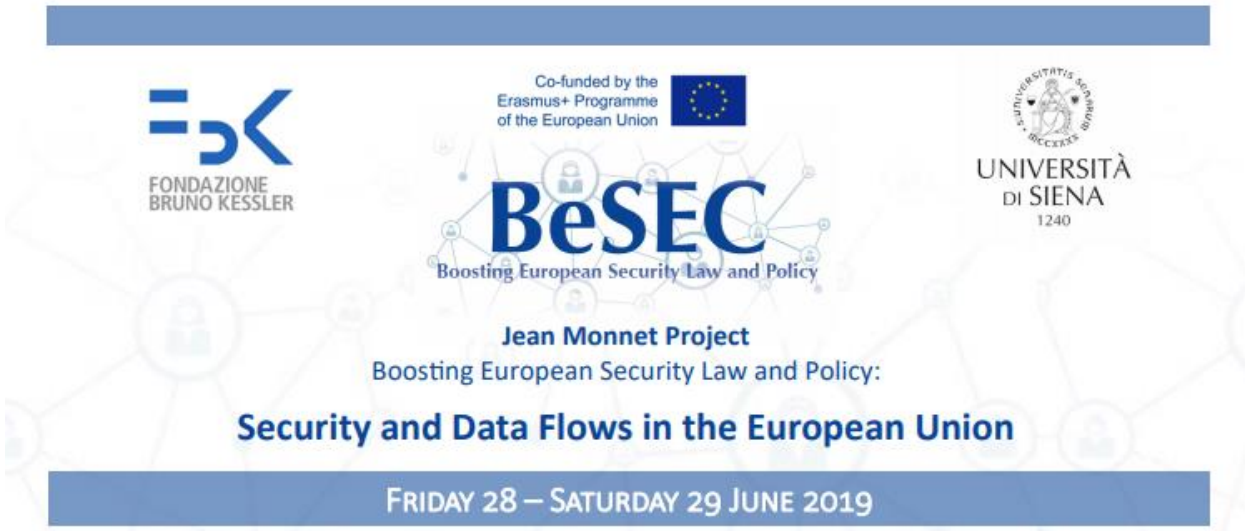


Speakers and Abstracts

PASQUALE ANNICCHINO, Bruno Kessler Foundation and Archimede Solutions

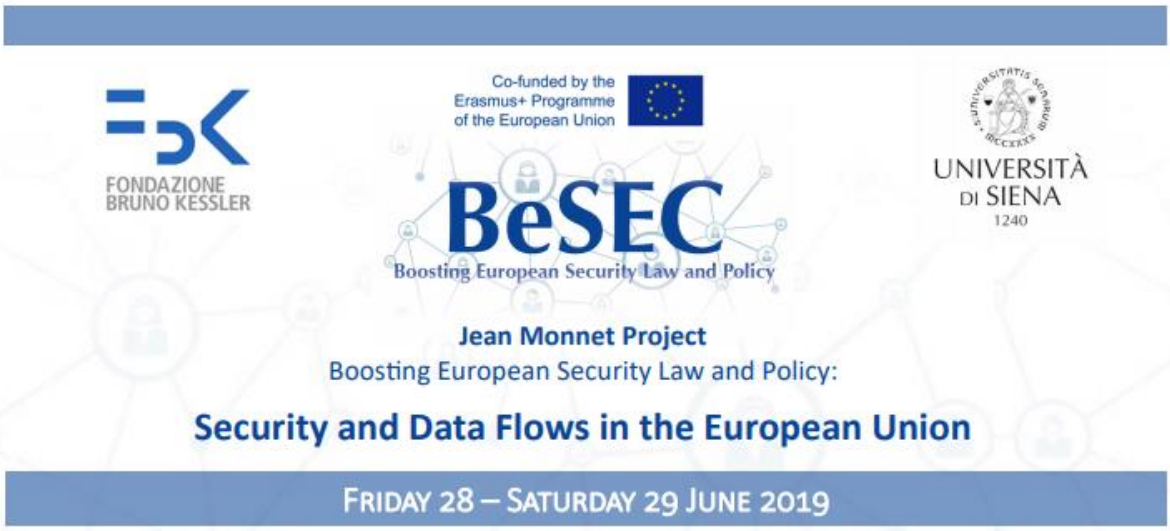
Dr. Pasquale Annicchino is a qualified Associate Professor of Law. He works on data protection and security in the context of different research and non-research projects. He also serves as DPO. In 2018 he was Visiting Professor at FGV Law School in Rio De Janeiro. He taught at St. John's Law School in New York and in several others European and American Law Schools. He is the Scientific Director of Lex Digital-Data Economy & Law Institute. His main research interests include the followings: National Security Law, Surveillance Laws, Global Law and Religion. Among his last publications: Law and International Religious Freedom. The Rise and Decline of the American Model, Routlege, 2017 (ICLARS Series on Law and Religion).

Abstract: Datification of society and the surveillance on religious minorities

The increasing use of technologies of surveillance through data gathering is here to stay. This contribution evaluates the paradigmatic shift brought to the field of the protection of the rights of religious minorities by highlighting recent developments in the U.S. and China. How can we provide tools and instrument that, by design, guarantee the protection of fundamental rights of religious minorities? What challenges pose the datification of society to legal scholars? These and other questions will be addressed.

ALESSANDRO CILARDO, University of Naples, Federico II

Alessandro Cilardo is an Associate Professor at the University of Naples Federico II. He authored around 75 peer-reviewed papers published in leading scientific journals and conferences, including various IEEE and ACM transactions. His research focuses on high performance computing, digital design methodologies as well as cryptographic processing components. He is involved in a number of funded projects at the national and the European level (7FP and H2020 projects). He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a member of the European Network of Excellence on High Performance and Embedded Architecture and Compilation (HiPEAC), and a member of the CINI Cybersecurity National Laboratory.



Abstract: At the foundation of cybersecurity: can we trust today's processing technologies?

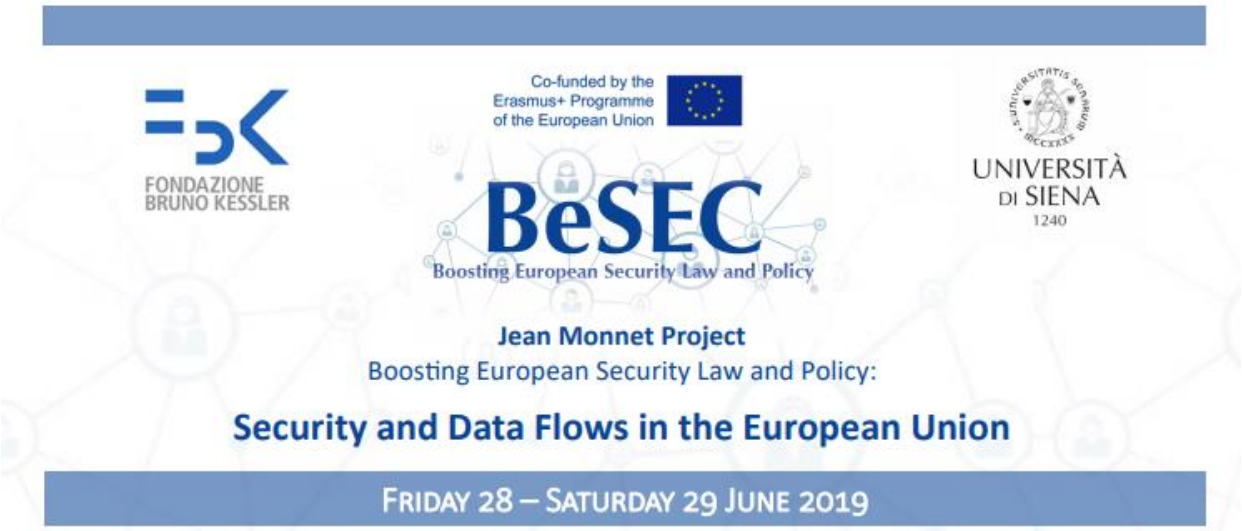
As shown by many recent exploits, digital security increasingly involves low-level processing technologies - the building blocks of our digital infrastructures- ranging from silicon chips, up to assembled components or whole systems. Such building blocks pose special challenges for digital security. To infrastructure integrators or system administrators they essentially appear as black boxes, yet they have potential disruptive effects in terms of security. Hardware trojans, backdoors, side-channel leakages, unprotected execution environments, etc. are all different flavors of the security vulnerabilities introduced by processing building blocks at different levels of the system architecture. By either interfering with the production cycle or controlling low-level physical mechanisms during the usage, an intruder can easily bypass higher-level security measures, e.g. access control or intrusion detection applications, which are ultimately just software programs running on top of potentially untrusted platforms. Not surprisingly, during the very recent years, we have witnessed a worldwide race toward owned processing technologies, including the recently started European Processor Initiative. Such long-term governmental strategies have of course strong commercial and economic motivations, but the control of the full production cycle, mostly for security purposes, plays an essential role as well. Consequently, the security dimension in processing technologies is expected to become increasingly relevant for public institutions and policy-makers in the near future. The talk will provide fundamental insights of the security issues behind today processing building blocks and their integration in digital infrastructures, as well as the challenges and opportunities that the European economy will soon face in this scenario.

ANDREA DE MARIA, Istituto Poligrafico, Zecca dello Stato

Andrea De Maria, Master Degree in Electronic Engineering, is managing the ICT R&D in the Italian Secure Printing House "Poligrafico e Zecca dello Stato Italiano", where he works from 2006 on secure documents and digital services. Before joining the public sector has worked on embedded security (telco and banking). Has launched a cooperation network with Research Centers such as Universities and Bruno Kessler Foundation to bring together all the necessary competencies to build secure systems for the Public Administration and the citizen.

Abstract: How a digital identity scheme has been built

Electronic identification (eID) is a key enabler for secure cross-border electronic transactions and a central building block for a European Digital Single Market. The eIDAS regulation allows citizen from



a Member State to get services from the Public Administration of other states without the need of getting another eID. The Italian Ministry of Interior, the Italian "Agency for Digital Italy" and the Italian Secure Printing House and Mint, together with FBK have built a secure eID based on the Italian ID card. What is the objective of the project, and how it was achieved? A novel approach for a government project.

IGOR FALCOMATÀ, ISACA Venice

Igor Falcomatà works as security consultant and ethical hacker, conducting penetration tests and risk analysis for public and private companies. He is also founder of Sikurezza.org, one of the biggest Italian infosecurity communities, an independent and hacker-centric place for information exchange and interaction between the underground, the academic world, researchers and users.

Abstract: Smart cities vs (?) cybersecurity

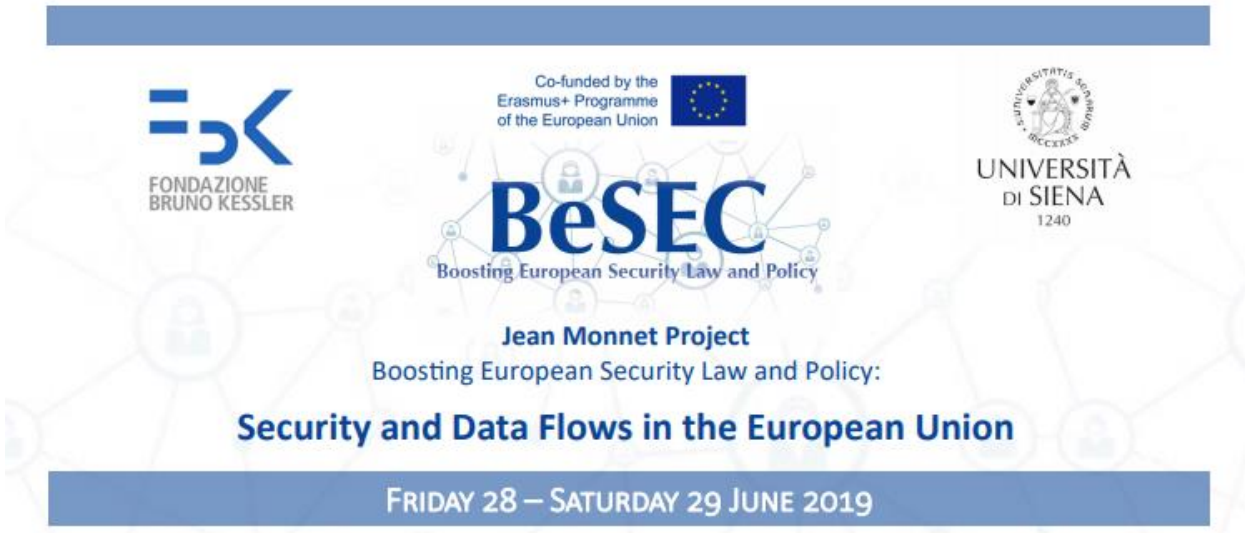
Billions of devices connected to the Internet, thousands of sensors in our (Smart) City IOT Security, System and Network Security, Application Security, Malware, Ransomware. What could possibly go wrong? A brief introduction the cybersecurity issues and challenges for the Smart Cities: what are the risks, what are the consequences, how can we avoid them?"

PAOLO GUARDA, University of Trento

Paolo Guarda, PhD in Comparative and European Legal Studies, is Assistant Professor of Comparative Law at the Faculty of Law - University of Trento. He teaches, among other courses, "Comparative ICT Law" and "ICT Law - Privacy and Security" and, is the author of several articles about issues related to Digital Age Law (Privacy, Data Protection, Intellectual Property Rigts, etc.). He has been collaborating for years in digital health research activities, in particular, most recently, within the "Trentino Salute 4.0 Project", a joint laboratory which involves the Autonomous Province of Trento (PAT), the Health Local Care Provider (APSS) and the Bruno Kessler Foundation (FBK).

Abstract: Ok Google, am I sick?': Artificial Intelligence, eHealth and data protection regulation

The healthcare sector has been impacted by Artificial Intelligence systems for several years. This is certainly favoured by the constant development of technologies based on sophisticated machine



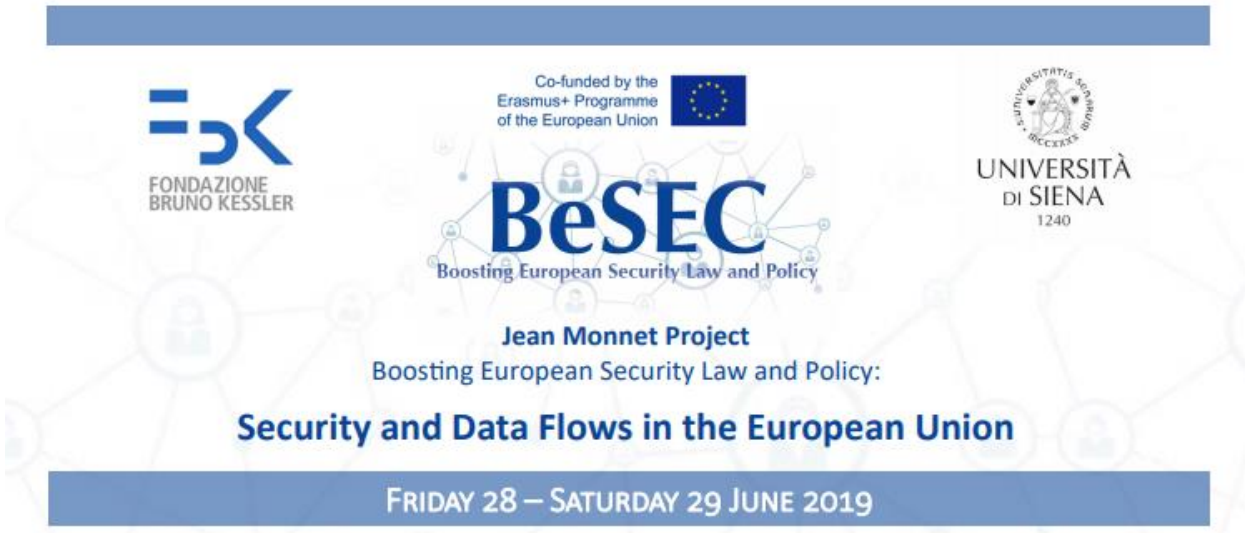
learning and techniques that are able to find complex patterns in data. However, several critical issues hinder AI's definitive affirmation: from a lack of clinical studies that can demonstrate its reliability and greater effectiveness with respect to traditional systems, to the criticalities related to the attribution of responsibility in the event of medical errors. In particular the application of data protection regulation to this specific scenario needs to be carefully evaluated. The correct management of this technology, through legal intervention in preventing possible dehumanization, plays a crucial role. This paper aims to investigate the impact of technologies based on AI in the healthcare sector, with particular attention to personal data protection issues.

ALAELDIN MAGHAIREH, Prince Mohammad Bin Fahd University

Dr. Alaeldin Maghaireh is an Assistant Professor at Prince Mohammad Bin Fahd University (PMU). Before joining PMU Dr. Maghaireh was a lecturer in Law at the Centre for Transnational Crime Prevention (CTCP) Australia. He supervised major research projects for Law Faculty/ Wollongong University and coordinated Master of Transnational Crime Prevention Tutorial Teaching Program (2010-2012). He is an expert in cyber criminology and Islamic Criminal Law with considerable experience in the First Instance Court in Jordan (1996-2000). His primary research interests are: Cyber criminology, criminal law, cyberterrorism, computer hacking, transnational organized crime and Islamic Criminal Law. He has published on cybercrime, Shariah law and related legal issues.

Abstract: Arabic muslim hackers: a digital road to paradise

Muslim hackers groups first emerged in 2003, when Arabic hackers spontaneously started creating their own websites and hacking forums mimicking more established Western hackers' websites. Cyberspace for them is a new road to God's satisfaction and Paradise. I have coined the word "HACTWER" to describe the unique and aggressive form of hackers distinguished from the well-known hackers. Hactwer is composed of the initials of the following five words: hacker, activist, criminal, terrorist, and warrior. These Muslim Arabic-background hackers continue to infiltrate computer systems to deliver a political messages; or and to seek personal and financial advantages; or and to facilitate terrorism activities or, even more dangerously, target financial services, data transmission, transportation system and critical infrastructure of other states



GIANLUIGI MARINO, Osborne Clarke

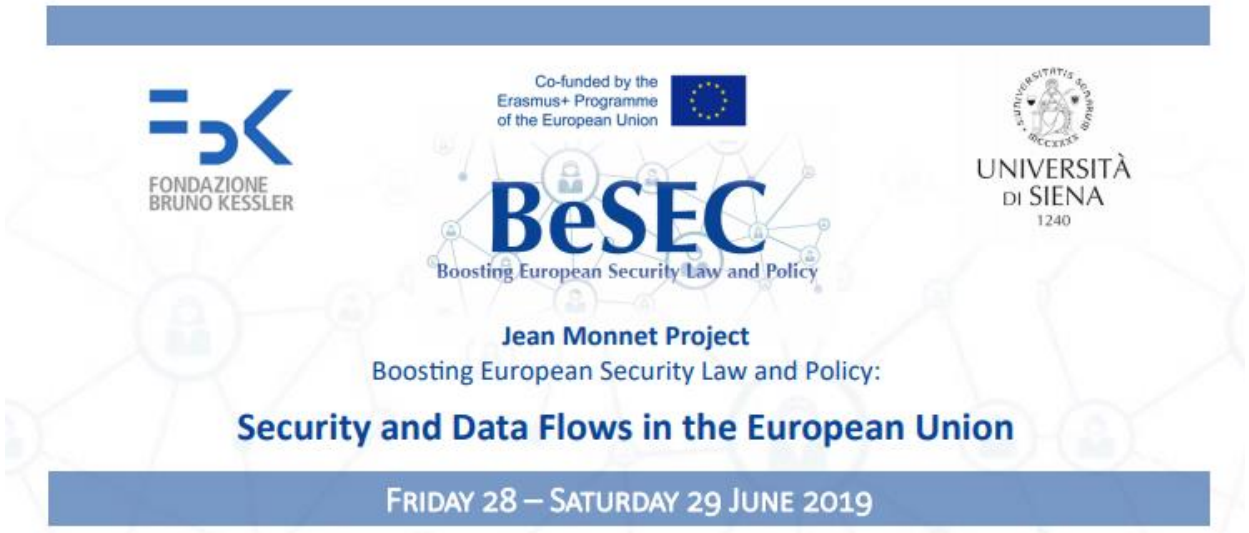
Gianluigi heads the Tech, Media and Commssector and the Data Protection practice of the international law firm Osborne Clarke, in Italy.
Gianluigi is an expert in privacy, cybersecurity and technology law. He assists clients with the digital transformation of business processes. Furthermore, he has gained substantial experience in drafting and reviewing personal data protection compliance programs and in providing assistance during and following Data Protection Authority raids. He also advises on media, online platforms law, e-commerce, consumer rights, misleading advertising, prize promotions, commercial contracts, outsourcing, internet service providers' liability, copyright and IP. Gianluigi is co-author of two textbooks on the GDPR and the Italian data protection law.

Abstract: Smart cities and data protection issues

The communities, the cities, in order to be smart need a huge amount of data to collect and process. When such information directly or indirectly refers to an individual, then data protection aspects – mainly addressed under the GDPR – should be taken into consideration. Although the data protection laws clearly identify the roles of the relevant subjects within the data processing, it is true that itis not always easy to attribute roles and responsibilities to such subjects. This is due, amongst other reasons, to the fact that there are a number of different entities active in the chain of value of the data processing in the ambit of smart cities. This has a significant impact in terms of identification of obligations and liabilities. A smart city project, maybe more than any other project, should meet the privacy by design principle in order to correctly identify the most suitable legal basis applicable to the different phases of the data processing, adequately select the dataset, establish how to inform the relevant data subjects, choose which security measures to apply, address to which extent data may be re-used and, last but not least, assess how to exploit the inferred data. Additionally, when solutions which imply decisions based solely on automated processing, the risk to disseminate cognitive biases should be addressed in order to reduce and mitigate an impact which is often hard to calculate and foresee.

GABRIELE RIZZO, Leonardo, Aerospace, Defence and Security

Professor Dr. Gabriele Rizzo, Ph.D., Currently Lead Scientist in Strategic Innovation and Principal Futurist in Leonardo, professional futurist advisor to EDA and both NATO Strategic Commands, Member at Large for Strategic Foresight and Futures Studies, and NATO expert for Cyberspace and



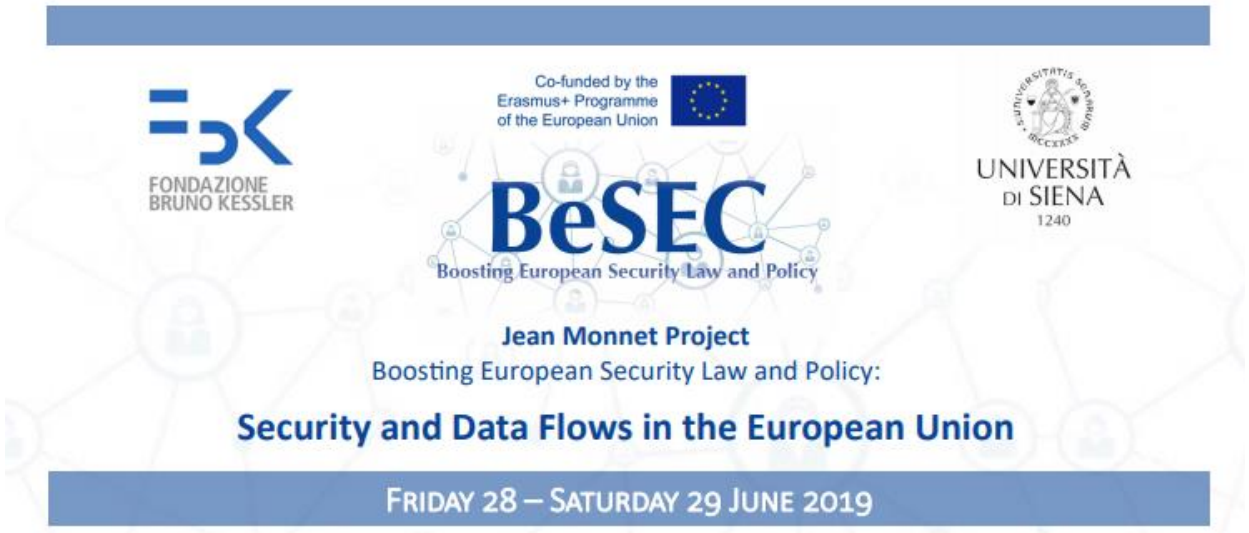
Cyber Defense. All this makes him a perfect fit both for EDA TechWatch and NATO ACT Futures Work, where he is editor and co-author of NATO Technology Trends, co-author of Strategic Foresight Analysis and Framework for Future Alliance Operations, chairman of their Technology tracks, and full contributor to Minimum Capability Requirements (Long Term Aspects and Main Shortfalls Areas), framing years 2040–2060.

Abstract: When cyberspace gets into the equation – What does it enable, what could happen and how can we prepare?

In 2016 cyberspace has been declared as a domain of operations by NATO and had thus entered the field of military thought. Cyberspace comprises the Internet, networks, systems, electromagnetic spectrum, peripherals, data, and users in the information environment: in short, cyberspace permeates everything, everywhere, in every domain. Operating in, through and on cyberspace is a vital requirement to maintain joint freedom of manoeuvre and information superiority, which are in turn crucial for the future force to gain and maintain the offset in operations.
Why tackling so directly this military angle? Much like there is no meaning for distance in cyberspace, there is no distinction between effectors: military-grade cyberattacks can and were used against citizens. It is then of extreme relevance understand the strategic military weight of cyberspace to explore in a structured way many of the consequences the very existence of cyberspace has, starting from a Defense perspective and following down to the strategic critical national infrastructures, the security forces, and the citizenship.
During this talk, after having set the scene defining the layers of cyberspace and the outline of the doctrine for cyberspace operations, we will present a threat landscape in and through cyberspace, moving to resilience and complexity. We will then glimpse to some deep future, exploring the concepts of hyperwar and its proposed response, the Centaur, concluding with a final outlook to the Imagination Age of 2040-2050 and how can we direct actions starting already today.

LUCIO SCUDIERO, Legance and Lex Digital

Lucio Scudiero is an italian qualified lawyer at Legance – Avvocati Associati; he advises clients on Data Protection, EU and Ict Law, particularly on the application of the GDPR, the ePrivacy Directive, the NIS Directive, the eIDAS Regulation and related European and national case law.
He also drafts and revises IT contracts, advising clients in the context of inspections and law enforcement operations undertaken by the Italian Data Protection Authority.
Furthermore, Lucio Scudiero has been a researcher on privacy and cybersecurity within Horizon2020 projects. He participates in conferences, workshops and courses as a speaker. He is executive director of Lex Digital.



Abstract: The protection of personal data in the performance of Energy Performance Contracts

The presentation aims to introduce some key issues related to the application of the GDPR related to the execution of Energy Performance Contracts (EPC). This type of contracts is concluded between the Public Administrations and a private partner which takes the risks to achieve the energy efficiency goals of the ECP (the ESCo – Energy Service Company); the ultimate recipients of the services provided by the ESCo are the members of the household subject to the efficiency and energy saving project. From a data protection law standpoint the execution of a EPC heavily relies on the collection of a large variety of personal data related to the tenants, such as their family status, their income and, above all, the monitoring of their consumption of energy, which can also take place by means of smart metering techniques. The GDPR applies to this setting and triggers several issues. First of all, it is necessary to allocate the privacy roles amongst the parties of an EPC.

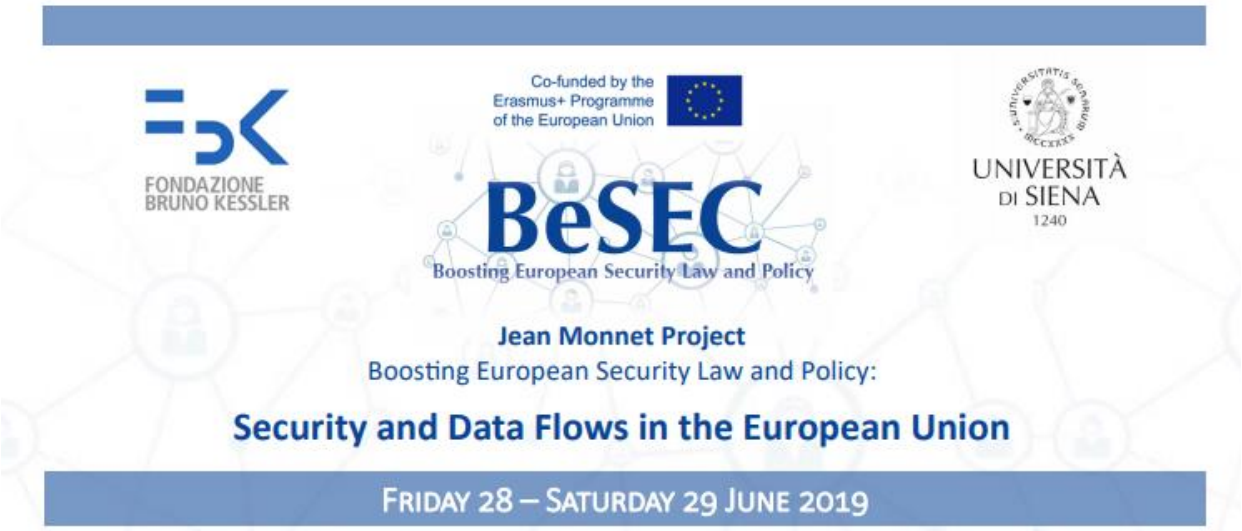
Secondly, the legal basis of the processing activities carried out may not be easy to identify: is it necessary to request the consent of the data subjects in order to profile their consumption habits? Finally, when the EPC provides for the observation of consumers' habits through the "smart meters" it seems necessary to appraise all the inherent risks for the protection of personal data of the tenants by means of a Data Protection Impact Assessment; in fact, the determination of behavioral patterns related to the tenants can lead to unwanted profiling activities.

PIERLUIGI SARTORI, Trentino Digitale

Pierluigi Sartori is the Chief Information Security Officer of Trentino Digitale SpA, a "Province of Trento" in-house company. CISSP, CISM, CGEIT, CRISC MBCI certified he developed the ISO/IEC 27001:2013 Information Security Management Sistem of Trentino Digitale. Worked for years in the field of information security, first in military sector and later in the private sector in multinational companies. Strong supporter of of the spread of "Security knowledge"; is a founding member and board member of ISC2 Italian chapter and ISACA Venice Chapter, where he also holds the role of President and CISM courses coordinator.

Abstract: Smart cities and privacy: the "balance" point

The "smart "evolution of cities makes it possible to achieve a dual objective. If, on the one hand, increase the citizen's sense of security (generally physical security), on the other, it is possible to provide several digital services to improve the user experience of who live the smart city. Smart services, in the not too distant future, will make life easier not only for residents but, for example,



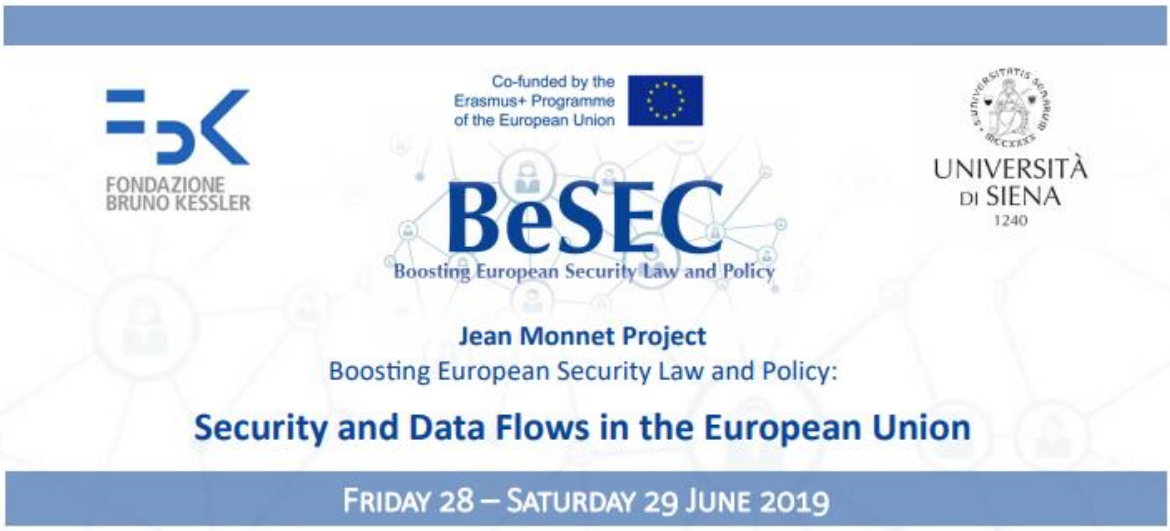
also for visitors. Having real-time information about local transport or the overcrowding of touristic point of interest allows the user a better experience. In this context, public administration plays an essential role because it has the opportunity to be closer and more visible. At the same time, however, public administration must guarantee that all personal data, collected and managed, are treated with a level of attention and transparency sufficiently high to respect and maintain user confidence. A point of attention is that the use of shared and/or open solutions needed to ensure the availability of services at a national level requires the personal data exchange between different subjects. Let's think, for example, about SPID authentication systems or electronic health records. It is essential for public administrations to guarantee that the small loss of privacy is offset by a set of services with an adequate level of security. And it is also essential to explain the pros and cons of this small loss of privacy. The only possible way to reach this goal is to adopt adequate security measures and make citizens aware of the effort being made to protect their personal data.

ELEONORA TAFURO AMBROSETTI, ISPI, Italian Institute for International Political Studies

Eleonora Tafuro Ambrosetti is a research fellow at the Russia, Caucasus and Central Asia Centre at ISPI. Prior to that, she was a Marie Curie fellow based at the Middle East Technical University (METU) in Ankara, Turkey, where she has also pursued her PhD. She has had research stays at the Saint Petersburg State University and at the London headquarters of the European Council on Foreign Relations (ECFR). She has also worked as a junior researcher at the Brussels office of the Foundation for International Relations and Foreign Dialogue (FRIDE) and at the Barcelona Centre for International Affairs (CIDOB). Eleonora's areas of interest include Russian foreign policy, EU-Russia and Russia-Turkey relations, and EU neighbourhood policies.

Abstract: The "ICT freedom VS security" dilemma: The Russian way

In an attempt to curb cybercrime or terrorist activities, governments enact laws ideally striking a balance between state security, on the one hand, and freedom of expression, privacy and other individual rights, on the other. The actual balance between the two sets of societal interests differs dramatically across different jurisdictions as it is embedded in a country's history, form of government, domestic concerns. My presentation sketches Russia's approach to the "ICT freedom vs security" dilemma. I will start with a brief overview of the factors shaping Russian approach, including the country's unique, periodically hostile relationship with Europe and the West in general, its tradition of thought about human rights, the relative weakness of the rule of law inside the country



along with an emphasis on preserving the territorial integrity of the world's largest state and fighting terrorism. I will particularly delve into the situation in the North Caucasus, Russia's troubled region that continues to struggle with sporadic acts of violence by Islamic militants, who have been skillfully mastering the chances offered by online communication and social networks. I will then mention the articles of the 1993 Russian Constitution that defend, at least on paper, freedom of expression, privacy of correspondence, and personal consent on the state's activities of data collection and storage and examine how the latest waves of legislation are diverging from the protection of those rights.

SIRIO ZOLEA, University of Macerata

Sirio Zolea has obtained an Italian and a French doctoral degree and he is currently a postdoctoral researcher in comparative law at the University of Macerata. He has published in several Italian and European law reviews about private law topics, mostly but not only concerning property. He has also worked on public law comparison, lastly speaking at the congress of the International Academy of Comparative Law, held in Fukuoka, about law in the age of populisms.

Abstract: A historical regression: from democratic and judicial control to a "Digital Police State"
*This paper has been conceived and written with Professor Vincenzo Zeno-Zencovich.

The evolution of modern States was marked, in continental Europe, by the creation (especially in Prussia and in the Austrian Empire) of the "Police State" (Polizeistaat) meant as an administrative form of Government based on the principles of hierarchy and territorial organization and subject to an embryonal rule-of-law. The use of Big Data by public authorities, profiling of individuals, algorithmic selection and decision-making, are bringing us back to the past. Especially after WWII the idea of "rule-of-law"; seemed to be inevitably linked to an ex ante judicial control over any public decision concerning individual freedoms, liberties and status. Things are radically changing -and not only in the field of national security, but in every domain of public choice -bringing to light a potential conflict between democratic values and digital societies.