SecurityResearch
Community of Users

CoU Brief
Cyber: crime and security

March 2019 / Issue 7

Summary statement

- The cyber domain would benefit from a more integrative approach, engaging different types of actors in the development of policies and strategies. In particular, cross-border cooperation would benefit from the exchange of data between various stakeholders. Efforts in the cyber field should be harmonised in order to create a level playing field in the EU.
- The rapid changing technologies and the vast amount of data to be processed create both opportunities and risks in the cyber domain. Interoperability of different systems and datasets would benefit (cross-border and cross-sector) activities in this domain.
- In the process of developing new solutions, the practitioner perspective should remain central. Innovative technologies and tools need to address needs of practitioners and, therefore, it is recommended to include practitioners in an early phase of the projects.

Introduction

This CoU brief summarises the topic 'Cyber: crime and security' and relevant EU-funded projects that participated in the 13th Meeting of the Community of Users (CoU) on Secure, Safe and Resilient Societies that took place 25 – 29 March 2019 at the BAO convention centre in Brussels.

The Community of Users is a DG HOME initiative that aims to improve information transfer of research outputs and their usability by different categories of stakeholders. During the meetings and thematic workshops, policy updates and information about H2020 projects are provided and interactive discussions facilitated to ensure that solutions and tools resulting from research will reach users.

European Commission

Scope & Relevance

As a result of our increasingly interconnected, interdependent and digitalised world, we have become more and more dependent on digital means. Examples of the way in which technologies impact our day-to-day life are manifold: connected mobility, cybersecurity, digital health systems, online privacy, our electronic identity, connected cities and electronic transactions. From a security perspective, defending society against those who intend to misuse those digital means has become increasingly challenging.

Therefore, fighting crime and improving cybersecurity have become a strategic priority for the EU. The Union is building resilience to cyberattacks, both on the side of capacity building as well as with regards to prevention and response coordination. Capacity building efforts are aimed at enhancing national capacities, industrial capabilities and risk management requirements and include financial support from the EU. Prevention and response coordination focuses on fighting (cyber)crime, operational support, coordinated response to large-scale cyber security incidents and crises and developing a single market for certified ICT products and services.[1]

The Directive on security of network and information systems (NIS Directive)[2] is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU, primarily focusing on increased national cybersecurity capabilities, EU level cooperation, and security and notification requirements.

Also, supporting Law Enforcement in fighting cybercrime and providing digital tools that they may use is one of the key issues of the safe and secure cyberspace in Europe. With the amount of digital data increasing, it is necessary to think how to support the work of Law Enforcement using Artificial Intelligence (AI) tools as well. A number of Member States and Associated Coutries have on-going initiatives to modernize the work of LEAs in this direction. This point is clearly raised in Communication on Working together for Artificial Intelligence, containing a Coordinated Action Plan, drawn up jointly with Member States and adopted by the Commission in December 2018.

Finally, the EU's multiannual financial framework 2021-2027 aims for a modern budget in order to ensure that Europe drives the digital transformation of society and economy, bringing benefits to all citizens and businesses. Compared to H2020 projects, it is a way to move forward to industrialize research results. Member states already agreed on the budget, apart from the cyber security.

Thematic focus areas

During the 13th CoU event, the Thematic Workshop on cybercrime security was divided in four different subthemes: law enforcement needs from digital tools, cyber security intelligence, building a cyber-security eco-system to secure European Society, and artificial intelligence. The discussions held during these sessions are presented below.

Law enforcement needs from digital tools

During the session on law enforcement needs from digital tools, the group was divided in four different workshops: digital forensics; Open Source Intelligence (OSINT)[3]; criminal analysis and cross border digital cooperation. The outcome of each workshop has been summarized below.

Digital forensics

The domain of digital forensics is particularly in need of tools and training to be able to cope with the vast amount of data on social media. Artificial intelligence (AI) is considered to be a useful tool to reduce the workload of digital forensics by algorithms that can automatically search for certain information in big data. The challenge in these automated tools is that they should automatically be updated in order to cope with the ever changing digital environment (e.g. wording referring to certain information on the internet is continuously changing).

Also, cross-border data sharing (between courts) is a challenge in the field of digital forensics. The need for normalisation of cross-border cooperation was raised in order to better address challenges such as language barriers. Moreover, a common legal framework on data, standards, quick research, and validation of tools, knowledge and training courses is welcome to further improve cross-border exchanges. The different tools used could be harmonised in order to identify what already exists and what gaps there are. However, this would requires clear guidelines on how to deal with the GDPR.

OSINT – Open Source Intelligence

As OSINT relies on open sources, accessibility and interoperability are crucial. OSINT would benefit from interoperable data in order for different sources to read and use the same type of data. Inherently linked to the use of open source data is the risk of misinformation. To mitigate this risk, the need for tools to counter misinformation was voiced during the 13th CoU event.

1 General introduction on Cyber 13th CoU event, March 2019.
2 EU 2016/1148
3 There is a need to clearly differentiate between digital forensics and OSINT: digital forensics encompasses the recovery and investigation of material found in digital devices. OSINT, on the other hand, is focused on retrieving data from open sources (which can serve as evidence at a later stage of an investigation).

A key challenge for law enforcement in the OSINT domain is to retrieve data from large companies (such as Facebook). A general methodology that would provide guidance on how data can be retrieved and used is welcomed.

Criminal analysis
The discussion on his topic was geared towards the currently ongoing negotiations with regards to an EU platform for the law enforcement community, to be hosted by Europol. This platform should facilitate the exchange of software, best practices, open source intelligence and connect existing initiatives. Hereby, the sustainability of existing projects would be enhanced.

Cross border digital cooperation
A major challenge in cross-border cooperation in the digital domain is the speed at which information can be shared and requested and the speed at which the digital environment is changing. Currently, there is a lack of certification and common understanding between the Member States; it is unclear what kind of information could be requested in which Member State, and in what format information could be shared. To this end, templates to request and provide digital evidence would benefit international cooperation. In order to actually realise smoother cooperation, it is essential to build trust between the Member States. In particular, attention would need to be paid towards ensuring a coordinated way of structuring data (as currently different categorisations are applied across the EU).

Another challenge is the gap between practitioners and research. Researchers use dummy data in order to invent new tools. However, tools based on such data might not match the reality faced by practitioners. Experts have observed efforts to mitigate this risk; an increase in the amount of data sharing from police forces with researchers has been identified.

Cyber security intelligence

The digital vulnerabililty of the EU is increasing: both cyber threats and the number of social media accounts, containing sensitive personal information, are on the rise. We are increasingly exposed to activities such as hashtag and traffic hijacking, the creation of fake profiles on social media, clickbait attacks, phishing and stolen credentials.[4] In addition, a montenisation trend (i.e. ransomware attacks) is becoming an increasinly prominent threat. Criminals use new technologies and exploit the absence of coherent laws and regulations. The current reality is that government authorities and companies are not changing or updating their software quickly enough, which makes it easy for attackers to identify the weak point in a system, infiltrate and exploit the old vunerabilities in a software.

Similarly, the availability of vast amount of datasets and the ability to process them to predict the future is changing the modus operandi and the level of insight of cyber intelligence authorities. Cyber Intelligence units collect information and data mainly from social media in order to improve the state of cyber security. In order to effectively address these new challenges, the traditional protection-focused approach to security is insufficient. A new risk-based and outward-looking approach is needed.

The interoperability of devices and cyber defense solutions is getting increasingly complex. Often operating systems (e.g. medical devices) are not compatible when it comes to cyber security software, which creates a complex ecosystem is exposed to security gaps an threats.

Software providers offer solutions which analyse the current phase of the attack based on the digital footprints (indicators) the attackers are leaving behind (streams, logins, domain, IP address). This allows them to present their customers daily report on possible threats so that they can be prepared and secure your image and customers. It would be helpful if competitors cooperate and allow data sharing to better protect the customer. Also, companies and public authorities need to invest in software that can help to prevent an attack before it actually happens.

The most important lessons from this session are that three fold. First, Cyber intelligence enables researchers and practicioners to be proactive and predict attacks which are likely to happen. Second, big data approaches (i.e. automation and Artificial Intelligence) are necessary to handle the volumes of data generated. Finally, attribution may turn out to be a major challenge (i.e. it is difficult to find a smoking gun in cyberspace).

Building a cyber-security eco-system to secure European Society

One of the issues that the EU cyber security market faces is the lack of cooperation between the supply and demand-side. In addition, there is insufficient collaboration between research and industry.[5] This gap is intended to be bridged by the four European Cybersecurity Competence Network pilot projects.[6] Early 2019, four pilot projects were selected: CONCORDIA, ECHO, SPARTA and CyberSec4Europewhich are expected to strengthen the EU's cybersecurity capacity and tackle future cybersecurity challenges for a safer European Digital Single Market.[7] In total, 63.5 million euros of EU contribution was made available to support the four pilot projects.

4 In one case, a fictive female character called Robin Sage created by a cyber security company pretended to working as a "cyber threat analyst" at the U.S. Navy's Network Warfare Command. Within less than a month, she amassed nearly 300 social-network connections among security specialists, military personnel and staff at intelligence agencies and defense contractors.
5 Ibid.
6 Resulting from the Horizon 2020 cybersecurity call "Establishing and operating a pilot for a European Cybersecurity Competence Network and developing a common European Cybersecurity Research & Innovation Roadmap"
7 www.ec.europa.eu/digital-single-market/en/news/four-eu-pilot-projects-launched-prepare-european-cybersecurity-competence-network

The goal of the pilot projects is to develop a European cybersecurity competence network. The pilots will deliver innovative marketable solutions to tackle the future cross-domain cybersecurity challenges. The four projects are expected to cooperate closely in order to advance towards a solid European cybersecurity ecosystem.

The objectives of each of the pilots are briefly presented below.

- **CONCORDIA**[8] (Cybersecurity Competence for Research and Innovation) is a multidisciplinary research an innovation project that intends to develop innovative, marketable solutions to protect Europe against cyberattacks. The pilot aims to build upon existing knowledge and expertise and foresees to establish a European Education Ecosystem for Cybersecurity. With a focus on capacity building, CONCORDIA aims to promote excellent research, market innovation, skill building, and a research roadmap for cybersecurity in Europe.
- **CyberSec4Europe**[9] intends to test and demonstrate potential governance structures for the network of competence centres. The project will address EU Directives and Regulations, such as the GDPR, PSD2, eIDAS, and ePrivacy, and help to implement the EU Cybersecurity Act. The project demonstration cases will address cybersecurity challenges within the vertical sectors of digital infrastructure, finance, government and smart cities, health and medicine and transportation. In addition to the demonstration of the governance structure and the operation of the network, CyberSec4Europe will develop a roadmap and recommendations for the implementation of the Network of Competence Centres using the practical experience gained in the project.
- **ECHO**[10], short for European network of Cybersecurity centres and competence Hub for innovation and Operations, aims to organize and optimize the cybersecurity efforts across the EU that are currently rather fragmented. The Central Competence Hub will serve as the focal point for the ECHO Multi-sector Assessment Framework enabling multi-sector cybersecurity dependencies analysis and management. ECHO aims to develop, model and demonstrate a network cybersecurity research and competence, with a hub of research and competence. ECHO intends to develop an adaptive model for information sharing to foster collaboration between the ECHO partners and related agencies.
- **SPARTA**[11] aims to develop and implement research and innovation collaborative actions, guided by concrete challenges in the cybersecurity domain. SPARTA will foster and facilitate collaboration means, thereby, boosting capacity building activities in this domain in the EU. SPARTA aims to re-imagine cybersecurity research, innovation and training by applying a more innovative approach.

Artificial intelligence

Artificial intelligence (AI) has become an area of strategic importance and a key driver of economic development. It can bring solutions to many societal challenges: from treating diseases to minimising the environmental impact of farming. However, socio-economic, legal and ethical impacts have to be carefully addressed, as well as the misuse of AI in cybercrime. AI is not new, but is becoming increasingly relevant, because there is more computing power, more data, and new algorithms. Currently AI is used for big data gathering, detecting of illicit content online and misinformation, open source intelligence and online identification.

A major gap can be identified in the legal aspect of AI; at the moment there is hardly any governance on AI in the Member States. Most member states have a national AI strategy, but not specifically on law enforcement. AI becomes especially difficult in the law enforcement context due to GDPR. Most of the work done on AI at the national level is project based. Moreover, the differences in the level of IT development, priorities, administrative organisation and legislation across Member States vary greatly.

The need for a continuous dialogue between the AI community and the security community was voiced. Discussions on ethics and technical robustness need to be held and, more importantly, the risk of corrupted data should be debated. On 9 April 2019 ethical guidelines have been shared.[12]

GDPR and Privacy

The EU General Data Protection Regulation (GDPR)[13] can be considered as the most important change in data privacy regulation in 20 years. The regulation will fundamentally reshape the way in which data is handled across every sector, from healthcare to banking and beyond.[14] The regulation presents both technological and organisational challenges for public administration and enterprises. Nevertheless, the general sentiment during the 13th CoU event was that the GDPR regulation should not be regarded as a problem but rather as a business opportunity. There are opportunities to develop innovative solutions that are GDPR compliant.

8 www.concordia-h2020.eu
9 www.cybersec4europe.eu
10 www.echonetwork.eu
11 www.sparta.eu
12 www.ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai
13 (EU) 2016/679
14 www.eugdpr.org

Current debates & stakeholder perspectives

Practitioners

The amount of data that practitioners in the field of cyber security need to digest as well as the speed at which the domain develops pose serious challenges for practitioners. The development of new tools and methods is welcomed, however, such developments would benefit from applying a bottom-up approach by involving practitioners at an early stage of the process.

Given the transboundary nature of cybercrime, practitioners repeatedly emphasised the need for more cooperation and coordination on the international level; this would allow for data exchange processes to run more smoothly. Nevertheless, in order for cross-border collaboration to become truly effective, practitioners would benefit from interoperable datasets and easier data sharing procedures (i.e. templates).

Industry & SMEs

As threats and solutions are rapidly evolving in the cyber security domain, there is ample of room for innovation. Industry stakeholders are encouraged to develop novel solutions that would help to enhance the EU security. In particular, encryption, big data processing and the GDPR provide opportunities for the industry. In order to ensure solutions meet the needs of the end users, the industry is encouraged to apply a bottom-up approach in their solution development processes.

Policy

Throughout the 13th CoU event, policymakers were invited to enhance their efforts towards facilitating cross-border cooperation. In the domain of cybersecurity, this entails enhancing interoperability, developing legal frameworks (that allow digital forensic evidence to be recognised across borders) and to start developing governance mechanisms on AI, to name a few. The fast-changing nature of the cybersecurity domain requires policymakers to apply a more risk-based and outward looking approach than that is currently being done.

Currently, the EU has a variety of policies in place related to fighting (cyber)crime and improving cybersecurity. There is a continuous policy response to the evolving threat landscape:

- **2013 EU cybersecurity strategy**: 'An Open, Safe and Secure Cyberspace': How to prevent and respond to cyber-disruptions and attacks? Today's Cyber Security Strategy outlines the EU's vision on how to enhance security in cyberspace and sets out the actions required, including to drastically reduce cybercrime.[15]
- **2016 Communication on strengthening Europe's cyber resilience system and fostering a competitive and innovative cybersecurity industry**: In its Communication of 5 July 2016 the European Commission announced the launch of a public-private partnership on cybersecurity and additional market-oriented policy measures to boost industrial capabilities in Europe.[16]
- **2017 Cybersecurity package**: the package builds upon existing instruments and presents new initiatives to further improve EU cyber resilience and response/ The European Commission puts forward the creation of a EU certification framework for ICT security products in its 2017 proposal for a regulation.[17]
- **2018 Proposal for the European competence centre and network**: The network would include existing and future cybersecurity centres set up in the Member States, whose members would typically be research centres and laboratories.[18]
- **Communications on Artificial Intelligence:** Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions on Artificial Intelligence for Europe.[19]
- **Coordinated Plan on Artificial Intelligence (COM(2018) 795 final)**: Delivering on its strategy on artificial intelligence (AI) adopted in April 2018 on 7th December the Commission presented a coordinated plan prepared with Member States to foster the development and use of AI in Europe.[20]
- **The NIS Directive** is the first piece of EU-wide legislation on cybersecurity. It provides legal measures to boost the overall level of cybersecurity in the EU.[21]
- **Cyber security act**: reinforces the mandate of the EU Agency for Cybersecurity, (European Union Agency for Network and Information and Security, ENISA) so as to better support Member States with tackling cybersecurity threats and attacks.[22]

15 www.ec.europa.eu/home-affairs/what-is-new/news/news/2013/20130207_01_en
16 www.ec.europa.eu/digital-single-market/en/news/communication-strenghtening-europes-cyber-resilience-system-and-fostering-competitive-and
17 www.ec.europa.eu/digital-single-market/en/cyber-security
18 www.ec.europa.eu/info/law/better-regulation/initiatives/ares-2018-1598442_en
19 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN
20 https://ec.europa.eu/knowledge4policy/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en
21 https://ec.europa.eu/digital-single-market/en/network-and-information-security-nis-directive
22 www.ec.europa.eu/commission/news/cybersecurity-act-2018-dec-11_en

- **GDPR**: As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based.[23]
- **Multiannual financial framework 2021-2027** 'a modern budget for a union that protects, empowers and defends': A new mechanism to protect the EU budget from financial risks linked to the rule of law.[24]

Research

The nature of the cybersecurity domain requires research to develop innovative solutions which are of immediate use to practitioners. To this end, research actors are encouraged to reach out to practitioners in order to better understand what their needs and challenges are; based on this, new tools and methodologies can be developed.

A key challenge in the research domain is the usage of data; both in terms of quantity and in the sensitivity of the data. Moreover, sharing data between stakeholders and authorities remains a challenge and the academic field is invited to identify possible pathways here.

Relevant projects & project hubs

Activities conducted as part of the following projects were outlined by project representatives during the 'Cyber; crime and security' session at the 13th CoU meeting:

- **AviaTor**
- **ARIES**[25] (September 2016 – February 2019) main goal is to deliver a comprehensive framework for reliable e-identity ecosystem comprising new technologies, processes and security features that ensure highest levels of quality in eID based on trustworthy security documents and biometrics for highly secure and privacy-respecting physical and virtual identity management, with the specific aim to tangibly achieve a reduction in levels of identity theft, fraud and associated crimes.
- **ANITA**[26] (May 2018 – May 2021), Advanced tools for fighting oNline Illegal TrAfficking, will design and develop a knowledge-based user-centred investigation system for analysing heterogeneous online and offline content for fighting illegal trafficking of drugs, counterfeit medicines, NPS and firearms.
- **ASGARD**[27] (September 2016 – February 2020) has a singular goal, contribute to Law Enforcement Agencies Technological Autonomy and effective use of technology. Technologies will be transferred to end users under an open source scheme focusing on Forensics, Intelligence and Foresight (Intelligence led prevention and anticipation).
- **Cerberus**
- **COPKIT**[28] (2018 – 2021) focuses on the problem of analysing, investigating, mitigating and preventing the use of new information and communication technologies by organised crime and terrorist groups. For this purpose, COPKIT proposes an intelligence-led Early Warning (EW) / Early Action (EA) system for both strategic and operational levels.
- **COMPACT**[29] (October 2017 – October 2020) cybersecurity for Public Administrations.
- **CONNEXIONs**[30] (September 2018 – Septemer 2021) aims to develop and demonstrate next-generation detection, prediction, prevention, and investigation services. These services will be based on multidimensional integration and correlation of heterogeneous multimodal data, and delivery of pertinent information to various stakeholders in an interactive manner tailored to their needs, through augmented and virtual reality environments.
- **CYBERTRUST**[31] Advanced Cyber-Threat Intelligence, Detection, and Mitigation Platform for a Trusted Internet of Things.
- **DANTE**[32] (September 2016 – March 2019), Detecting and ANalysing TErrorist-related online contents and financing activities, has delivered effective, efficient and automated data mining, analytics solutions and an integrated system to detect, retrieve, and analyse vast amounts of heterogeneous and complex multimedia and multi-language terrorist-related contents from both the Surface and the Deep Web, including the Dark Nets. DANTE aimed to discover (by "connecting the dots"), analyse and monitor potential terrorist-related activities and people.

23 www.ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
24 https://www.consilium.europa.eu/en/policies/eu-budgetary-system/multiannual-financial-framework/mff-negotiations/
25 https://cordis.europa.eu/project/rcn/202675/en
26 https://www.anita-project.eu/
27 https://cordis.europa.eu/project/rcn/203297/en
28 https://copkit.eu/
29 http://compact-media.eu/
30 https://www.connexions-project.eu/
31 https://cyber-trust.eu/
32 www.h2020-dante.eu

- **DEFenD**[33] (July 2018 – January 2021). The DEFeND project is focusing on engineering and trust and is dealing with data governance and privacy engineering for GDPR. DEFeND is an international partnership that will deliver a platform to empower organisations in different sectors to assess and comply to the GDPR.
- **ENFORCE**[34]
- **FTv3.0**
- **INCOGNITO** (January 2019 – January 2023), IdeNtity verifiCatiOn with privacy-preservinG credeNtIals for anonymous access To Online services.[35] The overarching goal of INCOGNITO is to combine state-of-the-art technologies in a platform that will allow users to easily understand what is needed to access online services with respect to their privacy and be able to prove specific attributes of their identity or their whole identity.
- **LETS-CROWD**[36] (May 2017 - October 2019) will overcome challenges preventing the effective implementation of the European Security Model with regards to mass gatherings. This will be achieved by providing the following to security policy practitioners and in particular, Law Enforcement Agencies (LEAs).
- **Magneto**[37] (May 2018 – April 2021) will revolutionize the capacity of Law Enforcement Agencies (LEAs) to deal with extreme volumes and diversity of data in order to accomplish highly- efficient crime prevention and investigation.
- **Papaya**[38] (May 2018 – May 2021), PlAtform for PrivAcY preserving data Analytics, claims to be the first global HRIS solution to ensure 100% GDPR compliance. Its goal is to transform traditional international human resource management into automated technology with the belief that managing global workforce and international payroll across many countries with outdated tools is time consuming and prone to many mistakes.
- **PDP4E**[39] (May 2018 – February 2021), Privacy and Data Protection 4 Engineering, will provide.
- **Poseidon**[40] (May 2018 – November 2020). Poseidon will develop and deliver an innovative intrinsically scalable platform, as an integrated and comprehensive solution aimed to safeguard the rights of data subjects, exploiting the cutting-edge technologies of Smart Contracts and Blockchain, as well as support organizations in data management and processing while ensuring GDPR compliance.
- **PROPHETS**[41] (May 2018 – April 2021) will deliver the strategic outcomes through seven critical objectives that will encompass extensive research exploring the key factors that underpin cybercriminal and online terrorist behaviour.
- **PERICLES**[42] (2017-2020) aims to develop a comprehensive approach to prevent and counter violent radicalisation and extremism.
- **RAMSES**[43] (September 2016 – August 2019) aimed to deliver much needed quantified evidence of the impacts of climate change and the costs and benefits of a wide range of adaptation measures, focusing on cities.
- **SAURON**[44] (2016 - 2017) addresses the topic CIP-01-2016-2017: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe and put the focus on protection of EU Ports under Transport Infrastructure and means of transportation type of CI.
- **Smooth**[45] (May 2018 – November 2020). SMOOTH assists micro enterprises in adopting and complying with the General Data Protection Regulation (GDPR) by designing and implementing easy-to-use and affordable tools.
- **SPIRIT**[46] (January 2018 – February 2021) aims to develop an "inspection skill" for robots that takes the step from programming of complex inspection tasks to configuring such tasks.
- **TENSOR**[47] (September 2016 – September 2019), Retrieval and Analysis of Heterogeneous Online Content for Terrorist Activity Recognition, seeks to develop a platform offering Law Enforcement Agencies fast and reliable planning and prevention functionalities for the early detection of terrorist activities, radicalisation and recruitment.

33 www.defendproject.eu
34 https://ec.europa.eu/energy/intelligent/projects/en/projects/enforce
35 www.incognito.socialcomputing.eu
36 https://letscrowd.eu/
37 http://www.magneto-h2020.eu/
38 www.papayaglobal.com
39 www.pdp4e-project.eu
40 www.poseidon-h2020.eu
41 https://www.prophets-h2020.eu/project/objectives/
42 http://project-pericles.eu/
43 http://www.ramses-cities.eu/home/
44 https://www.sauronproject.eu/
45 smoothplatform.eu
46 http://spirit-h2020.eu/
47 www.tensor-project.eu

- **The Future Trust project**[48] (June 2016 – June 2019) deals with questions related gaps privacy and engineering, analyses the impact of Artificial intelligence on privacy and calls for more work on explainability and governance in this field.
- **The I-LEAD project**[49] (September 2017 – August 2022) is a joint initiative from the core group of the European Network of Law Enforcement Technology Services (ENLETS). The project will go beyond the scope of ENLETS, since it is designed to integrate security research, and will connect security research with the European Agenda on Security to strengthen the cross border crime fighting, setting the perimeters for technology Pan-European cooperation between Law Enforcement Agencies (LEA), Industry and research community.
- **ILEANET**[50] (June 2017 – May 2022) aims to build a sustainable organisational Law Enforcement Agency (LEA) practitioners network focused on research & innovation addressing LEA challenges, together with a community of individuals interested to exchange and collaborate in this area.
- **I-REACT**[51] (June 2016 – May 2019) harden exisitng Software Systems and analyze Future Cyber Security Threats.
- **RED Alert**[52] (June 2017 – May 2020) will bring data mining and predictive analytics tools to the next level, developing novel natural language processing (NLP), semantic media analysis (SMA), social network analysis (SNA), Complex Event Processing (CEP) and artificial intelligence (AI) technologies.
- **Victoria**[53] (May 2017 – April 2020) Video analysis for Investigation of Criminal and TerrORIst Activities.

Possible synergies (and links to policies and practitioners' operations)

For an overview of Cyber related projects funded prior to 2018, see section 6 Crime and Terrorism) of DG HOME, "**Community of Users on Secure, Safe and Resilient Societies – Mapping Horizon 2020 and EU-funded Capacity-Building Projects under 2014-2017 Programmes**." The projects referenced within this section of the aforementioned document are universally geared towards tackling similar subjects as those discussed in this brief, and thus have the potential of exhibiting synergies with them.

Lessons learnt, challenges and way forward

The main challenges within the cyber domain can be linked to the capacities and capabilities existing to cope with the huge amount of data, the quality of data, the trustworthiness of data, and the rapid changes in technologies. Close cooperation and coordination between the Member States is a way to increase the ability of the EU to deal with the threat that cyber poses. Enhanced sharing of databases and equipment allow for closer (cross-border) cooperation. However, in order to realise such cooperation, it is essential to develop a level of trust between the various stakeholders. Cooperation requires trust.

Tools developed for the cyber domain would need to be more easily accessible and would benefit from being more flexible towards the rapidly changing technologies. In this regard, the inclusion of practitioners is essential. Carefully defining processes, certification and procedures around new technologies has been identified as a way to remain in control in this ever evolving field.

48 www.futuretrust.eu/
49 www.eos-eu.com/ilead
50 https://www.ileanet.eu/
51 https://cordis.europa.eu/project/rcn/203294/factsheet/en
52 https://redalertproject.eu/
53 https://www.victoria-project.eu/

Key Contacts

http://www.securityresearch-cou.eu/

DG HOME
Philippe Quevauviller
Philippe.Quevauviller@ec.europa.eu

Nada Milisavljevic
Nada.MILISAVLJEVIC@ec.europa.eu

Zsuzsanna Felkai Janssen
zsuzsanna.felkai-janssen@ec.europa.eu

EC DG CNECT
Jean-Francois Junger
Jean-francois.JUNGER@ec.europa.eu

Juha Heikkila
Juha.HEIKKELA@ec.europa.eu

JRC
Ignacio.Sanchez
Ignacio.Sanchez@jrc.ec.europa.eu

S. Gaines
sgaines@vicomtech.org

Forthcoming related events

- 14th CoU event, 16 – 20 September, Brussels, Belgium
- Security Research Event, 6 – 7 November, Helsinki, Finland