Information & Security

Published since 1998

ISIJ Monitor
vol. 43, no. 3 (2019): 385-396
https://doi.org/10.11610/isij.4329

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

ISIJ Monitor

DIGILIENCE 2019 Agenda and Abstracts

The first international scientific conference "Digital Transformation, Cyber Security and Resilience" (DIGILIENCE 2019) will take place in the Central Military Club in Sofia, the capital of Bulgaria. Here the reader can find the agenda by thematic sessions, with abstracts of the papers that do not appear in this volume. Minor changes in the agenda are possible, and the readers are invited to check current status at http://digilience.org/thematic-sessions.

2 October 2019

The Leadership Perspective

(Opening Plenary Session)

Acad. Yulian Revalski, President of the Bulgarian Academy of Sciences

HE Atanas Zapryanov, Deputy Minister, Ministry of Defence, Republic of Bulgaria

Karina Angelieva, Deputy Minister, Ministry of Educaition and Science, Republic of Bulgaria

Dr. Velizar Shalamanov, Chairperson, NATO Communications and Information Organisation (NCIO) Agency Supervisory Board

Konstantin Zografov, AFCEA Regional Vice President of South East Europe and President of the AFCEA-Sofia Chapter

Plenary Session I

Prof. Siraj Ahmed Shaikh, Coventry University, UK, *Cyber-Physical Systems Security: Research Challenges and Opportunities*

> Prof. Shaikh will provide a brief overview of some of the challenges in defending cyber-physical systems, and then run through some key areas of development in this domain. He will dive into some technical areas to reflect on research results of the Systems Security Group at the Institute of Future Transport and Cities (FTC) at Coventry University, including areas of design, policy and behaviour, alongside engineering.

Todor Tagarev, George Sharkov, Nikolai Stoianov, Velizar Shalamanov, *Network-based Steering of Bulgaria's Cybersecurity Research*

The increasing reliance of economies, public administrations, military and security services, and our everyday activities on advanced information and communication technologies brings benefits, as well as vulnerabilities. Providing security of ICT infrastructures and protection of essential services against cyberattacks is becoming increasingly important. Several countries already have dedicated cybersecurity research programs. Bulgaria is not among those countries, notwithstanding the grave problems it faces, as emphasized by the recent leakage from the National Revenue Service exposing the personal data of almost all tax-paying citizens. The authors therefore have developed and present a concept allowing to combine top-down programs and financing, which occasionally include cybersecurity-related themes, with bottom-up initiatives and use of variety of instruments to advance the national cybersecurity competences.

Information Sharing and Situational Awareness

(Parallel Session, Track 1)

Vesselin Bontchev and Veneta Yosifova, *Analysis of the Global Attack Landscape Using Data from a Telnet Honeypot*

See pp. 264-282 in this volume.

Jyri Rajamäki, Ilkka Tikanmäki and Jari Räsänen, *CISE as a Tool for Sharing Sensitive Cyber Information in Maritime Domain*

See pp. 215-2235.

Ivelina Vardeva

Generalized Net Model of an Automated System for Monitoring, Analysing and Managing Events Related to Information Security

See pp. 257-263 in this volume.

Veneta Yosifova and Vesselin Bontchev, *Possible Instant Messaging Malware Attack Using Right-to-Left Unicode Overriding Characters*

The right-to-left special Unicode character has a legitimate use for languages that are transcribed in a right-to-left direction or in an environment that combines both right-to-left and left-to-right languages, like web pages, emails, desktop documents and text messages. These writing systems include right-to-left languages such as Persian, Arabic and Hebrew. The "right-to-left" attacks have been used for many years for malicious purposes, mostly in email communications. Early in 2018, Kaspersky Lab published an article described a vulnerability in the Windows client of the popular instant messenger Telegram. This vulnerability uses the Unicode "right-to-left" character to obfuscate the name of the malware file. This paper describes a possible attack that we discovered. It uses a combination of the "right-to-left" override attack and instant messaging malware attack and presents a realistic threat for another widely used messenger - Microsoft's Skype for Linux. The purpose for conducting this research was to describe an exploit that we discovered and to warn the people who use this communication application about it, as well as to appeal to the producer for fixing it. Additionally, it is important to emphasize that the attack scenario developed by us also impacts other applications that allow file transfer (e.g., e-mail clients) and run on Linux systems with Wine installed.

Jussi Simola, *Comparative Research of Cybersecurity Information Sharing Models: The Common Cyber Ecosystem of ECHO*

See pp. 175-195 in this volume.

Jouni Pöyhönen, Viivi Nuojua, Jyri Rajamäki, and Martti Lehto, *Cyber Situational Awareness and Information Sharing in Critical Infrastructure Organizations*

See pp. 236-256 in this volume.

Vesselin Bontchev

A VBA P-Code Disassembler

Recently, we have observed a significant increase in the frequency with which Microsoft Office macros are being used as an attack vector. Microsoft Office uses a macro programming language called Visual Basic for Applications (VBA), which is powerful enough to do whatever the attacker needs. Usually, the malicious VBA macros are used to download the second stage of the malware (ransomware, banking Trojan, backdoor, etc.). They can be relatively small and are easy to modify or even to completely rewrite them each time, thus making them difficult to detect at the perimeter defences (e.g., with an e-mail scanner) with known-malware detection tools.

So far, we have seen malicious VBA macros being distributed with Microsoft Word, Excel, PowerPoint, Access, Visio, Project and Publisher documents. Microsoft Office has built-in protections against execution of foreign macros, but unless properly administered, they are easy for the user to disable and the malicious documents usually use some form of social engineering to convince the user to do so. Therefore, we need proper tools for inspecting the macro content of the received documents, in order to decide whether it contains any malicious code. During our research we have discovered that the publicly available tools lack the capability to discover all forms in which a malicious macro can exist. We have applied our findings from reverse-engineering the formats of Microsoft Office documents and have created a tool, which allows disassembling of the p-code into which VBA is compiled.

Human-centric Cyber Security and Resilience

(Parallel Session, Track 2)

Yantsislav Yanakiev and Dimitrina Polimirova, *The Role of the Human Factor in Cyber Security: Results from an Expert Survey in Bulgaria*

While technological solutions are being developed to enhance cyber security, there is increasing awareness that besides a technical approach the role of human performance, decision making and organizational culture are critical to increase the effectiveness of responses to evolving cyber threats. Hence, the focus of this paper is on the role of the human factors in cyber security. It presents an analysis of data from a Subject Matter Experts' study carried out in Bulgaria in the end of 2018 in the framework of the project "Cyber security and opportunities for application of innovative technologies in the state administration of the Republic of Bulgaria." The data was collected via online survey from 92 experts from the state administration, academia and business organizations.

The paper covers the following topics: 1) The most important issues in cyber security in Bulgaria and the role of the human factors among them; 2) Recruitment, Retention, Education & Training of IT personnel; 3) The human factors as a source of security breaches; and 4) Future research in the area of human factors in cyber security. Based on the analysis of the data, conclusions and recommendations are summarized regarding the ways to change the role of the human factor from the system's "weakest link" to a powerful resource to detect and mitigate cyber threats.

Venelin Georgiev, *Profiling Human Roles in Cybercrime*

See pp. 145-160 in this volume.

Valerii P. Mygal and Galina V. Mygal, *Problems of Digitized Information Flow Analysis: Cognitive Aspects*

See pp. 134-144 in this volume.

Jassim Happa, *Resilience from Self-Discrepancy Theory*

Threats take many forms, and reasoning about them to make organisations more resilient remains challenging given their, often, qualitative nature. Many resilience management models and standards exist. They help enterprises recover from harmful incidents. No approach today examines views that contribute to resilience concerns from multiple perspectives. In this paper, I argue it is necessary to consider a much broader spectrum of threats and harms in order to better understand the complex dependencies and interactions between an enterprise ('self') and the environment ('world'). This paper adapts the Self-Discrepancy Theory from psychology to help establish and reason about multiple views of the enterprise: the actual, ideal and ought enterprise, as viewed by the self and others. The paper also explores how changes in priorities and operations might affect the self (again, as seen by the self and others). This framework does not compete with existing models and standards. Instead, the purpose is to complement them by exhaustively creating different perspectives (views) of enterprises with the aim to re-contextualise resilience concerns. By using this framework, risk-owners can start asking questions that are analogous to: "what would my opponent do in my shoes?" or, "if I change my enterprise's operations, what effect might this have on my security (or vice versa)?" Viewing enterprises and their resilience from different perspectives is an underexplored topic in research, and is a key motivator behind this article. This paper acts as a positional paper, and further studies will be necessary to provide empirical evidence that shows that this approach is feasible in real-world settings.

Kirsi Aaltola and Petteri Taitto, *Utilising Experiential and Organizational Learning Theories to Improve Human Performance in Cyber Training*

See pp. 123-133 in this volume.

Silvia Matern, *e-Platform Architecture for Organisational Collaboration and IT Education*

See pp. 161-172 in this volume.

Yavor Papazov, George Sharkov, Georgi Koykov and Christina Todorova, *Managing Cyber Education Environments with Serverless Computing*

This paper presents the experience of the authors in their efforts to apply an innovative computation paradigm – "serverless" computing – into managing cyber education environments through the Course Manager platform, developed by the authors' team. The serverless paradigm, also referred to as Function-as-a-Service (FaaS), helps the developers abstract or automate away almost all infrastructure and operation overhead, allowing for what is often touted as "infinite scaling" applications, which can be a good fit for the rapidly increasing demand for practical cyber environments.

The authors provide an in-depth overview of the architecture and frontend of a cyber education environment management framework, designed to work in a serverless environment, and analyse the lessons learnt from using that framework in providing cyber trainings to students and IT professionals for more than a year.

3 October 2019

Plenary Session II

Lynne Charles, Deputy Head of Mission, British Embassy Sofia

Salvador Llopis Sanchez, European Defence Agency, *The Future of Command and Control Systems*

Kalina Bontcheva, The University of Sheffield, UK, *Assistive AI Tools for Analysing False Content, Disinformation Flows, and Online Influence Campaigns*

Georgios Chatzichristos, ENISA, *Putting AI into the EU Cyber Crisis Collaboration*

Artificial Intelligence (AI) is not something new. What is new is the pace within which information is disseminated in today's society and the amount of data produced that renders the use of advanced technologies like AI essential for organisations. AI systems have the potential to create competitive advantage and have been adopted by organisations both in operational and technical levels. Such systems are utilised to provide intelligence on the services which organisations offer, to distinguish behavioural aspects of systems and networks, and to help humans understand complex relationships between different entities of their working environment. In cybersecurity, AI systems have the ability to highlight anomalies on network traffic identifying invisible "unknown unknown things" in the systems, but also as an efficient classifier of vast amounts of data like in the case of threat intelligence.

In the EU cyber crisis cooperation context, most commonly referred as 'the Blueprint', AI uses are just beginning to emerge, mainly at the Open Source intelligence domain. The need for situational awareness, one of the Blueprint's main pillars, has driven ENISA to initiate the development of a project under the name 'Open Cyber Situational Awareness Machine – OpenCSAM) that attempts to address the need for accurate aggregation of relevant information and reporting. The project is using supervised learning and natural language processing to facilitate incident responders at all levels of administration in the drafting of situational awareness reports for the Blueprint.

Emerging Methods for Cyber Security and Resilience: AI, Blockchain, Fuzzy Sets

(Parallel Session, Track 1)

Notis Mengidis, Theodora Tsikrika, Stefanos Vrochidis and Yiannis Kompatsiaris, *Blockchain and AI for the Next Generation Energy Grids: Cybersecurity Challenges and Opportunities*

See pp. 21-33 in this volume.

George Sharkov, *Cyber Resilience of Systems-of-Intelligent-Systems*

Michal Turcanik and Martin Javurek, *Cryptographic Key Generation by Genetic Algorithms*

See pp. 54-61 in this volume.

Boris Bozveliev, Sotir Sotirov and Tihomir Videv, *Generalized Net Model of Possible Drone's Communication Control Cyber Theft with Intuitionistic Fuzzy Estimations*

See pp. 35-4 in this volume.

Tihomir Videv, Boris Bozveliev and Sotir Sotirov, *Modelling of Smart Home Cyber System with Intuitionistic Fuzzy Estimation*

See pp. 45-53 in this volume.

Marcin Niemiec, Andrzej Dziech, Miłosz Stypiński and Jan Derkacz, *Quantum-based Solutions for the Next-generation Internet*

See pp. 62-72 in this volume.

Neil Farrugia and Joseph G. Vella, *Automating Footwear Impressions Retrieval through Texture*

See pp. 73-86 in this volume.

Oleksandr Letychevskyi, *Algebraic Approach in Cyber Security*

The algebraic approach in cyber-security implies the usage of a symbolic model and applying formal methods that realize symbolic execution, proving the properties and verification of safety and security issues. It uses the behaviour algebra that is applied for the formalization of analysed object and translation of an object given as binary code or hardware specifications to behavioural algebra specifications. It provides also detection of vulnerabilities or possible hardware failures by static analysis or conducting symbolic modelling and using algebraic matching. The given technique was applied for the detection of vulnerabilities in binary code given as a set of Intel x86 instructions. It was implemented in the scope of GARUDA.AI modelling platform and algebraic modelling system on the set of known vulnerabilities from the CVE database and the known hardware failures.

Sean Costigan and Greg Gleason, *What If Blockchain Cannot Be Blocked? Cryptocurrency and International Security*

See pp. 13-20 in this volume.

Cyber, Hybrid Influence and the Role of Social Networks

(Parallel Session, Track 2)

Diego Fregolent Mendes de Oliveira and Kevin S. Chan, *Diffusion of Information in an Online Social Network with Limited Attention*

See pp. 362-374 in this volume.

Maksym Shchoholiev and Violeta Tretynyk, *The System of Operative Determination of the Level of Tension in Society Based on Data from Social Networks*

See pp. 375-382 in this volume.

Ralitsa Kovacheva, *Hybrid Threats in Bulgarian Media*

See pp. 333-348 in this volume.

Oleh Andriichuk, Vitaliy Tsyganok, Dmitry Lande, Oleg Chertov and Yaroslava Porplenko, *Usage of Decision Support Systems for Modeling of Conflicts during Recognition of Information Operations*

This paper presents the application of decision support systems to conflict modelling for identification of information operations. An information operation is treated as a complex weakly structured system. We present a model of conflict between two subjects, based on the second-order reflexive model, and a method for construction of the design pattern for knowledge bases of decision support systems. On that basis we suggest also a methodology allowing to use decision support systems for modelling of conflicts during information operations recognition. The methodology combines the use of expert knowledge and content monitoring data.

Yavor Raychev, *Cyberwar in Russian and US Military-Political Thought: A Comparative View*

See pp. 349-361 in this volume.

Todor Tagarev, *Understanding Hybrid Influence: Emerging Analysis Frameworks*

Over centuries countries and alliances in conflict have used all available means at their disposal, in addition to military forces, to gain a competitive edge. ‘Hybrid threat’ or ‘hybrid war’ is a new term designating the coordinated use of military and non-military means, that got traction in the analysis of the 2006 Israel-Hezbollah War and became widely used beyond the professional communities after the 2014 annexation of Crimea by the Russian Federation. One specific aspect of such conflicts is the lack of a clear distinction between 'war' and 'peace,' when a skilful player would apply available means to subjugate the opponent's will, and thus achieve its political objectives, without fighting. Economic leverage, energy dependencies, ideology, propaganda and disinformation, cyberattacks and corruption are just a few types of means for such diverse—or 'hybrid'—influence. While using different channels, it is their combined impact that can bring desired effects.

Finding an appropriate response to such hybrid influence requires a good understanding of own vulnerabilities, exposure and actual or potential impact over the public institutions, the economy and the society. This paper looks into emerging frameworks allowing to estimate the impact of hybrid influence and the extent to which they may be used to reflect the actual interdependencies and complexity of modern societies. While combining in various ways empirical data and expert assessments, all these frameworks facilitate the application of risk-aware allocation of limited resources to counter hybrid influence.

Policies and Solutions for Industry and Critical Infrastructure Protection

(Parallel Session, Track 1)

Walter Matta and Alessandro Cantelli-Forti, *An innovative Airport Physical-cyber Security System (APSS)*

See pp. 285-293 in this volume.

Sergiy Dotsenko, Oleg Illiashenko, Sergii Kamenskyi and Vyacheslav Kharchenko, *Integrated Security Management System for Enterprises in Industry 4.0*

See pp. 294-304 in this volume.

Sergiy Dotsenko, Oleg Illiashenko, Sergii Kamenskyi and Vyacheslav Kharchenko, *Integrated Model of Knowledge Management for Security of Information Technologies: Standards ISO/IEC 15408 and ISO/IEC 18045*

See pp. 305-317 in this volume.

Dafina Zoteva, Peter Vassilev, Lyudmila Todorova, Krassimir Atanassov, Lyubka Doukovska and Valery Tzanov, *Generalized Net Model of Cyber-control of the Firm's Dumpers and Crushers*

The paper presents generalized net model of a system for tracking and monitoring the movement and actions of a rm's dumpers and crushers. The model permits analysis regarding possible cyber manipulation of data, and highlights the key vulnerabilities of such systems.

Volodymyr Zaslavskyi and Maya Pasichna, *System Approach Towards the Creation of Secure and Resilient Information Technologies in the Energy Sector*

See pp. 318-330 in this volume.

Effective, Efficient and Cyber Resilient Organizations and Operations

(Parallel Session, Track 2)

Nikola Saranov, *Cooperation Model for Establishing Secure Digital Transformation in Corporations: Overview of Regulatory Issues*

See pp. 98-112 in this volume.

Velizar Shalamanov, Silvia Matern and Georgi Penchev, *Digitalization and Cyber Resilience Model for the Bulgarian Academy of Sciences*

This paper presents a concept for digital transformation of the Bulgarian Academy of Sciences – a national academic institution for both fundamental and applied research and education. It looks into four areas – project management; services; funding; and people to develop, operate and protect ICT infrastructure and applications. It explores options for these four areas, suggests an approach to select the most suitable ones, and the way of their integration through effective system for governance and management in the specific environment.

Latinka Todoranova and Bonimir Penchev, *Perspectives for Mobile Learning in Higher Education in Bulgaria*

The use of mobile technologies in education enables the access to and the implementation of modern teaching methods and tools. Nowadays, higher education faces a number of different challenges. Not only the technologies are developing at an extremely fast pace, but also the generations are changing – children are growing up in an environment where they are surrounded by different technological gadgets. These gadgets influence children’s communication, their access to information and also their learning habits. Upon entering the university, the learners continue to use their mobile phones for information exchange and communication. In response, higher education is trying to change in that direction. But it seems that the steps the higher education is taking are not fast enough to meet the expectations of the modern young people. The purpose of the research article is to define the problems and to outline the perspectives for mobile learning in higher education in Bulgaria.

Rositsa Velichkova, Iskra Simova and Stelian Dimitrov, *Impact of Climate Change on the Floods in Bulgaria*

In the Republic of Bulgaria, floods caused by natural phenomena or human activity may have adverse effects. Therefore, reducing the risk of disasters is of primary importance for the sustainable development of the country. The impact of climate change is expected to rise in the coming decades and to lead to increase in the frequency and magnitude of disasters. More frequent and stronger storms and floods, as well as long-lasting droughts and devastation forest fires can have particularly harmful effect on existing opportunities for society after such dangerous events. For this reason, and because of the complexity and extent of the disasters, unification of the efforts of all responsible institutions and their active inclusion in disaster risk reduction activities is necessary. These measures are expected to lead to a significant reduction in human, social, economic and natural damage and losses. This paper presents a descriptive analysis of the floods in Bulgaria for the time period 2010 – 2017. The study is based on precipitation in Bulgaria reflecting climate change. Existing statistical data is reviewed and analyzed and, based on that, recommendations are formulated.

Toddor Velev and Nina Dobrinkova, *The Logical Model of Unified, Innovative Platform for Automation and Management of Standards (PAMS)*

See pp. 113-120 in this volume.

Radka Nacheva and Snezhana Sulova, *Research on the Overall Attitude Towards Mobile Learning in Social Media: Emotions Mining Approach*

In this paper, we address the importance of classification and social media mining of human emotions. We compared different theories about basic emotions and the application of emotion theory in practice. Based on Plutchik's classification, we suggest creating a specialized lexicon with terms and phrases to identify emotions for research of general attitudes towards mobile learning in social media. The approach can also be applied to other areas of scientific knowledge that aim to explore the emotional attitudes of users in social media. It is based on the Natural Language Processing and more specifically uses text mining classification algorithms. For test purposes, we have retrieved a number of tweets on users' attitudes towards mobile learning.

Rositsa Velichkova and Iskra Simova, *Wildland Fire Suppression Measures with Water Resources from Nature*

Wildland fires occur and spread more often in hard-to-reach areas, quickly covering big territories due to the presence of combustible materials in the understory along with favorable meteorological conditions. The occurrence of fires is mainly due to two factors - human activities and natural phenomena. The subject of the current research paper does not focus on these factors, but on the idea of using the natural resources on fire-affected terrain. Fire suppression measures are primarily done with water and, in very rare cases, with chemicals. In these cases, the provision of sufficient sources of water in the vicinity of the burning terrain is crucial. That is why analysis of the terrain with its hydrological characteristics - the flow in time, especially in the driest months of the year, is required. This assumption is used as base and illustrated with a specific example of a geographically defined area, serving as a proof for the proposed idea.

4 October 2019

Research-based Innovation in Cyber Security and Resilience

Jyri Rajamäki, *Design Science Research towards Privacy by Design in Maritime Surveillance ICT Systems*

See pp. 196-214 in this volume.

Todor Tagarev and Nikolai Stoianov, *Scoping the Scenario Space for Multi-sector Cybersecurity Analysi*

The paper presents results from the ECHO project, supporting the identification and development of cyberattack scenarios. It explores the scenario space along four dimensions: (1) critical infrastructures and essential services, critically dependent on the ICT infrastructure; (2) types of malicious actors and their capabilities; (3) exploited vulnerabilities; and (4) short- vs longer term horizon. The exploration serves to span comprehensively the scenario space. The authors present the list of selected scenarios, storylines, and use cases, that are used in follow-up research to define key components of the capability requirements: technology roadmaps, cyber skills framework, information exchange and certification requirements.

Tobias Fiebig, *Governance Challenges for European CyberSecurity Policies: Stakeholders Views*

The author outlines possible approaches to cybersecurity governance and compares them against the EU proposal of a Network of Competence Centres, which should manage all European cybersecurity funding. He then presents results of testing this policy proposal against the opinions of key stakeholders (senior administrators from European Agencies, Data Protection Authorities, CISOs, managers, and academics) from the European economic area.

The presentation reflects results of the from the CyberSec4Europe project – one of the four pilot projects aiming to establish and operate a pilot for a European Cybersecurity Competence Network and develop a common European Cybersecurity Research & Innovation Roadmap.

Velizar Shalamanov and Georgi Penchev, *Methodology for Organizational Design of Cyber Research Networks*

The paper presents possible approaches for building a new network organization in the area of cybersecurity. The study is focused on selection of activities, processes and structures needed for the network governance and management. The study considers links between Enterprise Architecture approach, COBIT framework and network analysis with the task to elaborate a standard and comprehensive framework for analysis of IT related areas of organizational governance and management. Examples of NATO and EU initiatives for network organization design and implementation are explored with specific focus on ECHO project. Accreditation procedure based on participant's self-assessment is presented.

Zlatogor Minchev, *Research-focused Cyber Exercises: National State-of-the-Art Academic Experience and Perspectives*

The paper presents a practical approach for education and training, based on computer assisted, research-focused exercises in mixed cyber-physical realities. A respective solution has been developed in the last several years, encompassing academic research and training experience both at national and international level as a tool for verification of future cybersecurity transcedents. Special emphasis is placed on the polygon design and implementation, and user feedback from the usage for multimodal and multicriteria assessment of training effectiveness. Finally, the paper out-

lines some future trends towards extending mixed realities, advancing user monitoring and more effective and efficient training.

Borislav Sestrimski, *Study on the Level of Cybersecurity and the Mechanisms for Citizens' Contribution to Preventive Policies*

The report presents the outline of national project aiming to deliver analysis of Bulgaria's bodies responsible for cyber security at the national level, the features and capabilities of the law structures in the management of cyber incidents and to elaborate and test ideas on the role of the private sector and citizens in policy-making and mechanisms for international cooperation on cyber incidents at national level. The final goal is to recommend best practices for citizens' participation in providing cybersecurity. The author will briefly present other projects and their involvement, including CyberSec4Europe, one of the four EU pilot projects launched to prepare the European Cybersecurity Competence Network.

Vanina Pencheva and Hristina Georgieva, *Bridging the Gap between Research, Innovation and Standardization: The contribution of BRIDGIT2 Project*

The team of the BRIDGIT2 project has collected compelling evidence that standardization facilitates the market uptake of outcomes from H2020 and earlier framework programs and seeks for the research and innovation community to fully engage with standardization. It builds on the BRIDGIT project, which promoted the interaction between research and standardization and strengthened the capabilities of members of standardization bodies to become partners in research and innovation projects.

Nina Dobrinkova, *Innovation for Crisis Management: DRIVER+ and the Crisis Management Innovation Network Europe*

Launched in May 2014, the DRIVER+ (Driving Innovation in Crisis Management for European Resilience) project aims to cope with current and future challenges, due to increasingly severe consequences of natural disasters and terrorist threats, by the development and uptake of innovative solutions that are addressing the operational needs of practitioners dealing with Crisis Management. In a series of for trials, DRIVER+ demonstrated the benefits and enhanced the Trial Guidance Methodology (TGM), the Portfolio of Solutions (POS), and contributed to the shared understanding in Crisis Management across Europe, through the enhancement of the cooperation framework.

The Crisis Management Innovation Network Europe (CMINE) plays an important role for the latter and contributes to the uptake of project results. We will present CMINE and its task groups with a focus on the group dealing with wildfires.

Rosen Iliev and Kristina Ignatova, *Implementation of Cloud Technologies for Building Data Centres in Defence and Security*

See pp. 89-97 in this volume.

Preliminary Summary and Future Steps