroeidis and Siri Bromander
	Large Scale Data Collection of Tattoo-Based Biometric Data from Social-Media Websites Michael Martin, Jeremy Dawson, and Thirimachos Bourlai
	A Framework for Measuring Imagination in Visual Analytics Systems Michael A. Bedek, Alexander Nussbaumer, Eva-C. Hillemann, and Dietrich Albert
	Catchem: A Browser Plugin for the Panama Papers Using Approximate String Matching Panos Kostakos, Miika Moilanen, Arttu Niemelä, and Mourad Oussalah
10:30-12:30	**Session: Criminal Intelligence Analysis**
Seminar Room 2	Chair: Martin Boldt
	Customs Risk Analysis through the ConTraffic Visual Analytics tool Mikaela Poulymenopoulou and Aris Tsois
	Comparative Analysis of Crime Scripts: One CCTV Footage—Twenty-One Scripts Hervé Borrion, Hashem Dehghanniri, and Yuanxi Li
	Whose Hands Are in the Finnish Cookie Jar? Jukka Ruohonen and Ville Leppänen
12:30-13:30	Lunch Break Officers' Club
13:45-14:00	Bus from Conference Venue to Semiramis Hotel

Session: Tools and Techniques for Analyzing Data I

11:00-13:00 Monday, September 11, 2017 Room: Seminar Room 1 Chair: David Camacho

Paper I Full

Cyberbullying System Detection and Analysis

Yee Jang Foong and Mourad Oussalah

Cyber-bullying has recently been reported as one that causes tremendous damage to society and economy. Advances in technology related to web-document annotation and the multiplicity of the online communities renders the detection and monitoring of such cases rather difficult and very challenging. This paper describes an online system for automatic detection and monitoring of Cyberbullying cases from online forums and online communities. The system relies on the detection of three basic natural language components corresponding to Insults, Swears and Second Person. A classification system and ontology like reasoning have been employed to detect the occurrence of such entities in the forum / web documents, which would trigger a message to security in order to take appropriate action. The system has been tested on two distinct forums and achieves reasonable detection performances.

Paper II Full

Gender Classification with Data Independent Features in Multiple Languages

Tim Isbister, Lisa Kaati and Katie Cohen

Gender classification is a well-researched problem, and state-of-the-art implementations achieve an accuracy of over 85%. However, most previous work has focused on gender classification of texts written in the English language, and in many cases, the results cannot be transferred to different datasets since the features used to train the machine learning models are dependent on the data. In this work, we investigate the possibilities to classify the gender of an author on five different languages: English, Swedish, French, Spanish, and Russian. We use features of the word counting program Linguistic Inquiry and Word Count (LIWC) with the benefit that these features are independent of the dataset. Our results show that by using machine learning with features from LIWC, we can obtain an accuracy of 79% and 73% depending on the language. We also, show some interesting differences between the uses of certain categories among the genders in different languages.

Paper III Short

Author Profiling in the Wild

Lisa Kaati, Elias Lundeqvist, Amendra Shrestha and Maria Svensson

In this paper, we use machine learning for profiling authors of online textual media. We are interested in determining the gender and age of an author. We use two different approaches, one where the features are learned from raw data and one where features are manually extracted. We are interested in understanding how well author profiling works in the wild and therefore we have tested our models on different domains than they are trained on. Our results show that applying models to a different domain then they were trained on significantly decreases the performance of the models. The results show that more efforts need to be put into making models domain independent if techniques such as author profiling should be used operationally, for example by training on many different datasets and by using domain independent features.

Paper IV Short

Are we Really that Close Together? Tracing and Discussing Similarities and Differences between Greek Terrorist Groups using Cluster Analysis

Ioanna Lekea and Panagiotis Karampelas

This paper discusses the similarities and differences in both ideology expressed and practices employed by two terrorist groups that operated in Greece between the years of 1975 and 2017: Revolutionary Organization 17 November and Conspiracy of Fire Nuclei. Within this line of thought, we will briefly provide an outline of the political and ideological framework of the groups on focus in an effort to place them within the general historical and political context. We will then focus on the justification and deployment of the terrorist operations as presented in the communiqués published, as well as other announcements and notes distributed in the Social Media by the members of those two terrorist groups. In this context, we elaborate on the tactics of the terrorist groups: their targets, the weapons used and the consequences suffered as a result of their actions are analyzed, in order to evaluate their ideological and – perhaps - ethical standing. To analyze the communiqués of both organizations, two different text mining clustering techniques were applied and the outcomes enabled us to run a comparison between the two terrorist groups and also to examine the possibility of related means, ideology and people behind their different name.

Session: Criminal Intelligence Analysis			
11:00-13:00	Monday, September 11, 2017	Room: Seminar Room 2	Chair: Theodora Tsikrika

Paper I Full

An Inconvenient Truth: Algorithmic Transparency & Accountability in Criminal Intelligence Profiling

Erik T. Zouave and Thomas Marquenie

In the hopes of making law enforcement more effective and efficient, police and intelligence analysts are increasingly relying on algorithms underpinning technology-based and data-driven policing. To achieve these objectives, algorithms must also be accurate, unbiased and just. In this paper, we examine how European data protection law regulates automated profiling and how this regulation impacts police and intelligence algorithms and algorithmic discrimination. In particular, we assess to what extent the regulatory frameworks address the challenges of algorithmic transparency and accountability. We argue that while the law regulates both algorithms and their discriminatory effects, the framework is insufficient in addressing the complex interactions that must take place between system developers, users, oversight and profiled individuals to fully guarantee algorithmic transparency and accountability.

Paper II Full

How Analysts Think: How do Criminal Intelligence Analysts Recognise and Manage Significant Information?

Celeste Groenewald, B.L. William Wong, Simon Attfield, Peter Passmore and Neesha Kodagoda

The Criminal Intelligence Analyst's role is to create exhibits which are relevant, accurate and unbiased. Exhibits can be used as input to assist decision-making in intelligence-led policing. It may also be used as evidence in a court of law. The aim of this study was to determine how Criminal Intelligence Analysts recognise and manage significant information as a method to determine what is relevant for their attention and for the creation of exhibits. This in turn may provide guidance on how to design and incorporate loose and flexible argumentation schemas into sense-making software. The objective is to be informed on how to design software, which affords Criminal Intelligence Analysts with the ability to effortlessly determine the relevance of information, which subsequently could assist with the process of assessing and defending the quality of exhibits.

Paper III Short

A Survey of Intelligence Analysts' Perceptions of Analytic Tools

Mandeep K. Dhami

This article presents a survey of 278 intelligence analysts' views of fully operational analytic technologies and their newly developed replacements. It was found that usability was an important concept in analysts' reasons for and against using analytic tools. The perceived usability of a tool was not necessarily indicative of its perceived usefulness. Analysts' decisions to recommend an analytic tool to others were best predicted by how usable analysts perceived the tool to be rather than how useful they considered the tool to be. These findings have implications for the development and implementation of new analytic technologies in the intelligence community.

Paper IV Short

Behavioural & Tempo-Spatial Knowledge Graph for Crime matching through Associative Questioning and Graph theory

Nadeem Qazi and B.L. William Wong

Crime matching process usually involves the time tedious and information intensive task of eliciting plausible associations among actors of crimes to identify potential suspects. Aiming towards the assistance of this procedure, we in this paper have exhibited the utilization of associative search; a relatively new search mining instrument to evoke conceivable associations from the information. We have demonstrated the use of threedimensional, i.e. spatial, temporal, and modus operandi based similarity matching of crime pattern to establish hierarchical associations among the crime entities. Later we used these to extract plausible suspect list for an unsolved crime to facilitate the crime matching process. A knowledge graph consisting of tree structure coupled with the iconic graphic is used to visualize the plausible list. Additionally, a similarity score is calculated to rank the suspect in the plausible list. The proposed visualization aims to assist in hypothesis formulation reducing computational influence in the decision making of criminal matching process.

Paper V Short

Behavioural Markers: Bridging the Gap Between Art of Analysis and Science of Analytics In Criminal Intelligence

Junayed Islam and B. L. William Wong

Studying how intelligence analysts use interaction in visualization systems is an important part of evaluating how well these interactions support analysis needs, like generating insights or performing tasks. Intelligence analysis is inherently a fluid activity involving transitions between mental and interaction states through analytic processes. A gap exists to complement these transitions at micro-analytic level during data exploration or task performance. We propose Behavioural markers (BMs) which are representatives of the action choices that analysts make during their analytical processes as the bridge between human cognition and computation through semantic interaction. A low level semantic action sequence computation technique has been proposed to extract these BMs from captured process log. Our proposed computational technique can supplement the problems of existing qualitative approaches to extract such BMs.

Session: Tools and Techniques for Analyzing Data II

15:30-17:00 Monday, September 11, 2017 Room: Seminar Room 1 Chair: Lisa Kaati

Paper I Full

Adversarial Machine Learning in Malware Detection: Arms Race between Evasion Attack and Defense

Lingwei Chen, Yanfang Ye and Thirimachos Bourlai

Since malware has caused serious damages and evolving threats to computer and Internet users, its detection is of great interest to both anti-malware industry and researchers. In recent years, machine learning-based systems have been successfully deployed in malware detection, in which different kinds of classifiers are built based on the training samples using different feature representations. Unfortunately, as classifiers become more widely deployed, the incentive for defeating them increases. In this paper, we explore the adversarial machine learning in malware detection. In particular, on the basis of a learning-based classifier with the input of Windows Application Programming Interface (API) calls extracted from the Portable Executable (PE) files, we present an effective evasion attack model (named EvnAttack) by considering different contributions of the features to the classification problem. To be resilient against the evasion attack, we further propose a secure-learning paradigm for malware detection (named SecDefender), which not only adopts classifier retraining technique but also introduces the security regularization term which considers the evasion cost of feature manipulations by attackers to enhance the system security. Comprehensive experimental results on the real sample collections from Comodo Cloud Security Center demonstrate the effectiveness of our proposed methods.

Paper II Full

Text Mining in Unclean, Noisy or Scrambled Datasets for Digital Forensics Analytics

Konstantinos Xylogiannopoulos, Panagiotis Karampelas, and Reda Alhajj

In our era, most of the communication between people is realized in the form of electronic messages and especially through smart mobile devices. As such, the written text exchanged suffers from bad use of punctuation, misspelling words, continuous chunk of several words without spaces, tables, internet addresses etc. which make traditional text analytics methods difficult or impossible to be applied without serious effort to clean the dataset. Our proposed method in this paper can work in massive noisy and scrambled texts with minimal preprocessing by removing special characters and spaces in order to create a continuous string and detect all the repeated patterns very efficiently using the Longest Expected Repeated Pattern Reduced Suffix Array (LERP-RSA) data structure and a variant of All Repeated Patterns Detection (ARPaD) algorithm. Meta-analyses of the results can further assist a digital forensics investigator to detect important information to the chunk of text analyzed.

Paper III Full

Detecting Periodic Subsequences in Cyber Security Data

Matthew Price-Williams, Nick Heard, and Melissa Turcotte

Anomaly detection for cyber-security defence has garnered much attention in recent years providing an orthogonal approach to traditional signature-based detection systems. Anomaly detection relies on building probability models of normal computer network behaviour and detecting deviations from the model. Most data sets used for cyber-security have a mix of user-driven events and automated network events, which most often appears as polling behaviour. Separating these automated events from those caused by human activity is essential to building good statistical models for anomaly detection. This article presents a changepoint detection framework for identifying automated network events appearing as periodic subsequences of event times. The opening event of each subsequence is interpreted as a human action which then generates an automated, periodic process. Difficulties arising from the presence of duplicate and missing data are addressed. The methodology is demonstrated using authentication data from Los Alamos National Laboratory’s enterprise computer network.

Session: Criminal Analysis & Detection I			
11:00-13:00	Tuesday, September 12, 2017	Room: Seminar Room 2	Chair: Thirimachos Bourlai

Paper I Full

Detecting Crime Series Based on Route Estimation and Behavioral Similarity

Anton Borg, Martin Boldt and Johan Eliasson

A majority of crimes are committed by a minority of offenders. Previous research has provided some support for the theory that serial offenders leave behavioral traces on the crime scene which could be used to link crimes to serial offenders. The aim of this work is to investigate to what extent it is possible to use geographic route estimations and behavioral data to detect serial offenders. Experiments were conducted using behavioral data from authentic burglary reports to investigate if it was possible to find crime routes with high similarity. Further, the use of burglary reports from serial offenders to investigate to what extent it was possible to detect serial offender crime routes. The result show that crime series with the same offender on average had a higher behavioral similarity than random crime series. Sets of crimes with high similarity, but without a known offender would be interesting for law enforcement to investigate further. The algorithm is also evaluated on 9 crime series containing a maximum of 20 crimes per series. The results suggest that it is possible to detect crime series with high similarity using analysis of both geographic routes and behavioral data recorded at crime scenes.

Paper II Full

An Integrated Framework for the Timely Detection of Petty Crimes

Nikolaos Dimitriou, George Kioumourtzis, Anargyros Sideris, Georgios Stavropoulos, Evdoxia Taka, Nikolaos Zotos, George Leventakis, and Dimitrios Tzovaras

While petty crimes are considered misdemeanors from a judicial point of view and are typically punished with light sentences, they greatly affect citizens' perception of safety and are related to substantial financial losses. In this paper, we describe a technological solution for the timely detection of petty crimes, based on the developments of the EU project PREACT. Concretely, a modular framework is presented where an embedded system processes in-situ a camera stream for the realtime detection of petty criminality incidents and the timely notification of authorities. This paper provides details on the various hardware options and the key software components of the system, which include a set of appropriately implemented video analytics algorithms for the detection of different petty crimes as well as modules for the capturing, transcoding and secure transmission of video clips in case of an alarm. An evaluation of the system is also provided covering both experimental results on the accuracy of the platform but also focusing on the feedback received during the trials phase of P-REACT through the participation of external stakeholders. Evaluation during this phase was based on the live demonstration of system's operation in a series of simulated events corresponding to different types of petty crimes. In both cases evaluation results were very promising, attesting to the high innovation potential of the platform.

Paper III Short

A Statistical Method for Detecting Significant Temporal Hotspots using LISA Statistics

Martin Boldt and Anton Borg

This work presents a method for detecting statistically significant temporal hotspots, i.e. the date and time of events, which is useful for improved planning of response activities. Temporal hotspots are calculated using Local Indicators of Spatial Association (LISA) statistics. The temporal data is in a 7x24 matrix that represents a temporal resolution of weekdays and hours-in-the-day. Swedish residential burglary events are used in this work for testing the temporal hotspot detection approach. Although, the presented method is also useful for other events as long as they contain temporal information, e.g. attack attempts recorded by intrusion detection systems. By using the method for detecting significant temporal hotspots it is possible for domain-experts to gain knowledge about the temporal distribution of the events, and also to learn at which times mitigating actions could be implemented.

Session: Tools and Techniques for Analyzing Data III

15:30-16:30 Tuesday, September 12, 2017 Room: Seminar Room 1 Chair: Neesha Kodagoda

Paper I Full

IoT Data Profiles - The Routines of Your Life Reveals Who You Are

Johan Fernquist, Torbjörn Fängström and Lisa Kaati

Preserving privacy is getting more and more important. The new EU general data protection regulation (GDPR) which will apply from May 2018 will introduce developments to some areas of EU data protection law and increase the privacy and personal integrity by strengthen and unify data protection for all individuals in EU. GDPR will most likely have an impact on many organizations and put pressure on many organizations that handle data. In this work, we investigate to what extent data profiles consisting of data from connected things can be used to identify a user. We use time and event profiles that can be created based on when, where and how a user communicates and uses digital devices. Our results show that such data profiles can be used to identify individuals and that collecting and creating data profiles of users can be seen as a serious threat towards privacy and personal integrity.

Paper II Full

Interpretable Probabilistic Divisive Clustering of Large Node-Attributed Networks

Lisa Kaati and Adam Ruul

Social network analysis is an important set of techniques that are used in many different areas. One such area is intelligence and law enforcement where social network analysis is used to study various kinds of networks. One of the problems with social networks that are extracted from social media is that easily becomes very large and as a consequence difficult to analyze. Therefore, there is a need for techniques that can divide a large network into smaller communities that are more feasible to analyze. Existing community detection algorithms usually only focus on creating communities based on the underlying networks structure and therefore it can be hard to interpret the meaning of communities. In this work, we present two methods for community detection that allows a user to detect communities with an underlying meaning not only based on the relations in the network but also on attributes of the nodes. Our methods use iterative approaches that allow the user to define meaningful properties and are applicable on large social networks with attributed nodes.

Session: Criminal Analysis & Detection II

15:30-16:30 Tuesday, September 12, 2017 Room: Seminar Room 2 Chair: Anton Borg

Paper I Full

Towards a breakthrough Speaker Identification approach for Law Enforcement Agencies: SIIP

Khaled Khelif, Yann Mombrun, Gerhard Backfried, Farhan Sahito, Luca Scarpato, Petr Motlicek, Srikanth Madikeri, Damien Kelly, Gideon Hazzani and Emmanouil Chatzigavriil

This paper describes SIIP (Speaker Identification Integrated Project) a high performance innovative and sustainable Speaker Identification (SID) solution, running over large voice samples database. The solution is based on development, integration and fusion of a series of speech analytic algorithms which includes speaker model recognition, gender identification, age identification, language and accent identification, keyword and taxonomy spotting. A full integrated system is proposed ensuring multisource data management, advanced voice analysis, information sharing and efficient and consistent man-machine interactions.

Paper II Full

Period Analysis and Trend Forecast of Terrorism in SCO Region by Wavelet Transform

Ze Li, Duoyong Sun, Bo Li and Wei Ding

The analysis of terrorism over time is the lead force in counter-terrorism intelligence unit. Period analysis and trend forecast are essential in understanding regional terrorism dynamic features. In this paper, we proposed a wavelet transform based framework with periodic and prediction components and had the Shanghai Cooperation Organization (SCO) region investigated to analyze the periodic features and forecast the future trends. Based on the wavelet transform, first, the terrorism trend over the SCO region in the most recent 27 years (1989-2015) were analyzed with its periodic oscillation on multiple time scales. Then, wavelet transform based Wavelet Neural Network (WNN) model was used to forecast the future terrorism trend. Third, we had the predictive future trends cross-checked by both qualitative inference and quantitative prediction. Finally, we investigated the reasons of why the regional terrorism appeared periodically from different aspects. Results show that the regional terrorism trend experiences significant 13-years, 7-years, and 4-years periodic oscillation. Results also show that wavelet transform based forecast framework is of high accuracy and practical value in short-term forecasting of future trends.

Session: Models and Tools for Intelligent Decision Making			
10:30-12:30	Wednesday, September 13, 2017	Seminar Room 1	Chair: Panagiotis Karampelas

Paper I Full

Cyber Threat Intelligence Model: An Evaluation of Taxonomies, Sharing Standards, and Ontologies within Cyber Threat Intelligence

Vasileios Mavroeidis and Siri Bromander

Threat intelligence is the provision of evidence-based knowledge about existing or potential threats. Benefits of threat intelligence include improved efficiency and effectiveness in security operations in terms of detective and preventive capabilities. Successful threat intelligence within the cyber domain demands a knowledge base of threat information and an expressive way to represent this knowledge. This purpose is served by the use of taxonomies, sharing standards, and ontologies. This paper introduces the Cyber Threat Intelligence (CTI) model, which enables cyber defenders to explore their threat intelligence capabilities and understand their position against the ever-changing cyber threat landscape. In addition, we use our model to analyze and evaluate several existing taxonomies, sharing standards, and ontologies relevant to cyber threat intelligence. Our results show that the cyber security community lacks an ontology covering the complete spectrum of threat intelligence. To conclude, we argue the importance of developing a multi-layered cyber threat intelligence ontology based on the CTI model and the steps should be taken under consideration, which are the foundation of our future work.

Paper II Short

Large Scale Data Collection of Tattoo-Based Biometric Data from Social-Media Websites

Michael Martin, Jeremy Dawson, and Thirimachos Bourlai

The use of tattoos as a soft biometric is increasing in popularity among law enforcement communities. There is great need for large scale, publicly available tattoo datasets that can be used to standardize efforts to develop tattoo-based biometric systems. In this work, we introduce a large tattoo dataset (WVUMediaTatt) collected from a social-media website. Additionally, we provide the source links to the images so that anyone can re-generate this dataset. Our WVU-MediaTatt database contains tattoo sample images from over 1,000 subjects, with two tattoo image samples per subject. To the best of our knowledge, this dataset is significantly bigger than any current released publicly available tattoo dataset, including the recently released NIST Tatt-C dataset. The use of social media in deep learning, data mining, and biometrics has traditionally been a controversial issue in terms of data security and protection of privacy. In this work, we first conduct a full discussion on the issues associated with data collection from social media sources for the use of biometric system development, and provide a framework for data collection. In this study, within the process of creating a new large scale tattoo dataset, we consider the issues and make attempts protect the subject's privacy and information, while ensuring that subjects remain in control of their data in this study and the use of the data adheres to the guidelines proposed by the Heath Care Compliance Association (HCCA) and the U.S. Department of Health & Human Services.

Paper III Short

A Framework for Measuring Imagination in Visual Analytics Systems

Michael A. Bedek, Alexander Nussbaumer, Eva-C. Hillemann, and Dietrich Albert

This paper presents a framework for measuring imagination support in criminal analysis systems. Imagination is important for criminal analysts in their everyday work when they have to solve criminal cases. Typically, they are faced with a huge amount of information that is often ill-structured, do not contain all relationships, and are characterised by many uncertainties. In order to draw correct conclusions and to solve cases, analysts need imagination to find out facts from such data, or in other words: to detect the signals out from the noise. This paper describes a general framework for introducing imagination support in criminal analysis systems. The framework consists of two parts, first the operationalisation of imagination, and second, guidelines for an experimental setting of evaluating criminal analysis systems regarding their imagination support. This work is intended to serve as a baseline for future evaluation work of criminal analysis systems.

Paper IV Short

Catchem: A Browser Plugin for the Panama Papers using Approximate String Matching

Panos Kostakos, Miika Moilanen, Arttu Niemelä, and Mourad Oussalah

The Panama Papers is a collection of 11.5 million leaked records that contain information for more than 214,488 offshore entities. This collection is growing rapidly as more leaked records become available online. In this paper, we present a work in progress on a web browser plugin that detects company names from the Panama Papers and alerts the user by means of unobtrusive visual cues. We matched a random sample of company names from the Public Works and Government Services Canada registry against the Panama Papers using three different string matching techniques. Monge-Elkan is found to provide the best matching results but at increased computational cost. Levenshtein-based approach is found to provide the best tradeoff between matching and computational cost, while Jacquard index like approach is found to be less sensitive to slight textual change.

Session: Criminal Intelligence Analysis

10:30-12:30	Wednesday, September 13, 2017	Room: Seminar Room 2	Chair: Martin Boldt

Paper I Full

Customs Risk Analysis through the ConTraffic Visual Analytics Tool

Mikaela Poulymenopoulou and Aris Tsois

Customs risk analysis is crucial for detecting fraud and contraband goods in the massive flows of internationally traded goods. Most of non-bulk goods are transported in shipping containers and, as customs can control only about 2% of them, efficient customs risk analysis is crucial. In support to EU customs, the Joint Research Centre of the European Commission has developed the ConTraffic visual analytics research prototype that is currently used by EU customs on an experimental basis. This paper presents the main architectural elements of this application and some of the custom-made visualization and user-interaction techniques employed in order to help customs explore the large volumes of shipping container data and perform route-based risk analysis. Moreover, we validate the usefulness of this application with illustrative examples of route-based risk analysis workflows than can be performed with our system.

Paper II Full

Comparative Analysis of Crime Scripts: One CCTV Footage – Twenty-One Scripts

Hervé Borrion, Hashem Dehghanniri, and Yuanxi Li

In recent years, there has been a growing interest in the modelling of crime commission processes, in particular crime scripting, in physical and cyber spaces. This article aims to demonstrate the limits of unstructured scripting approaches, and advocates the development of more systematic techniques. For this, we examined the differences and similarities between various scripts. Twenty-one participants were trained in crime scripting, and tasked to produce individual scripts based on the same video footage of a shop robbery. Content analysis was applied to the scripts, which involved classifying the different steps of the crime commission process and analyzing their distributions. A scoring system was then developed to assess the relative degree of completeness of each script, and linear regression computed using the number of activities included as the predictor variable. This research provides the first evidence of the limits of creating scripts using an intuitive approach, and the need for applying semistructured goal-based methods.

Paper III Short

Whose Hands Are in the Finnish Cookie Jar?

Jukka Ruohonen and Ville Leppänen

Web cookies are ubiquitously used to track and profile the behavior of users. Although there is a solid empirical foundation for understanding the use of cookies in the global world wide web, thus far, limited attention has been devoted for country-specific and company-level analysis of cookies. To patch this limitation in the literature, this paper investigates persistent third-party cookies used in the Finnish web. The exploratory results reveal some similarities and interesting differences between the Finnish and the global web—in particular, popular Finnish web sites are mostly owned by media companies, which have established their distinct partnerships with online advertisement companies. The results reported can be also reflected against current and future privacy regulation in the European Union.

Poster: EISIC 2017 Poster Session		
10:30-11:00 15:00-15:30	Monday, September 11, 2017	Room: Foyeur

Poster I

Photometrix™ : A Digital Seal for Offline Identity Picture Authentication

Marc M. Pic and Amine Ouddan

Picture falsification on identity documents is a recurring problem. Text falsification can be mitigated on printed documents thanks to digital signature, but for picture the only safe strategy was to integrate an expensive electronic chip in the document. This paper proposes a low-cost alternative, allowing to check offline the authenticity of the image thanks to digitally signed characteristics extracted from the picture.

Poster II

How the use of ethically sensitive information helps to identify co-offenders via a purposed privacy scale: a pilot study *Pragya Paudyal, Chris Rooney, Neesha Kodagoda, B.L. William Wong, Penny Duquenoy, and Nadeem Qazi*

Poster III

Testing the viability of an automatic assessment tool to measure radicalization risk: a case study on Facebook

Javier Torregrosa, Irene Gilpérez-López, Raul Lara-Cabrera, David Garriga, David Camacho

Poster IV

A Monitoring Tool for Terrorism-related Key-players and Key-communities in Social Media Networks

Stelios Andreadis, Ilias Gialampoukidis, George Kalpakis, Theodora Tsikrika, Symeon Papadopoulos, Stefanos Vrochidis, and Yiannis Kompatsiaris

Terrorists communicate and disseminate their activities using social media, such as Twitter, where complex networks of user accounts are formed and need to be effectively analysed by Law Enforcement Agencies (LEAs). To this end, we propose a novel visualisation tool that assists intelligence analysts and investigators through the presentation of the network formation, components, key-players, key-communities and through support of keyword search in the terrorism domain, highlighting also suspended users and offering navigation in the user network.

Poster V

Terrorism Network Analysis Based on Bayesian networks: Models and Applications

Kun Cai, Duoyong Sun and Bo Li

Social network analysis (SNA) is widely used to explore terrorist organization networks. This paper explores the use of Bayesian networks to expand social network analysis involving Terrorism Networks, which can help users discover new relational links in terrorist organizations and identify special network nodes that cannot be identified by traditional methods. Through SNA tools, the models and applications of Bayesian networks in the identification of terrorist organization networks contain not only the network structure attributes, but also the social attributes.

EISIC 2017 – Transportation from Airport to hotels

Airport to Kifisia and hotels

There are two options in order to reach the Kifisia hotels from the airport.

You can take a taxi from the Airport to Kifisia (Semiramis Hotel at Kefalari) which normally costs between 30-40 euros depending on the hour of the day and the traffic. If you arrive between 00:00 and 05:00 the cost is around 60 euros.

Alternatively, you can take the Suburban Rail and Metro from Airport to Neratziotissa Station (Suburban Rail) and then from Neratziotissa Station (Metro Station Line 1) to Kifisia with one ticket that costs 10 euros. From the airport, there are three trains per hour, the first one on the 11th minute of the hour e.g., 10:11, the next one on the 26th minute e.g. 10:26 and on the 44th minute e.g. 10:44. The Metro trains are scheduled every 3-7 minutes depending on the hour of the day. The duration of the whole trip is approximately 1 hour and 10 minutes.

Detailed instructions to reach Kifisia Metro Station from the Airport can be found in the following link: https://goo.gl/maps/VfL2hsbEZ6k or by scanning the QR-Code. Please make sure that you will select M1 option for trains.

Kifisia Metro Station to Hotels

All the hotels are in walking distance from Kifisia Metro Station. The most distant hotel is Semiramis which is 15-20 minutes away while the other hotels are 10-15 minutes. Detailed instructions to reach Semiramis hotel from Kifisia Metro Station can be found in the following link: https://goo.gl/maps/fTCjLBeeBaA2 or by scanning the QR-Code. All the other hotels are on the way to Semiramis so you can follow the same path and stop to the respective hotel.

Hellenic Air Force Academy

HAFA is a Military Institute of Higher Education located in Dekelia Air Base providing education and degrees equivalent to that of Universities founded in 1931. HAFA's premises comprise a modern classroom building, a labs building, a conference complex, a library building, the commander's building, the dean's building, a faculty offices building, the cadets barracks and dining facilities and sport facilities.

Conference Venue location

EISIC 2017 will take place at the HAFA conference complex. The complex comprises the HAFA auditorium, which accommodates up to 1,200 people and is named after the HAF pilot “Lt Nikolaos Sialmas”, and three other seminar rooms in the attached building. Coffee breaks will be offered in the Conference Foyer while lunch will be served in the Dekelia Air Base Officers Club.

Access to Dekelia Air Base

Since Dekelia Air Base is a military base, access is restricted to people without special permission. For that purpose, conference attendees should have been registered for the conference by the final registration day and when entering the base, they should produce the valid ID or Passport whose number they submitted when registering for the conference. Important note People who will fail to complete the appropriate registration forms during the registration process or fail to present a valid identification document during entrance may be denied access to the conference.

Transportation from/to Conference Venue

Free Bus Service

There will be a free bus transportation service during the days of the conference from Semiramis Hotel, Kifisia to the conference venue and back the following dates and times.

08:15 Monday, 11th of September, 2017	From Semiramis Hotel to Dekelia Air Base
17:00 Monday, 11th of September, 2017	From Dekelia Air Base to Semiramis Hotel
19:15 Monday, 11th of September, 2017	From Semiramis Hotel to Dekelia Air Base
22:15 Monday, 11th of September, 2017	From Dekelia Air Base to Semiramis Hotel
08:15 Tuesday, 12th of September, 2017	From Semiramis Hotel to Dekelia Air Base
16:30 Tuesday, 12th of September, 2017	From Dekelia Air Base to Semiramis Hotel
08:15 Wednesday, 13th of September, 2017	From Semiramis Hotel to Dekelia Air Base
13:45 Wednesday, 13th of September, 2017	From Dekelia Air Base to Semiramis Hotel

By Car, Taxi, Train or Public Bus

Conference attendees who will reach the entrance of Dekelia Air Base by car have to park their vehicle in the visitors' parking area and they will be transported to the Conference Venue by the internal transportation service of the Base. The same applies to people who will reach the Base by any other means except from those who will use the free conference transportation service from the Kifisia hotels.

Coffee Breaks

In the designated hours, there will be served coffee, juices, tea, cakes and cookies in the Foyer area of the Conference complex.

Lunch

Lunch will be served at the outside area of the Dekelia Air Base Officers' Club close to the runway of the Base. Transportation from the Conference Complex to the Dekelia Air Base Officers' Club will be provided before and after the lunch. It is important for all participants to be on time at the designated area where the internal bus will be parked in order to avoid delays in transportation.

Reception

The Reception ceremony will take place to honor the conference participants on Monday, 11th of September 2017 at 19:30. Before the reception there will be a guided tour at the Hellenic Air Force Museum inside the Dekelia Air Base. The museum's collection includes more than forty aircrafts, radars, auxiliary ground equipment, antiaircraft armament, aircraft engines and armament, communications devices, aviation memorabilia, pilots' suits, personnel uniforms etc. Following the museum visit, a reception will take place at the outside area of the Dekelia Air Base Officers' Club. There will be free transportation service from the hotel to Dekelia Air Base and back according to the following schedule:

19:15 Monday, 11th of September, 2017	From Semiramis Hotel to Dekelia Air Base
22:15 Monday, 11th of September, 2017	From Dekelia Air Base to Semiramis Hotel

Gala Dinner

Gala Dinner is scheduled on Tuesday the 12th of September, 2017, 19:30 at the Hellenic Armed Forces Officers Club in the center of Athens. The Hellenic Armed Forces Officers Club is located at Rigillis 1 & Vasilissis Sofias (Platia Pavlou Mela), Athens, Post Code 10675 at the center of Athens. The Hellenic Armed Forces Officers Club is hosted at Sarogleion Building which is accessible from Evangelismos Station at Metro Line 3. Detailed instructions to reach Sarogleion building from Semiramis hotel can be found in the following link: https://goo.gl/maps/NuYsfz6fDQT2 or by scanning the QR-Code. Please select the M1 > M3 option to see the detailed instructions.

The trip from the hotel to the destination takes approximately 1 hour and 10 minutes and the one-way ticket costs 1.4 euros and can be purchased at any station. After the Gala Dinner, it is possible to walk in the center of Athens, Sintagma square and the area of the Greek Parliament or to visit Kolonaki area where there are several cafes or bars.

Information for Presenters

Full papers are allocated approximately 30 minutes while Short papers 20 minutes including a question-and-answer period after the presentation. The Session Chair introduces the speakers and moderates the question-and-answer period. A laptop with Microsoft office installed will be available in each conference room. Help is available to presenters for the installation of their presentation upon request. A basic audio-visual installation (speakers, microphone, projection screen, data projector) will be available in the rooms.

Poster Session

The poster sessions will be hosted the first day of the conference in the Foyer during the coffee breaks. Maximum height of the poster can be 140 cm and maximum width 104 cm.

Photographs

Photographs are allowed inside and outside the conference complex and in the area of the Officers' Club where lunch will be offered.

Smoking Policy

Smoking is not permitted inside the areas of the conference. Smokers can be accommodated outside the Conference complex.

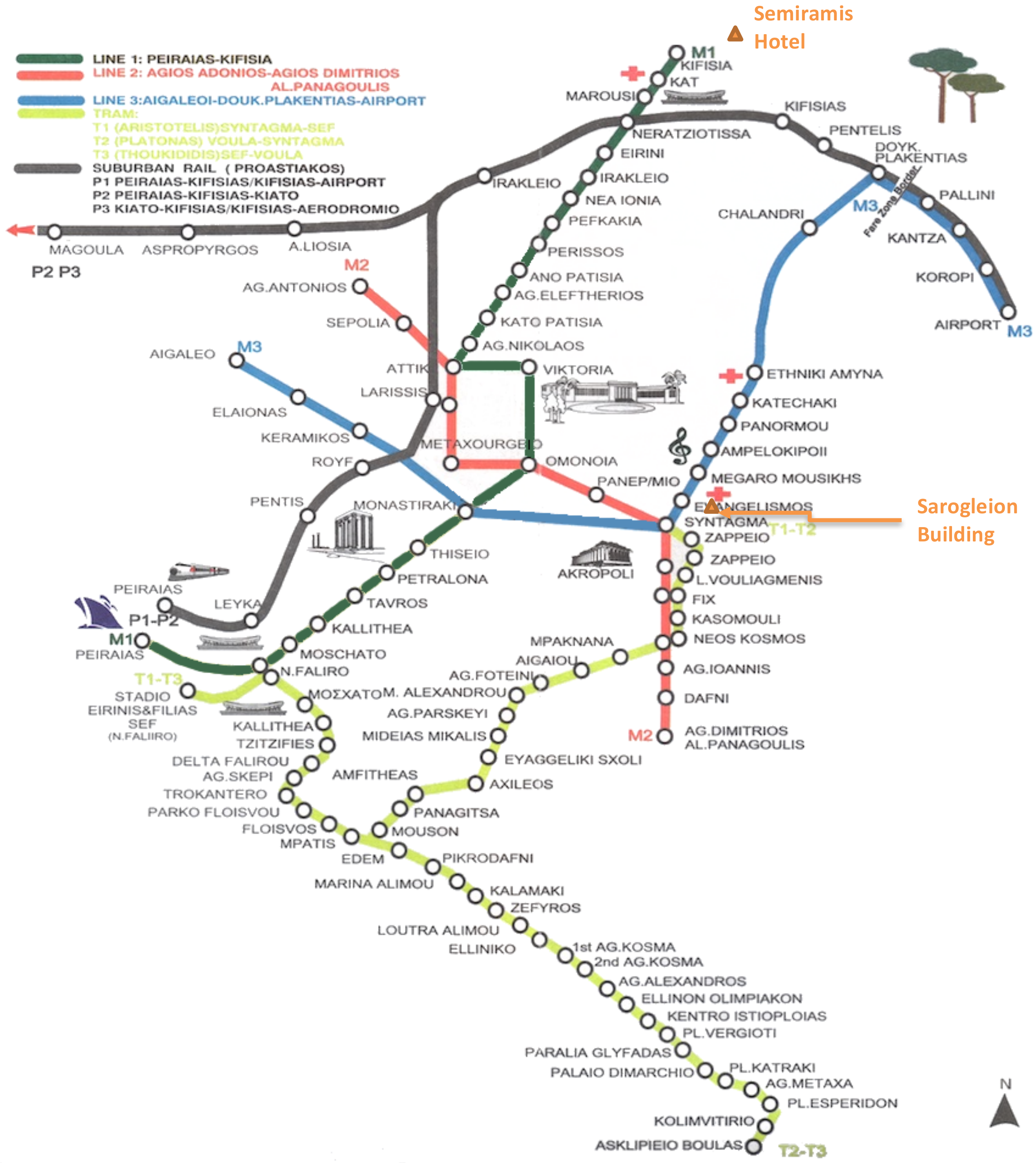
Mobile Phone Policy

As a courtesy to speakers and attendees please refrain from using mobile phones during the keynote speeches and presentations. Turn your mobile phone to vibrate before entering a session and leave the session if you receive a call.

WiFi

Free WiFi will be available to conference participants in the Conference Complex using a code that will be provided at the time of the registration and will be available for all the days of the conference.

EISIC 2017 – Athens Metro Map



Semiramis Hotel

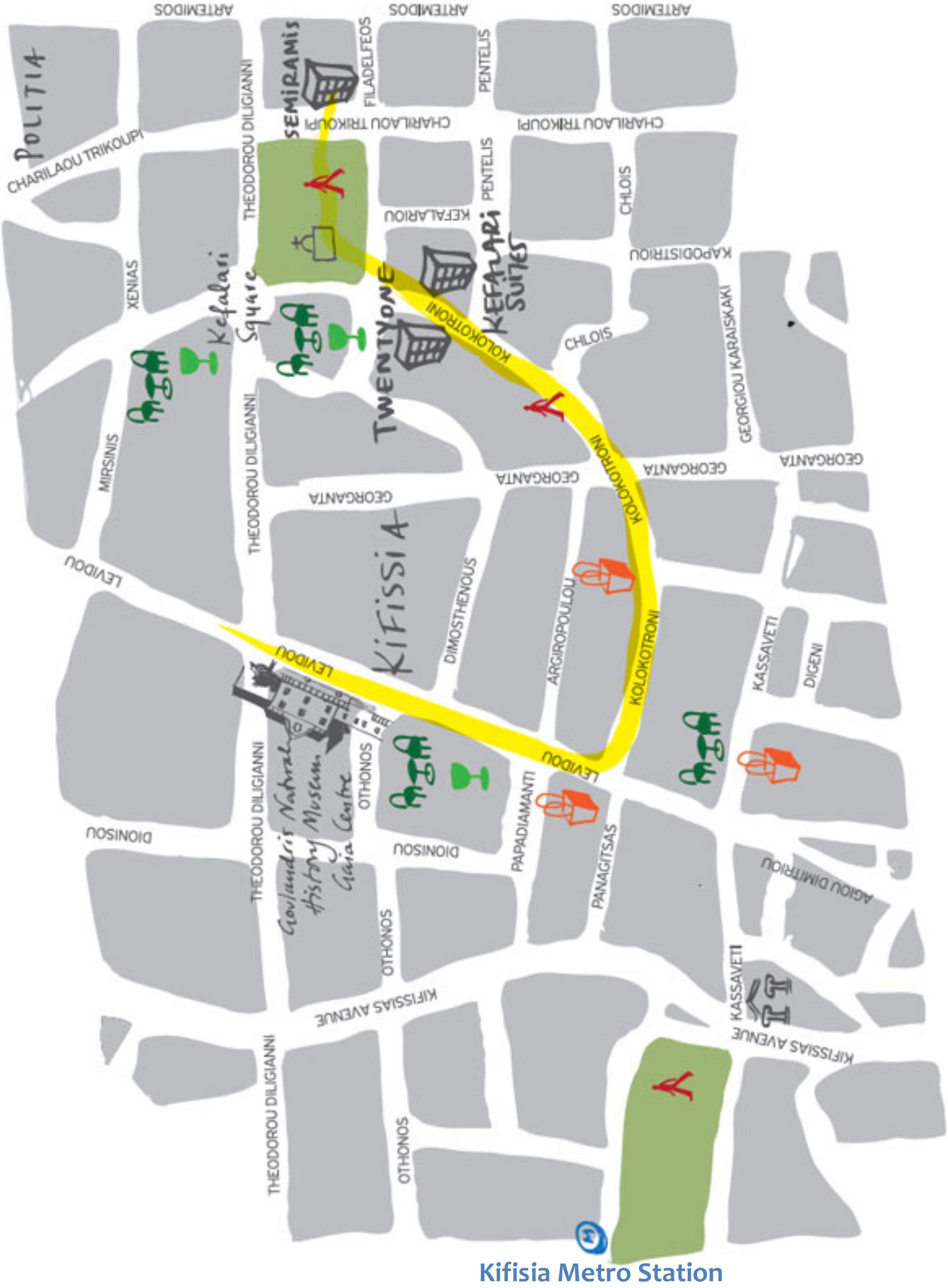
Sarogleion Building

Useful Links

Athens International Airport
http://www.aia.gr

Athens Urban Rail Transport
http://www.stasy.gr/index.php?id=1&L=1

EISIC 2017 – Kifisia Map with the Hotels



European Intelligence and Security Informatics Conference (EISIC) 2017

September 11-13, 2017, Dekelia Air Base, Dekelia, Greece

http://www.eisic.org

The Premier European Conference on Counterterrorism and Criminology

Designed by Panagiotis Karampelas, EISIC 2017