EUROPEAN COMMISSION
JOINT RESEARCH CENTRE

Information Note

JRC activities in the field of

Cybersecurity

Date: 28 January, 2016

JRC activities in the field of Cybersecurity

1. Societal and political context

Given the development of threats to cybersecurity and cybercrime in recent years, the Commission has designed a coordinated policy in close cooperation with Member States and the other EU institutions, as well as with the industry and relevant stakeholders.

The EU Cybersecurity Strategy, adopted in 2013, sets out five strategic priorities, which cover challenges that have both an EU-internal and an international dimension. Of direct relevance to the Digital Single Market (DSM) are the priorities aiming to raise the level of protection and resilience of European networks, to step up the response to online criminal threats, to develop industrial and technological resources for cybersecurity, and to enhance the level of cyber-security and privacy in the digital life of the citizen.

The Commission also proposed a Directive on Network and Information Security (NIS), which aims at strengthening preparedness, cross-border cooperation and information exchange amongst EU actors in important segments of the public and private sector, in order to better address and respond to cybersecurity incidents.

Moreover, a public-private forum on network and information security ('NIS Platform') was set up under the EU Cybersecurity Strategy with the aim of identifying good practices that organisations, across the value chain, can follow in order to tackle cybersecurity risks. A special focus of the Platform is to help SMEs tackle such risks. Activities on network and information security are supported by the European Network and Information Security Agency (ENISA), as well as by the Computer Emergency Response Team for the EU institutions (CERT-EU).

Reinforcing trust and security in digital services and in the handling of personal data is one of the objectives stated in the European Digital Single Market Strategy (DSM) published in May 2015. The strategy includes the intention of the European Commission to establish a Public-Private Partnership on cybersecurity in the area of technologies and solutions for online network security, in the course of 2016.

2. JRC activities

What is the issue to be addressed?

The EU Cybersecurity Strategy, adopted in 2013, sets out ways to strengthen network and information security across the EU. It protects the public and private sectors from intrusion and fraud, by strengthening cross-border cooperation and information exchange.

Since the launch of the Strategy, the European Commission has stepped up its efforts to better protect Europeans online, including the adoption of different legislative proposals and investing significantly in research and innovation.

What are the challenges (scientific or regulatory or both)?

The occurrence of cybersecurity incidents is growing rapidly. Such incidents could disrupt the supply of essential services we take for granted, such as, water, healthcare, electricity, transport or mobile services. Threats can have different origins – including criminal, politically motivated, terrorist or state-sponsored attacks as well as natural disasters and unintentional mistakes. As far as cybercrime is concerned, trends suggest considerable increases in scope, sophistication, number and types of attacks, number of victims and economic damage.

The DSM strategy identifies the reinforcement of trust and security in digital services and in the handling of personal data, as a key pillar of an economically viable and strong DSM.

Who are the customers?

DG JRC, is supporting work on digital trust and security for a wide group of policy DGs active in the topic of cybersecurity, including, CNECT, DIGIT, HOME, JUST, MOVE, TAXUD, ECFIN, ENER, HR and EEAS.

How is JRC contributing to address those challenges and with which tools?

In support of the Digital Single Market Agenda, DG JRC and DG CNECT have agreed to collaborate on the following initiatives:

- Establishment of a **cybersecurity contractual Public-Private Partnership (PPP),** with the definition of specific measures targeting the cybersecurity industry, to be included in the forthcoming mid-year 2016 Policy Package, covering cybersecurity standardisation, security compliance, conformity, labelling and identification and mitigation of zero-day vulnerabilities. The JRC actively participates to standardisation and technological harmonisation initiatives including cybersecurity aspects (*e.g.,* Best Available Techniques for the cybersecurity of smart-metering systems, the European Telecommunications Standards Institute (ETSI) cyber-security and "quantum safe cryptography" working groups *etc*.). JRC thus supports DG-CNECT in the identification of gaps in cybersecurity standards in the DSM and provides scientific-based policy options to support the harmonisation of the certification and standardisation of the cybersecurity industry and of the digital services and e-government platforms.

- **Review of the e-Privacy Directive, with its work on cyber-security and privacy of mobile devices and telecommunication services**, including digital platform tracking technologies and targeted adware. The JRC has considerable experience in online personal data handling, protection and privacy and has ongoing research activities on end-to-end privacy and secure online personal spaces, smart-phone ecosystems cybersecurity, malware and botnet analysis and network cybersecurity. JRC has successfully supported other DGs (*e.g.* DG-ENER) in the identification of policy mechanisms used to enhance the level of privacy in digital services (*e.g.* Data Protection Impact Assessment for the Energy smart-grid). The experience in this field will serve to provide advice in support of the revision of the e-Privacy Directive (foreseen by the DSM strategy roadmap), producing technological studies and scientifically based policy options to mitigate the cybersecurity and privacy threats of the mobile DSM and of terminal services, addressing also the aspects related to the digital platform tracking technologies and targeted adware.

In support of the EU Cybersecurity Strategy, DG JRC is contributing to the following priorities:

- **Fight against cybercrime**, with its collaboration with EUROPOL European Cybercrime Centre and National Law Enforcement Authorities, on the assessment of Best Available Techniques for targeted interception, contextualized decryption, fight against botnets and malwares, forensic tools and image analytics for the fight against child sexual exploitation. These activities include: analysis of the specific requirements of law enforcement, assessment of threats, mitigation measures and forensic techniques, development of prototypes, training of end-users, validation of prototypes with law enforcers, preparation of guidelines.

- **Achieving cyber-resilience**, with its activities carried out in close coordination with Member States authorities and critical infrastructure owners and operators, on identifying NIS vulnerabilities of European critical infrastructure and encouraging the development of resilient systems as well as with its support to the preparation and assessment, together with ENISA, of pan-European cyber incident exercises.

In support to the **EU Internal Security Agenda**, the JRC is collaborating with DG HOME on:

- Revision of the Decision 2001/413/JHA on **Combating Fraud and Counterfeiting of Non-cash means of Payment**, in particular with an evaluation of the vulnerabilities of new technologies used for non-cash means of payment (*e.g.,* virtual currencies).

In the **Energy Sector**, DG JRC is collaborating with DG ENER, on the following:

- Identification of Best Available Techniques for the implementation of the minimum **cybersecurity and privacy requirement for smart-metering systems** (implementing Recommendation 148(2012));
- Preparation of the forthcoming **EU Energy Cybersecurity Strategy**, foreseen by mid-year 2016, as part of the *ad-hoc* Expert Panel set-up for this task.

In the **Transport Sector**, DG JRC is collaborating with DG MOVE, on the following:

- **Cooperative Intelligent Transport System** (ITS), in the context of the C-ITS platform and forthcoming Masterplan, with its expertise in cybersecurity and privacy;
- **Digital Tachograph**, with the preparation of the technical specifications, including security mechanisms of the new smart tachograph.

Major international issues / cooperation?

In 2014, DG JRC established the Incident and Threat Information Sharing EU-Centre (ITIS-EUC, http://it is.jrc.ec.europa.eu) supporting DG ENER, to leverage open source intelligence for the identification of cyber vulnerabilities of industrial control systems for the energy sector (Gas, electricity, oil). Through its network of experts, the JRC is monitoring and collecting open source information on such vulnerabilities, analysing the information and providing summary reports to energy operators in the EU through its portal, twice per month. This information is stored in the online database of the ITIS-EUC portal for future use and reference. In addition, ITIS-EUC produces reports on cyber threats/vulnerabilities trends in Industrial Control Systems

(ICS) twice a year and also produces strategic guidance reports for further research in the field, thus constituting a unique body of knowledge in the Commission in this field.

EEAS has also recently stressed the growing issue of hybrid threats and hybrid warfare, blurring civilian and military domains and techniques, now extending into the cyberspace, the atmospheric space and military threats from sea-based cyber operations, conducted aboard naval vessels, against a coastal state.

What are the competences and facilities of the JRC?

JRC/ERNCIP's (European Reference Network for Critical Infrastructure Protection) Thematic Group (TG) on Cybersecurity of Industrial Automation and Control Systems (IACS) published its report on "Proposals for a European IACS Components Cyber-security Compliance and Certification Scheme". It now moves into the second phase of extracting good practices from designated existing standards and organising these into a common classification system covering an agreed set of domains of a Compliance & Certification scheme. These domains include, the definition of targets of evaluation, cybersecurity engineering domains and practices, vulnerabilities assessment, development process assessment, cyber robustness testing.

DG JRC's Experimental Platform for Internet Contingencies (EPIC) has been developed to assess the security, stability and resilience of cyber-physical systems, such as those found in Critical Infrastructures. The platform supports the execution of repeatable experiments in a fully controllable experimentation environment. It can efficiently recreate realistic network topologies and conditions, *e.g.,* the delay and loss characteristics of wide-area network (WAN) links of the Internet infrastructure. It has the operational capability to recreate in a controllable manner a wide range of disruptions, *e.g.,* host and link failures, Border Gateway Protocol (BGB) hijacking or Distributed Denial of Service (DDoS) attacks. EPIC could support CNECT's NIS strategy by carrying out specific studies and tests.

The JRC is chairing an Expert Group of the Smart Grid Task Force set up by DG ENER which aims at developing a Data Protection Impact Assessment template to be used for smart metering systems. The second objective of this group is to identify Best Available Techniques for the ten minimum functional requirements defined by the Commission's recommendation on the preparation for the roll out of a smart metering system. This tool will contribute to the overall risk management effort of this sector and will therefore improve the cybersecurity level of the smart grid environment.

The JRC has laboratories and equipment to support its activities in cybersecurity and privacy of Smart-Devices, smart-cards, Internet of Things, and digital identity. It hosts and maintains the European Root Certification Authority for the digital tachograph and the Public Key Infrastructure serving the EU Laissez Passer.

3. Emerging challenges

An emerging area of work is the block-chain technology which can cause disruptive changes to many sectors of the economy. This work is currently carried out with a specific focus on virtual currency (VC) as requested by V-P Dombrovskis. JRC is assessing the risks associated with different virtual currency concepts: fraud risk, technology vulnerabilities, misuse and systemic risk. This includes looking at VCs in general, but, also monitoring emerging VC concepts and Bitcoin, in particular. More specifically, this means assembling existing knowledge and research available on bitcoin with potential economic and financial stability implications and also monitoring how international institutions and regulators are tackling regulatory aspects related to VCs.

To support the opportunities arising from VC systems, JRC is analysing their underlying technologies and assesses, on the one hand, the possible cyber vulnerabilities linked with the VCs information technology architecture and, on the other hand, possible benefits to other sectors of the digital world (for example, online services and smart grids). Part of this work involved analysing bitcoin characteristics which determine whether bitcoin might become a relevant currency, by evaluating whether it fulfils the main functions of money: a medium of exchange, a unit of account and a store of value. The two most important challenges hindering its growth appear to be the particularities of bitcoin price formation and its extreme price volatility.

Furthermore, with the start of the preparatory work for the free-flow of data initiative, also scheduled for launch in the second half of 2016, the flow of data generated by Internet of Things (IoTs) machine-generated data, sensor-generated data will raise many cybersecurity challenges in the area of, data ownership, data traceability, data liability. These are topics in which JRC has strong competences ranging from security, privacy and identity management.