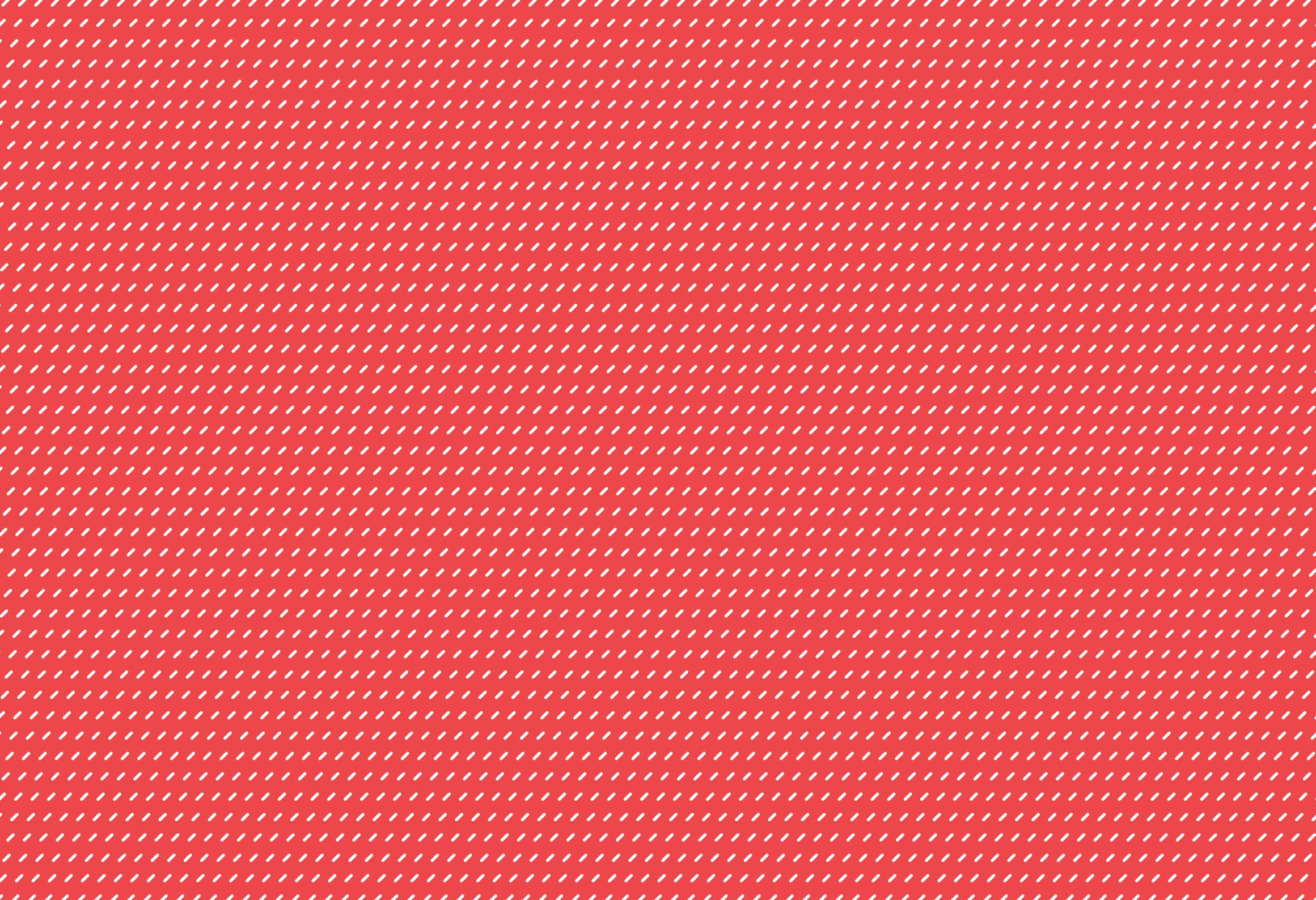




CURRENT AND
EMERGING
CHALLENGES IN
CYBERCRIME AND
CYBERTERRORISM

10-11 MARCH 2016

NIUWSPOORT INTERNATIONAL
PRESS CENTRE
DEN HAAG



WELCOME

It is with great pleasure that we welcome you to the Current and Emerging Trends in Cybercrime and Cyberterrorism event being held over the next two days here at the Nieuwspoord International Press Centre in Den Haag, Netherlands. The event has been organised as a cornerstone in the final stages of the COURAGE, CAMINO and CyberROAD projects, and is part of an overall thinking and knowledge exchange process to consolidate the projects' combined vision for the future of research in the fields of cybercrime and cyberterrorism across the EU.

We'd like to take this opportunity to thank all of our invited speakers, and the extended stakeholder communities surrounding each of the projects, for allowing us to draw upon your expertise and experience to help shape each of the respective research roadmaps, a process that has enabled us to address the tangible wants and needs of society within them. Presenting at the event are a selection of these individuals, who have volunteered to present to us some of their thoughts and work in tackling contemporary cyber-issues and to provide further insight into some of the challenges that we face today, and will continue to face over the coming years. The event

itself aims to provide all stakeholders with a forum to exchange ideas and highlight challenges, alongside contemporaries from across Europe, so that together we can develop strategies and priorities for a common roadmap to fight cybercrime and cyberterrorism. In particular, throughout the two-day event we hope to gather insights from across Europe and beyond, to discuss further developments in the methodology, technology, and foundations for the design and effective implementation of a European roadmap for the fight against cybercrime and cyberterrorism. The event will contribute towards the development of a consolidated roadmap between COURAGE, CAMINO, and CyberRoad which will be presented to the European Commission later in 2016. This roadmap will aim to clarify the various interpretations, commonalities, and differences emanating from the European cybersecurity community as well as the results of the three projects, thereby paving the way for a more structured and well-founded approach to future research initiatives. In this booklet we'd like to introduce to you each of the projects, our efforts to develop to a consolidated approach to defining future research priorities, as well as providing an introduction to each of our invited speakers and the agenda for our event over the next two days.

Prof. Babak Akhgar

on behalf of the COURAGE, CAMINO and CyberRoad projects



Centre of Excellence in Terrorism,
Resilience, Intelligence and
Organised Crime Research

AGENDA

OUR PLAN FOR THE NEXT TWO DAYS

THURSDAY 10.03.2016

- 13:30 14:00 Registration and Coffee
- 14:00 14:05 Welcome/introduction
Gabriela Bodea, TNO
- 14:05 14:45 Keynote speech
Raoul Chiesa, Security Brokers Italy

*"Cyber Terrorism: wrong assumptions &
true facts: what I hope will never happen"*

SESSION 1 LAW AND LAW ENFORCEMENT (NEEDS, CHALLENGES, SOLUTIONS AND PRACTICE)

Moderator Cormac Callahan (Aconite)

- 14:45 15:05 DI Geoff Halpin
Yorkshire and Humberside Regional
Cybercrime Unit
- 15:05 15:25 Pim Takkenberg
TNO
- 15:25 15:45 Jerzy Kosinski
WSPolSzczytno –Higher School of the Police
- 15:45 16:05 Judyta Kasperkiewicz
University of Silesia in Katowice, Faculty
of Law and Administration, Department of
Forensic Science
- 16:05 16:15 Q&A
-
- 16:15 16:30 Coffee Break
-

**SESSION 2 SOLUTIONS FOR THE FUTURE:
COURAGE-CAMINO-CYBERROAD IDEAS**

16:30 18:00 *Working session with audience*

Babak Akhgar
representative of project COURAGE

Michal Choras
representative of project CAMINO

Davide Ariu
representative of project CyberROAD

18:00 19:00 Networking reception

FRIDAY 11.03.2016

**SESSION 3 CITIZENS, ENTERPRISE AND PRIVATE
INDUSTRY (NEEDS, CHALLENGES, SOLUTIONS
AND PRACTICE)**

Moderator Davide Ariu (University of Cagliari)

09:30	09:50	Gary Hibberd Agenci UK
09:50	10:10	Rocco Mammoliti & Massimiliano Aschi Poste Italiane
10:10	10:30	Dimitris Kavallieros & Christoforos Ntantogian KEMEA/UI NFC2 Project
10:30	10:45	Q&A
<hr/>		
10:45	11:15	<u>Coffee Break</u>
<hr/>		

SESSION 4 GOVERNMENT, POLICY, STRATEGIES AND AWARENESS RAISING

Moderator Luigi Rebuffi (EOS)

11:15	11:35	Quentin Revell UK Home Office Centre for Applied Science and Technology
-------	-------	---

11:35 11:55 Robin de Haas
The Hague Security Delta

11:55 12:15 Stuart Hyde
CCL Group Ltd UK

12:15 12:35 Olivier Burgersdijk
EC3/Europol

12:35 12:45 Q&A

12:45 13:45 Lunch

SESSION 5 EMERGING TECHNOLOGIES AND SOLUTIONS (INCLUDING LEGAL CONSIDERATIONS, BEST PRACTICES ETC.)

Moderator Michal Choras (ITTI)

13:45 14:05 Dr Argyro Karanasiou
Bournemouth University

14:05 14:25 Prof Dr. Bert-Jaap Koops

Professor of regulation and technology,
Tilburg University

14:25 14:45 Prof Wojciech Mazurczyk
Fern University and PW, Warsaw

14:45 14:55 Q&A

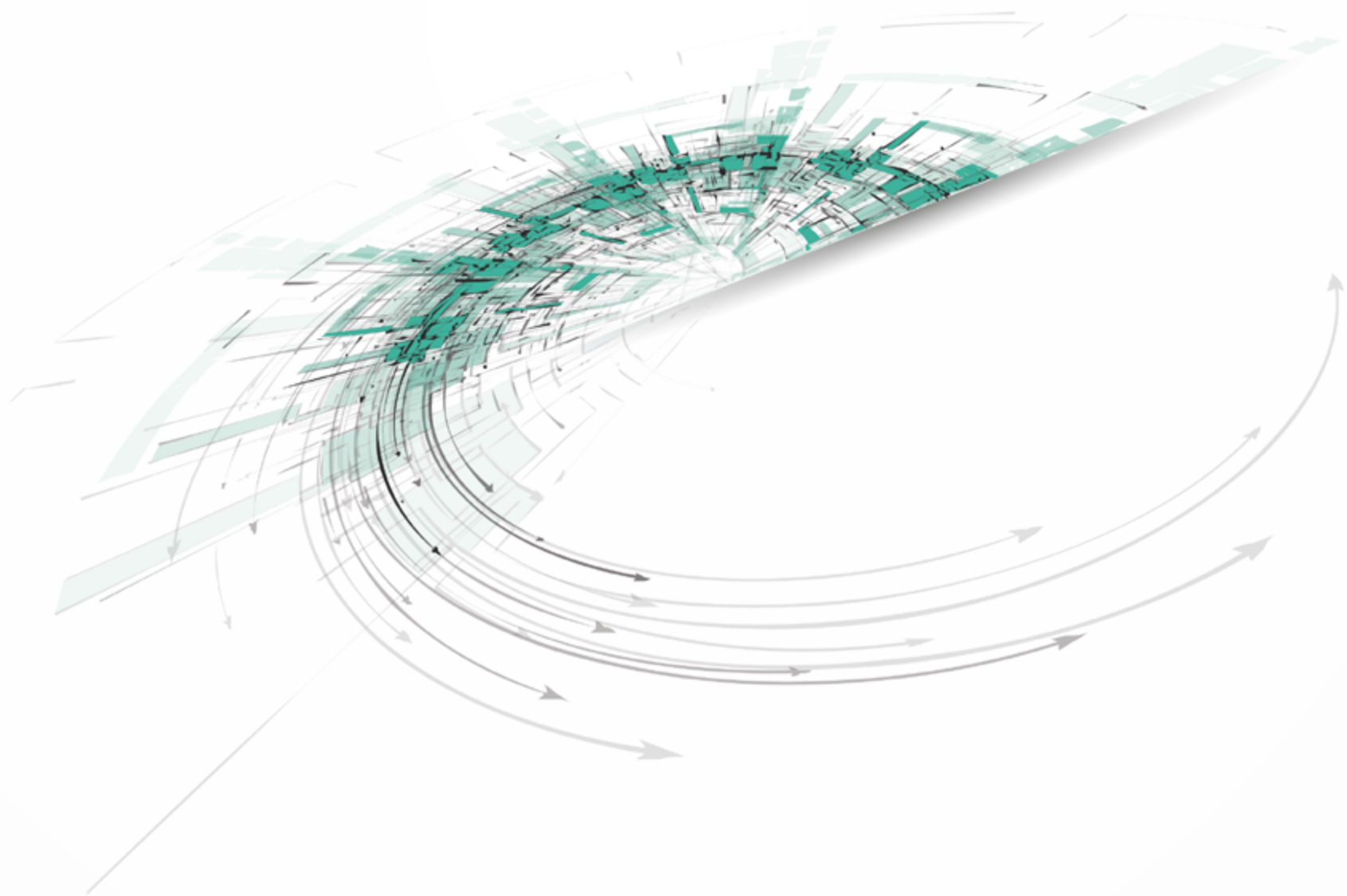
14:55 15:05 Coffee Break

15:05 16:00 *Wrap-up and final Q&A*

Babak Akhgar
representative of project COURAGE

Michal Choras
representative of project CAMINO

Davide Ariu
representative of project CyberROAD



SPEAKERS

MEET OUR SPEAKERS

DR. ARGYRO KARANASIOU

Dr Argyro Karanasiou is an Associate Professor (Senior Lecturer) specialising in IT and Media Law, affiliated with the Centre for Intellectual Property, Policy & Management (CIPPM) and with the Data Science Institute (DSI) at Bournemouth University (United Kingdom). She is also affiliate faculty staff of Harvard Law School (2014-now), responsible for the course CopyrightX: CIPPM in the UK. Currently, Argyro is involved in media related projects with the Council of Europe (Regional Expert on online media and reconciliation in South Eastern Europe) and with the OSCE Representative on Freedom of the Media. Recently (Jan 2016), Argyro was invited to join the EFF's group of experts on Free Trade Agreements and Digital Services, providing expertise on how TISA and TTIP will affect online consumers in the EU. In 2013 (Indonesia) and 2015 (Brazil), she was awarded an Internet Society IGF Ambassadorship and in 2014 she was named a PhD Ambassador by the Information and Privacy Commissioner in Ontario, Canada. Her research discusses techno-legal conceptual frameworks for decentralised internet

regulation with a particular focus on free speech, data protection, media ownership, and user empowerment. Her current projects span a wide range of topics from IoT/wearable tech to big data and mesh networks. Argyro tweets [@ArKaranasiou](#) on all things tech.

PROF. BABAK AKHGAR

Prof Babak Akhgar is Professor of Informatics and Director of CENTRIC (Centre of excellence in terrorism, resilience, intelligence and organised crime research) at Sheffield Hallam University and Fellow of the British Computer Society. He gained considerable commercial experience as a strategy analyst and methodology director for several international companies. Prof. Akhgar has more than 100 referred publications in international journals and conferences on information systems with specific focus on knowledge management and its application with contemporary security contexts (e.g. Application of social media in crisis management, intelligence based combating of terrorism and organised crime, gun crime, cyber security, public order and cross cultural ideology polarisation). He is technical coordinator of the COURAGE project.

PROF. BERT-JAAP KOOPS

Bert-Jaap Koops researches the interaction between technology and law, in particular criminal law and regulation issues. His main research fields are cybercrime, cyber-investigation, privacy, and data protection. He is also interested in topics such as DNA forensics, identity, digital constitutional rights, 'code as law', and regulatory implications of human enhancement, genetics, robotics, and neuroscience. With a personal postdoc (1999), VIDI (2003) and VICI

(2014) grant, Koops is one of the few Dutch researchers who received all three stages of NWO's (Netherlands Organisation for Scientific Research) personal research-grant scheme. From 2005-2010, he was a member of De Jonge Akademie, a young-researcher branch of the Royal Netherlands Academy of Arts and Sciences <https://www.tilburguniversity.edu/webwijs/show/e.j.koops/>. He is currently working on the COURAGE project.

DR. CHRISTOFOROS NTANTOGIAN

Dr. Christoforos Ntantogian received his B.Sc degree in Computer Science and Telecommunications in 2004 and his M.Sc degree in Computer Systems Technology in 2006 both from the Department of Informatics and Telecommunications of University of Athens. In 2009 he received his Ph.D. from the University of Athens (Department of Informatics and Telecommunications). Currently, he is an adjunct lecturer and senior researcher at the Department of Digital Systems of the University of Piraeus. Dr. Christoforos Ntantogian has participated in numerous projects realized in the context of EU Programs (e.g., CONTENT, ANA, CASCADAS). His research interests lie in the intersection of data analysis, applied mathematics and system/software security to develop practical systems with security intelligence. Christoforos currently works on the UINFC2 Project.

CORMAC CALLANAN

Cormac Callanan owns/operates an independent consultancy company from Dublin, Ireland called Aconite Internet Solutions

www.aconite.com) which provides expertise in policy development in the speciality area of international cybercrime and Internet security & safety. Qualified in Computer Science he has over 25 years working experience on international computer networks and 15 years' experience in the policy area of illegal content and cybercrime activities on the Internet. He was co-author of the Council of Europe Guidelines on Cooperation between Law Enforcement and Internet Service Providers quoted by the European Court of Human Rights as achieving the appropriate balance between sharing data and data protection. He is a member of the Irish Internet Safety Advisory Committee reporting to the Irish Department of Justice. He has provided training at Interpol and Europol and to law enforcement agencies around the world on the subject of emerging and developing technologies, cybercrime and the role of internet industry. Cormac is currently working on the COURAGE project.

DR. DAVIDE ARIU

Davide Ariu holds a research assistant position at University of Cagliari, working with the Pattern Recognition and Application Lab (<http://pralab.diee.unica.it>). He has a background on Pattern Recognition and Machine Learning applications to Computer Security, having obtained a Ph.D. in Computer Security in 2010. In 2007 he has been visiting Scholar at the Georgia Tech Information Security Center in Atlanta (U.S.). He has currently published 20 papers on peer-reviewed international journals, conferences, and workshops. He is one of the lecturers of the Computer Security course at the Department of Electronic Engineering, and is also among the organisers of Building Trust in the Information Age, a summer school on Computer Security and Privacy. Within PRA Lab Davide Ariu is also responsible for coordinating the activities concerning the

participation of the Lab in European, national, and regional projects. Currently, he is the project manager of the European projects DOGANA and CyberROAD. Formerly, he has been the manager of the projects ILLBuster and MAVEN, and of the regional project STATAIn 2015 he co-founded PLURIBUS ONE (<https://www.pluribus-one.it>), a research intensive spin-off of the University of Cagliari.

DIMITRIOS KAVALLIEROS

Dimitrios Kavallieros holds a BSc in Information Management and an MSc in Ethical Hacking and Computer Security. He has held previous posts as a Network/System Administrator in Pentelis Childrens Hospital, Programmer in Computer Solution SA. Since 2014 he has worked as a Research Associate at the Center for Security Studies (KEMEA), highly involved in European and National Research Programmes mainly focused in Cloud Security, Cybersecurity/Cybercrime and the relevant Ethical, Legal and Societal impact. Dimitris is currently working on the UINFC2 Project.

GABRIELA BODEA

Gabriela Bodea is senior policy researcher with TNO. Her area of research is the social impact of ICT. She specializes in privacy in relation to information and communication technologies, and in particular in relation to various aspects of e-Government (such as electronic authentication, homeland security, identity management); the future internet; and emerging and converging technologies. Gabriela currently works on the COURAGE project as part of her role at TNO.

GARY HIBBERD

Gary was appointed as Managing Director of Agenci Information Security in 2012 but began his career as an IT programmer back in 1985 and has had a passion for all things cyber related since then. His broad range of experience in almost every discipline in IT means he knows ‘What good looks like’ when it comes to protecting your business and reputation. He is a published author, experienced and qualified in Information Security & Business Continuity who is a passionate speaker on cyber security and related disciplines. He is regularly asked to present at conferences and schools to help raise awareness and understanding of real world, business related issues affected by our digital world. Gary has helped businesses as diverse as the RSPCA to LateRooms.com to improve their security and recovery capabilities across the world and held the role of European Crisis Management Leader for GE Money.

DI. GEOFF HALPIN

Geoff is the Detective Inspector leading the police Regional Cyber Crime Unit which forms part of the Yorkshire & Humber Regional Organised Crime Unit, and is recognised as one of the leading experts on cybercrime law enforcement in the UK. He leads a team of specially trained officers and staff working with partners in law enforcement, industry and academia to investigate and prevent the most serious incidents of cyber-crime at a regional, national and international level. He came to law enforcement from an academic background, having studied computing at university including security, artificial intelligence and neural networking/pattern recognition. He has over 20 years’ experience as a police

officer in Nottinghamshire, West Yorkshire and at the Regional Organised Crime Unit working in a variety of specialisms including homicide investigation, serious and organised crime, intelligence and cyber-crime. He has a particular interest in the use of computers for predictive policing including crime and disorder prevention, and intelligence development.

LT. COL. JERZY KOSINSKI

Lt Col Jerzy Kosiński, PhD Eng - professor at the Institute for Research on Crime and Terrorism, Police Academy in Szczytno. His scientific specialties are cybercrime and digital evidence. He was previously a member of Interpol and Europol expert groups on cybercrime. He has organised a series of cyclic international scientific conferences addressing the “Technical aspects of ICT crime”, “Electronic payment instruments abuses” and “IPR crime in Internet”. Author of numerous publications and presentations at conferences in the field of their specialization in science, J. Kosiński is also an expert witness in the cybercrime area.

JUDYTA KASPERKIEWICZ

Judyta Kasperkiewicz is a Polish advocate and Ph.D. candidate at Silesia University in Katowice, Poland. She specializes in cybersecurity and intellectual property law. She has substantial experience in criminal, civil and family law gained in Poland and the United Kingdom. She is a publisher of reviewed academic articles in law. She lives in New York.

LUIGI REBUFFI

Luigi Rebuffi has been with EOS ever since its creation in 2007. Having proposed and launched the initial idea of EOS in 2003, he now plays a strategic role in defining the mission and objectives of EOS; coordinates the implementation of the agreed strategy with Members and Partners; and supports and advises the EOS Members. Mr Rebuffi leads EOS' comprehensive advocacy approach and plays a key role promoting public-private cooperation on security in coordination with the activities of ASD and EOS Members. He ensures the effective and efficient implementation of projects, directs and manages the EOS team, and has a decisive impact in influencing EU policy-making in security through communication with the European Institutions at the highest level. In this capacity, he is an advisor on security issues to the Cabinets of several EC Commissioners, is a Member of the Security Advisory Group on EU Security Research of DG ENTR and is President of the Steering Committee for security research of the French ANR (National Research Agency). Having a background in nuclear engineering, before EOS he worked in different positions at ITER, Thomson CSF, and Thales.

DR. MICHAL CHORAS

Michal Choras obtained his Doctor of Science (habilitation) degree in computer science from AGH Cracow in 2014. Since 2015 he holds the professor position at University of Science and Technology (UTP) in Bydgoszcz, where he is the Chair of Teleinformatics Systems Division. Earlier, he obtained M.Sc. and PhD in telecommunications from UTP in Bydgoszcz in 2002 and 2005, respectively. He also works as consultant and project manager at ITTI Sp. z o. o.

His interests include cyber security, information management and pattern recognition in several domains, such as image processing, security (network security, urban security, and biometrics) and safety (crisis management, critical infrastructures). He has been involved in EU FP7 projects (e.g. INTERSECTION, INSPIRE, TACTICS, CIPRNet) and EDA projects (e.g. ATHENA). Currently, he is the coordinator of FP7 project CAMINO (www.fp7-camino.eu) on cybercrime and cyberterrorism. He is an author of over 150 reviewed scientific publications, including a number of publications regarding methods for cyber security, pattern recognition, image processing and security/safety applications. He is also a reviewer and Programme Committee member for over 35 journals and over 35 conferences. Currently, he is a vice-chair of IMG-S Thematic Area 7 on cyber security.

OLIVIER BURGERSDIJK

Olivier is currently head of strategy for the European Cybercrime Centre (EC3). After completing his university education (Criminology), Olivier Burgersdijk joined the Rotterdam-Rijnmond police force in The Netherlands (1998-2001), where he was active in the areas of conducting evaluations on major criminal investigations of serious and organised crime, as well as strategic analysis. From 2001 to 2006 Mr Burgersdijk supported as consultant various regional police forces and prosecution services in The Netherlands in the areas of quality management, evaluation and information management. From 2006 till present Mr Burgersdijk is active within Europol in different functions with responsibilities for information exchange and information management at strategic as well as technical levels. Since November 2012, he has held the post of Head of Strategy within the European Cybercrime Centre,

overseeing strategic analysis, outreach, expertise, R&D, specialised forensic tools & techniques.

PIM TAKKENBERG

Since 2014 Pim Takkenberg has held the position of Cyber Security director with Northwave. Mr. Takkenberg graduated from the high-grade Master's Programme in Police Leadership in 1999. In 2011 he graduated from the FBI National Academy (247). In 2006, Mr. Takkenberg joined the Dutch National High Tech Crime Unit (NHTCU). As head of the NHTCU, Mr Takkenberg was responsible for a unit dedicated to investigating advanced and organized forms of cybercrime. Successful cases conducted by the unit include the Bredolab Botnet takedown, the investigation of DigiNotar hack, and the investigation of the hacking of major telecommunication company KPN. In 2013, Mr. Takkenberg joined the Ministry of Interior and Kingdom Relations as head of the Cyber Intelligence Team (CIT). The CIT conducts investigations into digital attacks containing an aspect of cyber espionage or cyber sabotage, carried out primarily by state actors, and which in turn form a threat to Dutch national security and economy.

QUENTIN REVELL

Quentin has worked for the UK Home Office since 2001 developing technical surveillance tools and methods. Quentin has lead the development and support of a national GIS system - used for countering serious and organised crime. From 2010 he managed the Home Office - Biometric Centre of Expertise and supported the Home Office's Senior Biometric Advisor to provide horizon scanning and

technical assurance to the Home Office and across UK government / international partners. His research helped establish Centre for Applied Science and Technology (CAST) as a leader in understanding the use of automatic facial recognition from CCTV, and the issues of facial comparison. More recently Quentin has moved to work on Digital Investigations area and lead their Open Source Investigations programme. This programme brings together his knowledge of identity and surveillance to assure the Home Office that its use of Open Source Investigations across all of its priority areas (to Prevent terrorism, Cut crime and Control immigration) is Safe, Legal, Effective and efficient - now and into the future.

RAOUL CHIESA

Raoul Chiesa was born in Torino, Italy. After being among the first Italian hackers back in the 80's and 90's (1986-1995), Raoul decided to move to professional InfoSec, establishing back in 1997 the very first vendor-neutral Italian security advisory company; he then left it in 2012, and established along with former and new partners "The Security Brokers", a visionary joined stock company providing niche, cutting-edge security consulting services and solutions. Raoul is among the founder members of CLUSIT (Italian Information Security Association, est. 2000) and he is a Board of Directors member at ISECOM, OWASP Italian Chapter, and at the Italian Privacy Observatory (AIP/OPSI); he has been one of the coordinators of the Working Group "Cyber World" at the Center for Defence Higher Studies (CASD) between 2010 and 2013 at the National Security Observatory (OSN) at Italy's MoD. He is a former member of the ENISA Permanent Stakeholders Group (2010-2012 and 2013-2015), an independent "Special Advisor on Cybercrime and Hacker's Profiling" at the UN agency UNICRI, and a Member of the

Coordination Group and Scientific Committee of APWG European chapter, the Anti-Phishing Working Group, acting like a “Cultural Attachè” for Italy. Since July 2015 he’s a Board Member at AIIC, Italian Experts Association on Critical Infrastructures, a Subject Expert for ADETEF (different French ministries) at ENCYSEC (Enhancing Cyber Security), a project funded by the European Union, and a member of the ITU (UN-Geneva) Roster of Experts on Cybersecurity. Raoul publishes books, white papers and articles worldwide, which are often translated in different languages (English, French, Italian, Romanian, Spanish, Chinese) as main author or contributor, while being since more than 20 years a worldwide known and appreciated Key Noter and Speaker; giving all of the above, Raoul is a regular contact for worldwide medias (newspapers, TV, radio, podcasts and bloggers) when dealing with Information Security issues, ICT security incidents and IT trends.

ROBIN DE HAAS

Robin de Haas is Program Manager for the Hague Security Delta. After getting a Master of Business Administration with a specialization in Change Management, Robin served in the Dutch Army as an officer during military service. After this he joined Randstad for three years and worked as an intermediary between businesses and personnel. Robin worked for 17 years at TNO Defence, Safety and Security as program manager for the Next Generation Combat Aircraft and the Replacement F-16 program. His involvement with the Hague Security Delta started in 2007 working as program manager of the Secure Haven project. This project worked out scenario’s and blueprints for the municipality of The Hague to become a city that combines economy and security and is nice to live and work in. He was head of the department Networked Organizations which has

expertise on Crisis management, Critical Infrastructures, Urban Security and Cyber Security. Robin has been responsible since 2011 for the development of TNO’s cyber security R&D portfolio. As a program manager at The Hague Security Delta his main focus area is creating and stimulating triple helix cooperation between government, businesses and knowledge institutes in the field of Cyber- National- and Urban Security.

ROCCO MAMMOLITI

Rocco Mammoliti has over 15 years of experience in the information security industry and has also carried out research and innovation in information engineering and biomedicine. He is the author of several scientific publications on topics related to modelling, data mining, and ICT security as well as on issues of innovation and new technologies. He has worked for companies of significant importance in the field of IT and telecommunications industries such as Bull and Telecom Italy, covering in time the roles of Head of IT Security and Chief Information Security Officer. He is a member of international professional associations including the IEEE and the Computer Society. His main areas of expertise are related to domains in the Network & Information Security, creation and management of SOC (Security Operations Center) and CERT (Computer Emergency Response Team), Abuse & Cybercrime Prevention, Child Online Protection, etc. He is currently Head of Security function of Poste Italiane, in which he oversaw the creation of the Italian Post Office CERT. He holds the position of Technical Manager of Scientific-Technological District Cyber Security and General Manager of GCSEC Foundation (Global Cyber Security Center), of which the Italian Post Office is a founding member.

STUART HYDE

Stuart Hyde QPM has Completed a full career within the Police service in the UK with Exemplary Service and national recognition through the awarding of the prestigious Queens Police Medal and presentation of an Honorary Doctorate for commitment to Cybercrime prevention and detection. Director of Stuart Hyde Associates and spokesperson on a range of technical and cyber issues supporting a number of individuals and organisations with specific Digital Forensic, Cybercrime and personal consultancy. He has a unique understanding of national strategic and operational tactical understanding to help create effective improvements and solutions.As a member of the Europol Internet Security Advisory Board and Vice President of two Not for Profit organisations he is ideally placed to add value to any debate on Cybercrime. He is a Director of Solutions for CCL Digital Forensics and an Associate for the innovative Cybx cyber Exercise training facility at the Emergency Planning College.He runs Stuart Hyde Associates and has developed the concept of Digital Leader to address the lack of cyber and digital knowledge amongst senior and middle managers.

DR. WOJCIECH MAZURCZYK

Wojciech Mazurczyk received his B.Sc., M.Sc., Ph.D. (Hons.), and D.Sc. (Habilitation) degrees in telecommunications from the Warsaw University of Technology (WUT), Warsaw, Poland, in 2003, 2004, 2009, and 2014, respectively. He is currently an Associate Professor with the Institute of Telecommunications, WUT, where he is the Head of

the Bio-Inspired Security Research Group and a Researcher at the Parallelism and VLSI Group at Faculty of Mathematics and Computer Science at Fern Universitat, Germany. He is an author or co-author of over 100 papers and over 30 invited talks devoted mainly to network security. His research interests include bioinspired cybersecurity and networking, information hiding, and network security. He is involved in the technical program committee of many international conferences, including the IEEE INFOCOM, the IEEE GLOBECOM, the IEEE ICC, and ACSAC. He also serves as a reviewer for major International magazines and journals. Since 2013, he has been an Associate Technical Editor of the IEEE Communications Magazine (IEEE Comsoc) and an IEEE Senior Member.

CONSOLIDATED RESEARCH AGENDA

OUR COMBINED VISION FOR THE FUTURE OF CYBERCRIME RESEARCH

In response to suggestions made at the joint first review meeting of the CAMINO, COURAGE and CyberROAD projects, held at the offices of the European Commission, Brussels on June 4th 2015, the three consortia have undertaken to consolidate each of their respective outputs into a single, unified and easily digestible research roadmap that can be distilled to inform future works, related policies and funding initiatives that address the challenges being faced by society due to the proliferation of cybercrime and the threat of cyberterrorism. Underpinning each of the existing cyber roadmap frameworks were a series of integral and interlinked dimensions. These four features; Technical, Human, Organisational, and, Regulatory, are each individually attributed to all aspects of cybersecurity strategy, resilience, and vulnerabilities. Due to the broad and complex scope of cybersecurity concerns and challenges,

each research agenda items, essential research agenda item fits into at least one dimension of the THOR categorisation, however many are at least partially linked to more than one. Therefore, the THOR analysis does not propose itself to be the sole identifying means of categorization, rather as a set of key underlying factors that are flexible, dynamic and interchangeable in order to address the plethora of fluctuating contemporary European cybersecurity challenges. The following provides an overview of the topics included in the current draft of this consolidated agenda, highlighting a number of what we collectively consider to be priorities for future research and practice. We do not consider these topics to be comprehensive, and invite you to submit your own ideas throughout the conference at bit.ly/CyberRoadmap.

TECHNICAL

STRENGTHENING EMERGING TOOLS FOR BIG DATA ANALYSIS, CLOUD FORENSICS AND SECURITY

Cyber-attacks are not always immediately visible due to their nature or intensity (e.g., amount of traffic they introduce). Therefore, recently techniques using big data tools have been adapted. Recent research has shown that in depth analysis of large volumes of data (received from different segments of IT networks) has a unique capability of revealing interesting patterns. This concept can potentially be adapted and applied to many cyber-security areas, namely: spam detection, botnets detection, malwares analysis, web-based infection, network intrusion detection systems.

Consolidated Roadmap				
Dimensions (THOR)	Regulatory	Dealing with different levels of legal frameworks for illegal content: questions of geolocation and jurisdiction	Electronic identity and trust services for data protection across borders	Comprehensive legal system to fight against CC/CT
	Organisational	Adapting organisations to the cross-border nature of the Internet and cybercrime/terrorism	Creating user-friendly terminology, language and features to assure a better understanding of cyber security challenges	Promoting EU institutional support to generic challenges and obstacles at the enterprise/company/SME level including incentives for cyber insurance
	Human	Collective awareness and education for increased societal resilience to CC/CT threats	New standards for private data minimisation, appropriate use and re-use of data and Privacy Enhancing Technologies	Definition, characteristics and behaviors of the offenders and victims in cybercrime
	Technical	Strengthening emerging tools for big data analysis and cloud forensics and security	Establishing metrics and framework for cyber security testing	Countering cyber crime affecting mobile and IoT devices
Topics				

This topic is focused particularly on the correlation of capabilities for big data analysis and scalability of big data tools and methods. The topic includes also consideration on challenges related to the realistic workload conditions of currently used test-beds that have to operate in real-time or near real-time. Moreover security of big data infrastructures is also addressed.

As a result of the recommendations given in this topic, we expect that typical network monitoring solutions will evolve to context aware systems which allow the user to identify current cyber security problems and what is more important – their roots. The second important expectation is the test beds community using wide variety of data samples (data sets) containing different malwares, real and synthetic network traffic characteristics (or other challenging problems) that will be widely available to researchers.

ESTABLISHING METRICS AND FRAMEWORKS FOR CYBER SECURITY TESTING

One of the most important and demanded aspects in every product, system or even organisations is quality; guaranteeing fundamental characteristics such as reliability or availability in any system, moreover if it is a security one, is an essential part of revealing the development team's confidence in their system or product. Therefore, activities focused on maintaining and improving this quality are needed, and the most effective ones are testing and simulation processes. Concepts such as automated tools or cyber exercises between companies will help to raise the awareness of not only cyber security responsible people, but also of the rest of the staff. And finally, in order to promote and encourage the realisation of all these necessary actions, proper regulations and standards

should be made and discussed, and thus achieve a desirable and prepared environment to benefit all these good practices.

Therefore, the key points of this topic include Security-by-Design issues, development of representative security metrics, sharing of information about vulnerabilities, and building open test beds for testing cyber security. On the other hand, issues of access control and trust management in distributed environment are also addressed. Finally, the ultimate goal of development and implementation of the specified topic milestones is objectiveness and measurability of cyber security for assurance purposes.

COUNTERING CYBERCRIME AFFECTING MOBILE AND IOT DEVICES

Nowadays, one of the main challenges affecting countering cyber-crime is large and still increasing amount of malware samples. Evolution and changeability of malwares and botnets (e.g. new, fast-evolving botnet architectures) are also factors that should be addressed by the research communities to more effectively fight against cybercrime. This is particularly important in the context of limitations of existing signature-based scanners and malware detectors. On the other hand, cybercrime affects also mobile devices, and in the near future will affect micro devices (now not often connected to the Internet), that will be exposed to cyberattacks in conjunction with growing popularity of IoT (Internet of Things) concept.

Primarily, this topic focuses on development of new paradigms for fighting against malware targeting mobile and small/micro devices, including new ways to counter evolving and robust botnets and their detection. Investment in large-scale (even Internet-scale) testing environment is also one of the points addressed in this topic, due

to the need for prediction of botnet evolution, safe observation of malware spreading directions and timing, as well as setting up the most effective containment strategies.

HUMAN

COLLECTIVE AWARENESS AND EDUCATION FOR INCREASED SOCIETAL RESILIENCE TO CC/CT THREATS

This topic focuses on the identification and facilitation of new approaches to enable the increased resilience of society to cybersecurity threats through increasing the awareness and education levels of stakeholders across society; ranging from citizens through to security professionals, policy makers and the full spectrum of private sector and critical infrastructure providers. Prevention strategies, and in this context, particularly those associated with increasing awareness and standards related to online safety and information security play an important role in improving societal resilience to cybercrime, while 'human security' specifically is an important factor as popular attack vectors such as social engineering and phishing continue to exploit human security vulnerabilities.

Under this topic research should focus on the identification of new approaches to increasing societal awareness, and subsequently readiness, to deal with cybersecurity threats and thus cybercrime. Where necessary, the impact of new and emerging technologies and behavioural changes that occur because of them should be identified and considered. The research proposed should identify and address awareness and education requirements across levels

and sectors, such as national teaching curricula, law enforcement and other public and private sector institutions.

NEW STANDARDS FOR PRIVATE DATA MINIMISATION, APPROPRIATE USE AND RE-USE OF DATA AND PRIVACY ENHANCING TECHNOLOGIES

With surveillance powers and techniques a very current topic, both from the perceived excessive use in some quarters and the inadequate interpretation of available evidence in others, the roadmap towards more effective implementation of Privacy Enhancing Technologies is inexorably entwined with the development of forthcoming legislation, and the regulatory interpretation of these. In particular DPR, eIDAS, and Payment Services Directive 2's early adoption through SecuRe Pay, introduce requirements for the adoption of PETs (Privacy Enhancing Technologies), albeit through the adoption of undetermined techniques or technologies, even in advance of their formal ratification into EU or Member State legislation. These advance regulatory roadmaps provide an interesting, and often unexpected, set of requirements to the organisations handling sensitive personal data.

Other issue raised in this topic is the fact that under a range of current regulations and industry standards, across a wide and varied range of industries, the use of data is frequently, but not universally, restricted to the use originally intended when data was collected. Users also face a range of opt-ins or opt-outs to the use, or subsequent re-use, of this data. The advent of big data has made the search for new uses of data held on existing systems a growth industry, but there are strong Human and Ethical concerns raised through this re-use. The application of these existing data

sets for LEA purposes has caused some debate, and our Roadmap will provide pointers to those issues that need to be addressed and to what timescale.

DEFINITION, CHARACTERISTICS AND BEHAVIOURS OF THE OFFENDERS AND VICTIMS IN CYBERCRIME

The scale and proliferation of Internet use as a means to facilitate crime has also introduced new challenges for the social and behavioural sciences, in addition to the technological and criminological disciplines we normally associate with studies in the domain. Due to the potential overlaps and absences of clarity in distinguishing between cybercrime, cyberterrorism, cyber warfare, and often the inability to immediately identify the origin of an attack means that there is significant benefit in assessing the impact of an attack and discerning the potential motivations behind it. The enormous widespread impact exerted by modern cybercrime means that individuals and groups involved in committing, responding to, and preventing events, is equally expansive. The sheer quantity and diversity of the number of criminals and victims of cybercrime means that despite the importance of analysing the various different actors, there has been little progress to date.

In order to develop and deliver improved intervention and prevention measures, this research topic proposes research to help build our understanding of the diverse range of actors involved. Research has shown that cybercrime is no longer the reserve of technically skilled individuals and groups, so more work is needed to establish the underlying factors that contribute to the profiles of victims and offenders alike, in addition to establishing human, environmental and other PESTLE factors that drive cybercrime.

ORGANISATIONAL

ADAPTING ORGANISATIONS TO THE CROSS-BORDER NATURE OF THE INTERNET AND CYBERCRIME/ TERRORISM

Nowadays, competitiveness is global, so any company or system can receive an attack from anywhere on the planet. Therefore, it is vitally important that regulatory differences between countries are known and understood, and in consequence organisations should be aware of this fact and protect their assets and intellectual property taking this into account. Organisations need to adapt to think, protect their systems and networks, and cooperate without borders. Therefore, key research points of this topic concern homogenisation of law, cooperation between Law Enforcement Agencies (LEAs), CERTs, governmental cooperation in terms of cross-border monitoring and information sharing. Top priority milestones include also interoperability of forensic, in particular tools and best practices.

CREATING USER-FRIENDLY TERMINOLOGY, LANGUAGE AND FEATURES TO ASSURE A BETTER UNDERSTANDING OF CYBER SECURITY CHALLENGES

The definitions and understanding of terminology used in reference to cybercrime and cyberterrorism are, in some instances, inconsistent across EU Member States, potentially causing confusion and in extreme cases hinder law enforcement, prosecution and

international cooperation efforts due to the ambiguity surrounding the subject area in general. Harmonising terminology in both areas of cybercrime and cyberterrorism is crucially important in defining how the LEA sector should cooperate in an EU and broader international context. Without a clear understanding of the characteristics that distinguish them, these areas will be hard to address properly across all relevant levels. The absence of equal representation and understanding of terms from both areas of cybercrime and cyberterrorism, the lack of definition of terms and the different taxonomy in current use in the field is identified as a problem by academia, LEAs, and by entities representing legal and ethical organisations as well as from the critical infrastructure stakeholders.

In this topic, it is proposed that efforts must be made to increase levels of knowledge exchange among stakeholders, leading to the provision of harmonised and standardised terms through the development of a new taxonomy framework that involves all aspects of cybercrime and cyberterrorism, specifying their differences and commonalities.

PROMOTING EU INSTITUTIONAL SUPPORT TO GENERIC CHALLENGES AND OBSTACLES AT THE ENTERPRISE/ COMPANY/ SME LEVEL INCLUDING INCENTIVES FOR CYBER INSURANCE

Common / unified institutional support is needed to promote changes at the Enterprise, company and SME levels. The creation of an expert committee at the request of the main involved countries can contribute to overcoming these obstacles and challenges at a European level. In addition, an information sharing platform can help the approach and collaboration between interested parties, making quick and efficient ideas/problems sharing possible. This support

will assure the minimum protection needed in these organisations.

On the other hand, it is widely accepted that achieving perfect security is impossible. Security accidents and data breaches will occur regardless the amount of security controls and practices applied (though with much lower frequency). Thus, organisations have to deal with the residual risk. Recently, insurance, a usual treatment approach for residual risk, was applied to the cyber world. The developing cyber insurance market faces a number of unique as well as usual (for insurance) challenges. In particular, heavy information asymmetry, lack of statistical data, interconnected security and correlated risks, rapid change of risk landscape, unclear underwriting language, etc.

REGULATORY

DEALING WITH DIFFERENT LEVELS OF LEGAL FRAMEWORKS FOR ILLEGAL CONTENT: QUESTIONS OF GEOLOCATION AND JURISDICTION

Cybercrime is inherently a cross border issue, potentially involving a number of different countries and territories each with their own legal frameworks and jurisdictions. This 'internationalisation' of crime creates new challenges for law enforcement. This includes issues such as the reporting and deletion of illegal content, the collection of court evidence, cross-border accessibility of data and other issues.

In this research topic, the identification and development of new methods that enable LEAs to gather and share information across

geographic borders resulting in improved cross border cooperation among international and public/private authorities and to support the development of new standards for harmonising collaboration between the private sector and law enforcement.

ELECTRONIC IDENTITY AND TRUST SERVICES FOR DATA PROTECTION ACROSS BORDERS

The research community will need to address the technical standards to be agreed for the degrees of identity and authentication, and the circumstances under which each is appropriate. The research community will play a vital role in this area as what is perceived to be ‘uncrackable’ in some Member States (or nations outside the European Union) could have relatively trivial flaws when looked at from outside. A majority of classes and applications of Cybercrime and Terrorism contain a misrepresentation of identity or attempt to authenticate access to goods or services that the attacker has no legitimate use for. Currently a plethora of standards exists that enable the identification and authentication of genuine users. At present there is no interoperability of these, and poor controls over the degree to what constitutes ‘strong authentication’ sufficient for each respective application.

The proposed research identified in this topic includes the timetable for the implementation of eIDentity, Authentication & Signature regulations, and the steps necessary to ensure its impact internationally. Equally, with the payments industry now being required to look at early adoption of the Second Payment Services Directive (PSD2), the Identity/Authentication roadmap has moved forward dramatically as one of the key cybercrime asset classes, and one of the most likely candidates for higher level eIDAS requirements.

COMPREHENSIVE LEGAL SYSTEM TO FIGHT AGAINST CC/CT

This topic reflects the current needs and challenges that facilitate requirements for improvements to the legal systems and related processes that impact upon all phases of cybercrime cases. One of the main efforts to be done in this area is the improvement of digital forensic products, services and procedures. In particular, it is important to ensure an adequate flow of information at the different stages of the investigation - from disclosure of crime, securing and preserving evidence and its processing, up to the judicial decision.

In this context it is also important to ensure and develop appropriate levels of knowledge and expertise across all the actors involved in the judicial process. The major improvement in information sharing and cooperation between victims, LEAs (the Police), the prosecution and forensic experts and finally the judges/courts is needed.

SUBMIT YOUR OWN
IDEAS FOR FUTURE
RESEARCH ITEMS AT

[BIT.LY/CYBERROADMAP](https://bit.ly/cyberroadmap)

COURAGE PROFILE

CYBERCRIME AND CYBERTERRORISM EUROPEAN RESEARCH AGENDA



The COURAGE (Cybercrime and cyberterrorOrism (E)UropeanResearch AGenda) project is funded by the European Commission's seventh framework programme for research. COURAGE will produce a research agenda and roadmap for cybercrime and cyberterrorism using the expertise of the consortium partners, advisory board members and the project's extended network of domain experts and stakeholders.

The research agenda will identify the major challenges; reveal research gaps and recommend practical research approaches to address these gaps through strategies that are aligned to the real-world world requirements of practitioners, policy makers, citizens and other stakeholder groups. These strategies will be supported by test and evaluation schemes defining metrics and performance indicators used to assess the impact of actions taken as a result of

the project's research roadmap. COURAGE's work is undertaken with the overall objective of defining practical, grounded approaches that will assist in supporting business and critical infrastructures, the capability of crime investigators and enhancing the overall security of European society as a whole.

To achieve this, COURAGE has undertaken to address a broad range of key challenges, such as the speed and implications of technological change, raising awareness and education levels, the transnational scope and nature of cybercrime, data protection and cooperation and information sharing issues, amongst others. The COURAGE approach is based on three pillars:

1. A user centric methodology - to identify gaps, challenges and barriers based on real-world needs and experiences.
2. An analytical and semantic approach - to deliver taxonomy; create a common understanding of the subject, and to review current and existing approaches and initiatives aiming to positively impact upon the domain.
3. A competitive and market oriented approach – to foster the practical implementation of counter-measures, using effective test and validation solutions.

<https://www.courage-project.eu/>

[@FP7_COURAGE](#)

COURAGE PARTNERS

[European Organisation for Security](#)

[CFNTRIC, Sheffield Hallam University](#)

[United Nations Interregional Crime and Justice Research Institute](#)

[Cybercrime Research Institute](#)

[TNO](#)

[Swedish Defence Research Agency](#)

[Office of the Police and Crime Commissioner for West Yorkshire](#)

[Engineering Ingegneria Informatica](#)

[Aconite Internet Solutions](#)

[EstEnter Polska](#)

[Conceptivity SARL](#)

[Institut Jozef Stefan](#)

[Selex ES SPA](#)

[Fraunhofer Institute of Optronics, System Technologies and Image Exploitation](#)

[Tilburg University](#)

[International Cyber Investigation Training Academy](#)



CAMINO PROFILE

COMPREHENSIVE APPROACH TO CYBER ROADMAP COORDINATION AND DEVELOPMENT

The CAMINO (Comprehensive Approach to cyber roadMap coordINation and develOpment) project was founded with the goal of providing a roadmap for improving resilience against cybercrime and cyber terrorism. The consortium has roots in the Integrated Mission Group Security (IMG-S) Cyber Theme Area, where the cyber security partners have an extensive experience in developing roadmaps. The participation of the Supporting Members in the CAMINO project, coming from Europe and North America (USA and Canada), ensured that the roadmap benefits from the vast knowledge and experience. The consortium have a very practical approach, with most partners being SMEs with a good understanding of what is realistic and practical and with an interest in finding a constructive roadmap complementing LEA and research organisations — without creating a bottleneck

of problems and obstructions. The consortium used a holistic approach, analysing functions and capabilities addressing technical and human issues which are inter-related with legal and ethical aspects. We followed so called CAMINO THOR approach where cyber security is perceived comprehensively in 4 dimensions: Technical, Human, Organisational, and Regulatory. In each of the dimensions some items are proposed for the roadmap. In parallel with looking at the human and technical aspects, the project is focused on strong involvement of various different groups and operators such as LEAs, CERTS, personal users, governments, industry and research and commercial organisations. During the project we developed the CAMINO roadmap (research agenda). For each THOR dimension we identified 3-4 top priority topics that have to be addressed to more effectively fight against cyber crime and cyber terrorism. Each of these topics is described in the roadmap and is presented in the unified way. Topic description includes summary of key research objectives, summary of stakeholders with their roles in relation to given topic and detailed timeline. In this timeline we specified concrete milestones for three different time-spans (2017, 2020 and 2025). Such timelines briefly explain also current situation in given topic and expected (desired) end-vision at 2025, after the roadmap milestones achievement. Finally, topic timelines include summary of research activities that should be performed, leading to the defined milestones achievement. Also, we constituted the CAMINO Cyber Think-Tank. Its main objective is the exchange of experience and knowledge, as well as the dissemination of information related to the effective measures against cyber crime and cyber terrorism. Its members would like to support national and international decision makers and EC in the area of cyber security.

<http://www.fp7-camino.eu/>

[@fp7_camino](#)

CAMINO PARTNERS

[ITTI Sp z o.o.](#)

[CBRNE Ltd](#)

[Consiglio Nazionale delle Ricerche](#)

[Data Fusion Research Center AG](#)

[Espion Ltd](#)

[Everis Aeroespacial y Defensa S.L](#)

[Montpellier University](#)

[Police Academy in Szczecin](#)

[S21sec Information Security Labs S.L](#)

[Sec-Control Finland Ltd](#)



CYBERROAD PROFILE

DEVELOPMENT OF THE CYBERCRIME AND CYBERTERRORISM RESEARCH ROADMAP

CyberROAD (Development of the Cybercrime and Cyberterrorism Research Roadmap) is a research project funded by the European Commission under the Seventh Framework Programme. The project is aimed to identify current and future issues in the fight against cybercrime and cyberterrorism in order to draw a strategic roadmap for cyber security research. The CyberROAD roadmap leverages on a sound roadmapping methodology and is built on top of a detailed snapshot of the technological, social, economic, political, and legal scenario on which cybercrime and cyberterrorism do develop. Within this scenario, research gaps and priorities are identified.

WHY CYBERROAD?

Recent studies on the evolution of the principal cyber threats reveal scenarios characterized by the growth of cyber criminal activities.

Even though the level of awareness of cyber threats has increased, and law enforcement acts globally to fight against them, illegal profits have reached unsustainable figures. The estimated annual cost over global cybercrime is 500 billion dollars (more than 500 million victims per year, 18 victims per second). More than 600000 Facebook accounts are compromised every day. In addition to the economic reasons, cyber attacks often hidden political and social motivations which constitute a serious threat to national security (hacktivism, cyber espionage, cyber warfare).

WHAT IS CYBERROAD DOING?

The main objective of CyberROAD is “developing the Cybercrime and Cyber-terrorism research roadmap”. This roadmap is built through an in-depth analysis of all the technological, social, legal, ethical, political, and economic aspects on which cybercrime and cyberterrorism are rooted. The research roadmap is being built by the means of a sound roadmapping methodology and by co-ordinating the efforts of the CyberROAD consortium along three key directions: Technology; Society; Cybercrime and cyberterrorism

The CyberROAD Consortium: The project, being implemented by a consortium of 20 partners from 11 different countries, relies on a large body of competences. The consortium, which is also supported by a board of external advisors, represents all the players and the stakeholders involved in the fight against cybercrime and cyberterrorism: law enforcement, public bodies, universities and research centers, as well as companies and industries.

<https://www.cyberroad-project.eu/>

[@cyberroad_eu](#)

CYBERROAD PARTNERS

[University of Cagliari - PRA Lab](#)

[Technical University of Darmstadt - Germany](#)

[INDRA - Spain](#)

[Poste Italiane - Italy](#)

[SecurityMatters - Netherlands](#)

[Vitrociset - Italy](#)

[Foundation for Research and Technology - Hellas](#)

[INOV - Portugal](#)

[National Center for Scientific Research DZDemokritosdz - Greece](#)

[SBA Research - Austria](#)

[PROPRS Ltd - UK](#)

[Research and Academic Computer Network - Poland](#)

[Policia Judiciária - Portugal](#)



UINFC2 GET HANDS ON!

ENGAGING USERS AND PREVENTING AND FIGHTING CYBERCRIME AND CHILD SEXUAL EXPLOITATION

The vociferous proliferation of cybercrime has resulted not only in an increased number of reported incidents, but also in the ferocity, persistence, variety and potential impact (both societal and economic) of the underlying attacks on an increasingly diverse range of targets (i.e. persons, services, entities). This increase can be attributed to a range of factors, such as: a) the overall growth of the internet; b) the penetration of web services in our daily lives; as well as c) the latest technological achievements in ICT that enable many criminal actions to be transferred online; due to perceptions of anonymity and potential to obscure evidence. As one specific facet of this overall trend, the internet has seen a stark rise in its use as a vector for online sexual solicitation of children as well as the possession and subsequent distribution of explicit and abusive material.

In response, the UINFC2 project aims to assist in the cooperation and coordination among all major EU stakeholders, National Authorities, Law enforcement Agencies, National Hotlines & relevant EU bodies through the (real-time) provision of structured, analysed and correlated information. UINFC2's main objective is to design, develop and pilot a software platform providing intelligent analysis of collected or maintained data. The UINFC2 platform facilitates automated monitoring and inspection of provided data, as well as seamless crawling of suspicious content in the effort to identify the extent of possible incidents, information to make available to relevant stakeholders in order to enhance their capacity and capability to detect and remove explicit and abusive material from the web.

The platform will be tested during ongoing pilot operations carried out at a European level. The Input and feedback from these tests aims to capture end-user requirements and comments, leading to the refinement of the platform and the expansion of its functionality.

GET HANDS ON WITH THE PROJECT!

As part of this process, we're delighted to invite you to get hands on with the UINFC2 software platform over the course of the conference. You can find us situated in the conference staging area throughout the duration of the conference, so please feel to come and give the system a try for yourself!

<http://www.uinfc2.eu/wp/en/>

[@UINFC2](#)



These projects received funding from the European Commission's Seventh Framework Programme for research, technological development and demonstration under grant agreement numbers: 607306 (CAMINO), 607949 (COURAGE) and 607642 (CyberROAD) under FP7- SEC-2013.2.5-1.

