

Summer 2021

EURESCOM message

The magazine for telecom insiders

CELTIC News 1/2021



Security and Trust in 5G and Beyond

The Kennedy perspective
Absence makes the team forget

Events
Joint EuCNC & 6G Summit

A bit beyond
The dark side of data





Join the Industry-Driven Research Programme for a Smart Connected World

CELTIC-NEXT Call for Project Proposals – Deadline: 22nd November 2021

Do not miss the opportunity to participate in CELTIC-NEXT, the industry-driven European ICT and telecommunications research programme under the umbrella of Eureka. Submission deadline for the next call for project proposals is 22nd November 2021.

CELTIC-NEXT projects are collaborative private-public partnership R&D projects. All Eureka member countries and associated countries can financially support them. More information on public funding and national contacts per country can be found on the CELTIC-NEXT Public Authorities Website. Please talk to your national contact early in the process.

Easy proposal process

Preparing and submitting a CELTIC-NEXT project proposal is easy. Just register on the CELTIC-NEXT online proposal tool, fill in the Web forms, and upload your proposal in pdf. Access to the proposal tool and to a proposal template is available via our Call Information page (<https://www.celticnext.eu/call-information>).

Benefits of participating in CELTIC-NEXT

- You are free to define your project proposal according to your own research interests and priorities.
- Your proposals are not bound by any call texts, as long as it is within the ICT/telecommunications area see: see CELTIC-NEXT Scope and Research Areas.
- CELTIC-NEXT projects are close to the market and have a track record of exploiting their results soon after the end of the project.
- High-quality proposals have an excellent chance of receiving funding, with an average success rate higher than 50 %.
- The results of the evaluation will already be known in January 2021.

If you have any questions or need help, do not hesitate to contact us; we are pleased to help you.

Contact

CELTIC-NEXT Office
Xavier Priem
office@celticnext.eu
Website: www.celticnext.eu



Dear readers,

5G has further increased the importance of cybersecurity. While network security has already been of high importance, the new usage scenarios enabled by 5G have dramatically increased the stakes. Just think of automated driving and IoT applications in factories, and it becomes clear that network security has become not only a central topic for the ICT domain, but for economy and society as a whole.

In this issue of Eurescom message, we explore what is done in Europe to advance security and trust in 5G and beyond. We present selected research and innovation projects that have contributed to novel solutions for making 5G and future 6G networks more secure.

In the first article of the cover theme, Eurescom message editor Anastasius Gavras gives an overview on security and trust in 5G and beyond. The next article presents 5G PPP project INSPIRE-5Gplus and its holistic security vision for 5G and beyond networks.

In an exclusive interview for Eurescom message, three cybersecurity experts from ENISA share their views on security threats and strategies for 5G and beyond.

In the final article of the cover theme, a team from the 5G-VINNI project present the defence perspective on 5G, adding another dimension to the topic.

This edition of Eurescom message also includes a variety of further articles on different, ICT-related topics. See, for example, the new opinion article by Eurescom director David Kennedy on the drawbacks of working from home in his column "The Kennedy Perspective". Under "Events", we report about three important virtual events – the final workshop of 5G PPP infrastructure project 5G EVE, the Joint EuCNC & 6G Summit, and a workshop on liability and accountability organised by the INSPIRE-5Gplus project. See also our "News in brief" section, which features the European Green Digital Coalition and the lat-

est Ericsson report on 5G mobile subscriptions. Finally, in the latest "A bit beyond" article you can learn about the dark side of data.

My editorial colleagues and I hope you will find value in this edition of Eurescom message, and we would appreciate your comments on the current issue as well as suggestions for future issues. Enjoy reading our magazine.

Milon Gupta
Editor-in-chief



EVENTS CALENDAR



31 August 2021 – 3 September 2021

IoT Week

Online Event

<https://iotweek.org>

7 – 10 September 2021

IEEE International Mediterranean Conference on Communications and Networking (MeditCom 2021)
Hybrid In-Person Conference (Athens, Greece) and Virtual Conference

<https://meditcom2021.ieee-meditcom.org>

13 – 16 September 2021

IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC 2021)

Virtual Conference

<https://pimrc2021.ieee-pimrc.org>

7 – 11 December 2021

IEEE Global Communications Conference (GLOBECOM 2021)

Madrid, Spain

<https://globecom2021.ieee-globecom.org>

SNAPSHOT



Virtual exhibition booth



At this year's fully virtual EuCNC & 6G Summit on 8-11 June 2021 also the booths in the exhibition were virtual. The image shows the vir-

tual booth of 5G PPP project 5G EVE, which offered information via video and brochure as well as live access to a 5G EVE expert team.



Further information

is available on the Joint EuCNC & 6G Summit website – <https://www.eucnc.eu/> Source:

Wristify

Contents

	3	Editorial	
	4	Events calendar	
	4	Snapshot	
THE KENNEDY PERSPECTIVE	6	Absence makes the team forget	
COVER THEME		Security and Trust in 5G and Beyond	
	7	Security and Trust in 5G and Beyond – An Overview	
	9	A holistic security vision for 5G & Beyond networks – The INSPIRE-5Gplus project	
	11	Military use of 5G – Advantages of 5G from a defence perspective	
	14	Security threats and strategies for 5G and Beyond – Interview with cybersecurity experts from ENISA	
		CELTIC News	
<i>CELTIC Chair's Corner</i>	3	The Eureka Clusters Programme – A New Era of Joint Thematic Calls	
<i>Events</i>	4	AI-NET Kick-Off Event – CELTIC Flagship Project for Intelligent Network Automation	
<i>Public Authority Profile</i>	6	Supporting the Telecommunications Area in Spain through CELTIC-NEXT – Centre for the Development of Industrial Technology (CDTI)	
<i>Project Highlights</i>	8	5G-PERFECTA – 5G and next generation mobile performance compliance testing assurance	
<i>Update from the CELTIC Office</i>	10	Relaunch of CELTIC-NEXT in revised Eureka Clusters Programme	
	11	High number of proposals in Eureka Clusters AI Call 2021	
	11	6 new projects received CELTIC-NEXT label	
EVENTS	16	Demonstration of 5G end-to-end validation platform – Final 5G EVE webinar	
	17	On the Road to 6G – Joint EuCNC & 6G Summit	
	19	Accountability and Liability for 5G and Beyond – INSPIRE-5Gplus workshop	
NEWS IN BRIEF	20	European Green Digital Coalition established ++ Over 580 million 5G mobile subscriptions by the end of 2021	
A BIT BEYOND	22	The dark side of data – How data garbage hurts business and the environment	

Security and Trust in 5G and Beyond



Imprint

Eurescom message, summer issue 2021
ISSN 1618-5196 (print edition)
ISSN 1618-520X (Internet edition)

Editors: Milon Gupta (editor-in-chief), Anastasius Gavras, Uwe Herzog

Submissions are welcome, including proposals for articles and complete articles, but we reserve the right to edit. If you would like to contribute, or send any comments, please contact:
Eurescom message · Wieblinger Weg 19/4 · 69123 Heidelberg, Germany · Phone: +49 6221 989-0 · Fax: +49 6221 989-209 · E-mail: message@eurescom.eu

Advertising: Luitgard Hauer, phone: +49 6221 989-405, e-mail: hauer@eurescom.eu

Eurescom message is published twice a year. Eurescom message on the Web: <http://www.eurescom.eu/message>

Data Protection Declaration: <https://www.eurescom.eu/data-protection-declaration.html>

© 2021 Eurescom GmbH. No reproduction is permitted in whole or part without the express consent of Eurescom.

Absence makes the team forget

Challenges of home working



David Kennedy
Eurescom
kennedy@eurescom.eu

We have been in various stages of lockdown for over a year now and it has fundamentally changed the way we interact for both work and social interactions. Many praise this as a liberalisation of the work-life balance, but I'm not so sure. I believe that we may be losing something of great value that cannot easily be replaced by an audio conference.

The benefits of home working

When we discuss the benefits of home working, we seem to always assemble a list of personal points that appear to favour the individuals' perspective. These generally include: time management flexibility; no office interruptions/distractions; ability to self-organise the home office; better environment for conference calls; no commuting, and more time with family.

Inherent in these is the permission we give ourselves to intersperse the work with many home actions: do the laundry, walk the dog, get the shopping while everyone else is at work. Now I am not saying these are bad things, but it actually dilutes the home – work boundary in a way which may actually be counterproductive.

Then you find that people start to use personal issues as the reason they should work from home – I am expecting a delivery, I have to keep an eye on my mother, etc., – and while this in itself should not affect productivity, the logic that we don't go to the office because we have a lot of personal things to organise is threatening to the focus our work should have for the equivalent of a working day.

The challenges of home working

The biggest challenge of home working is ensuring the work gets appropriate focus in the life vs. work balance discussion. Home is by nature designed about our own comfort, entertainment and enjoyment. We have fitted our homes out to give us the life comforts we want and to support all out personal interests. This means the chal-



© AdobeStock

lenges we face when working from home are: time management; home interruptions/distractions; increased risks of misunderstandings due to the limitations of emails; long response times between colleagues due to individual schedules; boredom, taking naps, too much tv/music in the background; and less time with colleagues.

Some of the advantages are the biggest challenges as well. The most damaging aspect is that we are much more restricted in our expressions when using emails, messages and video links than when we meet person to person.

The top issue home-office workers find problems with is “disconnecting” from work. Without the clear-cut change of location and defined office hours, many people have difficulties clearly dividing their personal and professional time. Our use of the one platform, e.g., emails for both work and private communications means that our social connections keep popping up while we are working.

The office perspective

From the perspective of the relationship between the individual and the company certain vital concerns arise. The absence of regular person-to-person communication can be a challenge for some people. The biggest issue is to do with the value assessment of the contributions the individuals are making in their absence from the office. This is reflected in the concern of many home workers that their professional efforts wouldn't be fully appreciated as they were not in the office and their colleagues wouldn't automatically see what they are doing.

If we try to list the concerns from the company perspective, we can see that many of the intan-

gible aspects of the beneficial work environment are challenged: keeping the team spirit; maintaining the company culture; understanding and sharing the company policies; team members underworking or overworking in the home environment; and team members feeling lonely or left out.

And this can be compounded by the

difficulty of having tough talks about performance or participation issues over the video link. It is much more intimidating to try and bring up difficult personnel issues over the phone than by speaking directly to each other.

A simple example of the challenge we face today is the question if it is acceptable that audio conferences are interrupted by children running in or by the dog attacking the postman. I've just been in an international conference where the speaker was interrupted by his very young daughter and, while it was not anything to complain about, it did distract him from his presentation to several hundred people. How should we view this – acceptable in the new world or unprofessional?

Conclusion

I have to be honest here and admit that I have not used the home-office option myself, as I need the physical delineation between the home and the office to put me in the right mindset for work. Yes, I do answer emails in the evening and other things, but then I know that I am not at work and can keep it in context.

The biggest challenge I feel is the loss of the casual team interactions over coffee. I have always managed to get a lot of updates, give help on immediate issues and generally get a feel for how my colleagues were managing the work and the, hopefully short-term, overloads. Home working occasionally does not damage this, but prolonged absence due to the COVID situation has precipitated means that you have learned to do without this dialogue – and that is not good for anyone.

Security and Trust in 5G and Beyond

An Overview



Anastasius Gavras
Eurescom
gavras@eurescom.eu

While network security has always been important as a means to protect the physical infrastructure, and the data and content flowing through the network, it is gaining increased attention in the course of 5G and beyond 5G networks, because networks become deeply rooted in our society in the business, governmental and private spaces.

There is an increasing concern about the availability and integrity of networks. All of us have experienced anxiety induced by the outage of network services, whether related to Internet connectivity at the office or at home, or if the mobile network is not reachable due to a failure. Some of the recent cases of mobile network outage could be traced back to malicious or unintentional interventions with the network configuration. Confidentiality and privacy concerns are surfacing in the news when there are breaches of security resulting in a significant impact on customer data. Such cases shatter at least the trust in the technology or the mobile network operators.

Taking a look at some of the fundamental innovations leveraged by 5G, we can derive risks that did not exist with current networks, at least not to such a high extent. Virtualisation and softwareisation are technologies that induce a very high degree of flexibility and agility in the deployment of new services, but at the same time induce complexity. Despite the benefits for every vertical sector and our daily life, complex networks bring along risks that need to be identified and mitigated. The impact of local events, like faults or security breaches, can cause cascading effects, eventually leading to large-scale disruptions.

Generally speaking, end users and consumers accept that software is not perfect. We are used to regular updates pushed by the vendors of our smartphones or our desktop PC operating system vendors. However, when listening to network administrators, there is an unprecedented

amount of software updates that have to be deployed in the network infrastructure just to ensure service continuity and security.

Last but not least the role of network component and infrastructure suppliers has found its way to the news headlines as a potential source for 5G network security concerns, even if supply chain considerations are not new concerns for network operators. While this risk is identified by the European Union Agency for Cybersecurity (ENISA), which published a number of recommendations to mitigate 5G network risks, the U.S. took extreme measures when U.S. president Donald Trump signed an executive order laying the groundwork to block Chinese telecommunications companies from selling equipment in the U.S.

Risk scenarios

The EU toolbox of risk-mitigating measures for cybersecurity of 5G networks classifies the 5G network risks in 5 areas:

- **Insufficient security measures** – This area is not new and best practices exist since the dawn of computer networks. It is a matter of education, awareness and enforcement of measures to minimise misconfiguration of networks and enforce access control.
- **5G components supply chain** – This area already becomes not that straightforward, because it involves some sort of supply chain evidence and certification that all related 5G components used for building a 5G network are sourced from trusted sources and perform the functions as advertised. Questions could be raised with respect to the organisational and technical applicability of such measures. For example, the update of a certified component that belongs to a fully certified service chain implies a re-certification not only of the component in question, but of the complete service chain.
- **Main threat actors** (state interference or organised crime) – This area calls for a strong role of national and European authorities in assessing the risks associated with suppliers and possibly applying restrictions on suppliers of key 5G network assets. Some of the risks in this area can be mitigated by the measures applicable to the first and second area, i.e., enforcing high standards for secure management, operation and monitoring of networks,

as well as ensuring high software and system quality and integrity.

- **Interdependencies of 5G networks with critical infrastructures** – Similarly, this area calls for a strong role of authorities in assessing the risks of cascading effects that a 5G network outage may have on critical infrastructures such as energy production and distribution, transportation systems, etc. Beyond the enforcement of high security standards, this area depends on measures that must be in place for reinforcing resilience and continuity of operations of affected critical infrastructures. The identification of potential cascading effects including mitigation scenarios belong into this area.
- **End user devices** – This area is potentially very vulnerable and represents in itself a large attack vector. While smartphones are generally maintained by the respective vendors, albeit with decreasing maintenance durations due to shorter life expectancy of devices, it is the large number of IoT devices (e.g., simple surveillance cameras, low-end home routers, smart TVs, etc.) that are installed and “forgotten”. These devices contain software, which “ages”, in the sense that vulnerabilities are discovered but not fixed by their respective vendors. Often vendors disappear from the market for various reasons, leaving behind an armada of devices that can be exploited for attacking networks.

Digital sovereignty

The identification of the above risk areas triggered a public debate about the fact that a limited number of components for deploying a 5G network could be sourced from trustworthy suppliers in Europe and, even worse, we could not build a 5G network in Europe without components supplied by other regions of the world.

Digital sovereignty refers to control over our own digital assets – hardware, software and last but not least our data, not only limited in scope to 5G networks. Digital sovereignty has become a concern for many policy-makers that voiced worries about too much control by too few actors in the large tech companies. From a European perspective this includes the fact that none of these large tech companies are located in Europe.

In the cybersecurity area, the Cybercrime Magazine reports a list of the “Hot 150”, the

most innovative companies in the cybersecurity market [1]. It should be highly worrying for policy-makers that the list includes only 5 companies located in the EU; mostly smaller companies that grew out of the anti-virus business.

Liability

Further challenges, in particular with respect to trustworthiness, are induced by the multi-party, multi-layer nature of the 5G ecosystem, which makes it difficult to establish liability relations in case something goes wrong.

Traditionally product liability – as judged in most court cases to date – is limited to “products” in the form of tangible personal property. However, the correct functioning of a future network service – in the simplest case the correct functioning of a networked sensor device – includes the functioning network and service. Therefore, the product or service may become defective upon (i) Network or service failure (even

temporal) and (ii) Discovered security vulnerabilities. Smart networked devices have a far-reaching impact on device and network vendors, service companies, insurers and consumers.

The open questions in this respect are: How should the legal framework on liability evolve in order to cater for such liability chains? Beyond this, how would liability delegation work?

Conclusion

Following the publication of comprehensive and detailed reports on 5G cybersecurity threats by ENISA [2], the main stakeholders in the landscape, including mobile network operators, vertical industry customers, as well as member state and EU officials have sufficient insight to engage and enact a long-term plan to protect European 5G and beyond 5G networks. Such a plan includes specified security measures, 5G good practices for operation and security assurance and last but not least a strong involvement of

European citizens to raise awareness towards adoption of a basic cybersecurity conscious mindset and related behaviour during the use of sophisticated 5G network services.

References

- [1] Cybercrime Magazine Hot 150 list – <https://cybersecurityventures.com/cybersecurity-500/>
- [2] ENISA reports on 5G cybersecurity threats – <https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks>



A holistic security vision for 5G & Beyond networks

The INSPIRE-5Gplus project



Jordi Ortiz
University of Murcia, Spain
jordi.ortiz@um.es



Ramon Sanchez-Iborra
University Center of Defense,
Spanish Air Force Academy
ramon.sanchez@ud.upct.es



Antonio Skarmeta
University of Murcia, Spain
skarmeta@um.es

The recently arrived 5G architectures will enable a plethora of services and applications never imagined some time ago. However, its complex network infrastructure is prone to suffer cybersecurity attacks that must be tackled in order to ensure users' privacy and security. In this line, the Horizon-2020-funded INSPIRE-5Gplus project aims at progressing the security vision of 5G & beyond systems by designing and developing a smart, trustworthy and liability-aware security platform for these kinds of systems. To this end, state-of-the-art technologies such as Zero-Touch Network & Service Management (ZSM), Software Defined Security (SD-SEC) modes, Artificial Intelligence (AI)-based techniques, and Trusted Execution Environments (TEE) are being adopted to provide a security aware architecture and its associated closed-loop of security functions.

To this end, a High-Level Architecture (HLA) for supporting zero-touch end-to-end smart network and service security management in 5G and beyond networks has been designed and is being implemented. By leveraging the flexibility of software-defined technologies (e.g., Software Defined

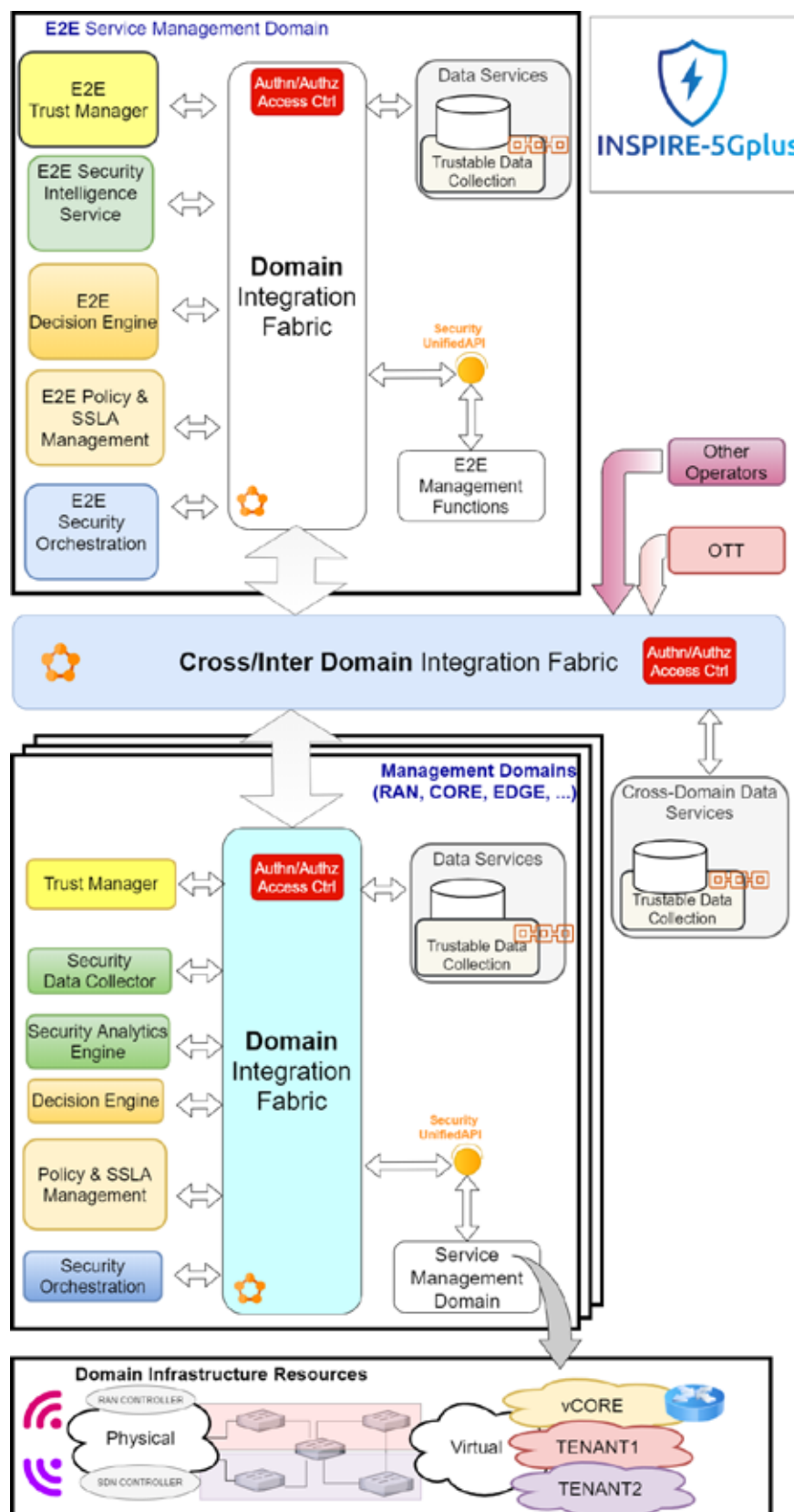


Figure 1: INSPIRE-5Gplus' High Level Architecture (HLA)

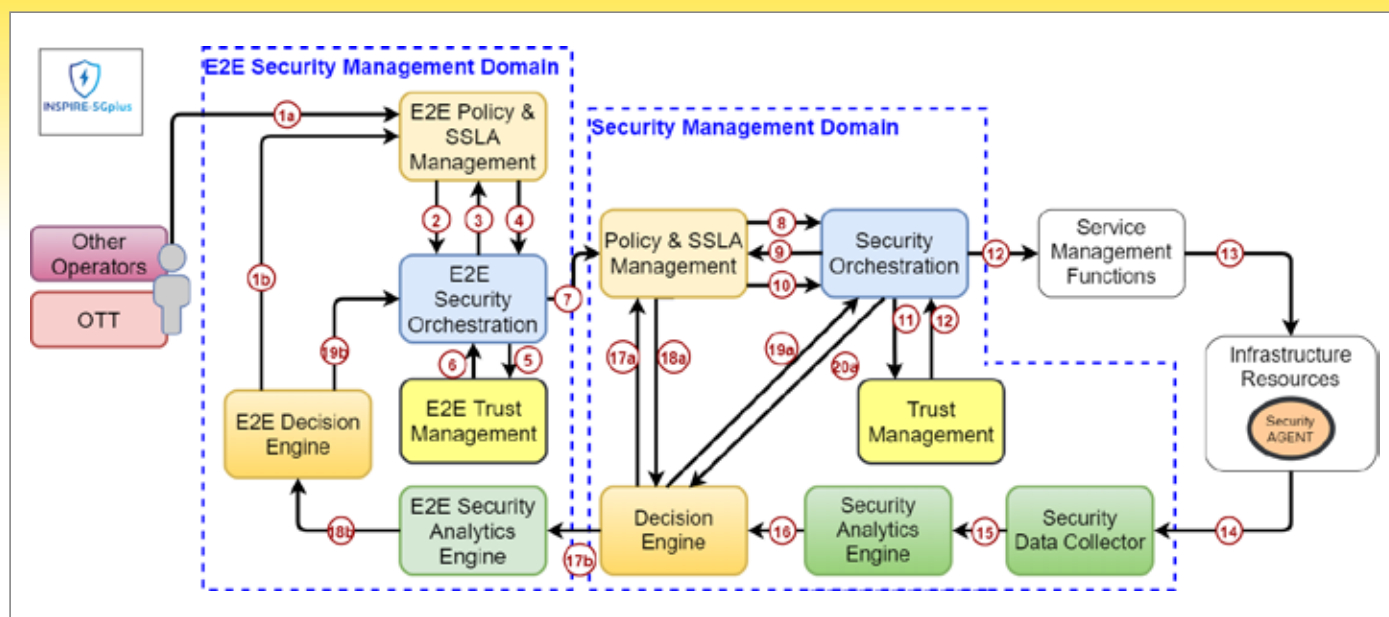


Figure 2: INSPIRE-5Gplus' multi-domain closed-loop interactions

Networks (SDN)/Network Function Virtualization (NFV)) and AI/ML techniques, the INSPIRE-5Gplus HLA will permit end-to-end orchestration and management that enforce and control security policies in real-time and adapt to dynamic changes in threats landscape and security requirements in 5G and beyond networks. Autonomous network orchestration is managed by a closed-loop mechanism that relies on continuous monitoring information to achieve the desired zero-touch automation driven by the introduction of AI techniques. Besides, the project is defining advanced mechanisms to foster trustworthiness of smart SD-SEC solutions in a multi-tenant/multi-domain setting as well as new schemes to enforce liability of involved parties when security breaches occur and/or system fails.

In the following sections, this article explores the overall INSPIRE-5Gplus' HLA and the security management closed-loop on which the project relies, to provide not only protection but also trustworthiness and liability in a fully automated end-to-end smart network and management framework.

INSPIRE-5Gplus architecture

The 5G architecture deals with a huge diversity of services, applications, and use cases that can be classified into three different families: enhanced Mobile Broadband (eMBB), Ultra Reliable Low Latency Communications (URLLC) and massive Machine Type Communications (mMTC). This is achieved by providing a unified and interoperable ecosystem of different and complementary technologies. The promised omnipresence of 5G and beyond networks calls for a secure and trustworthy system to meet the stringent requirements of

the aforementioned families of use cases and services.

In order to deal with this variety of applications INSPIRE-5Gplus has defined an end-to-end HLA supporting the separation of security management concerns. This framework will exploit novel AI-driven security models to enable smart and proactive security management that can intelligently predict, prevent, detect and mitigate cyber threats. On the other hand, novel SDN/NFV orchestration and management mechanisms will be integrated to enforce and control security policies in real-time and adapt to dynamic changes in threats landscape and security requirements.

Figure 1 presents the high-level architecture, which is split into security management domains (SMDs) to support the separation of security management concerns. Each SMD is responsible for the intelligent security automation of resources and services within its scope. The E2E SMD is a special SMD that manages security of E2E services (e.g. E2E network slice) that span multiple domains. The E2E SMD coordinates between domains using security orchestration. The decoupling of the E2E security management domain from the other domains allows escaping from monolithic systems, reducing the overall system's complexity, and enabling the independent evolution of security management at both domain and cross-domain levels.

Each of the SMDs, including the E2E SMD, comprises a set of functional modules (e.g. security intelligence engine, security orchestrator, trust manager) that operate in an intelligent closed-loop way to enable software-defined security (SD-SEC) orchestration and management. This functionality will be further explained in the next section. Each functional module provides a

set of security management services that can be exposed inside the same domain or cross-domain to the authorized consumers, using the domain-integration fabric or the cross-domain integration fabric, respectively.

In addition to a multi-domain design, the INSPIRE-5Gplus security architecture is extensible to multi-operator and Over-The-Top (OTT) environments by considering their security threats and requirements. Although it is developed with a focus on single operator environment needs, the inter-domain fabric provides an inherent capability for security management among disparate networks as shown in Figure 1. The security-aware services available from the operator are made accessible to third parties, such as other operators or OTT services, via the inter-domain integration fabric exposed services. In the same way, this same operator may reach other operators' inter-domain fabric to accomplish an E2E service request originated locally.

Security management closed-loop

INSPIRE-5Gplus has adopted a closed-loop-approach in which a series of automatic security functions are able to coordinate for inspecting the network infrastructure and its crossing traffic in order to detect security anomalies and take automatic measures to mitigate the impact of possible attacks. To this end, the entities forming the HLA integrate cognitive capabilities through the exploitation of novel AI/ML-based security techniques. Thus, the security functions are capable of interacting among each other in an autonomous way, following the ZSM paradigm.

There are two starting points for the whole process (see Figure 2) at the End-to-End (E2E) Secu-

rity Management Domain (SMD) level (1a,1b), both implying the provision of an E2E Security Service Level Agreement (SSLA) coming from an external entity (e.g. OTT) or internally as an AI based reaction, such as those provided by the E2E Decision Engine.

Once the SSLA arrives to E2E SSLA Manager, a refinement process (2,3,4) is performed producing an orchestration High-Level Security Policy Language (HSPL) which in turn is refined in multiple orchestration Medium-Level Security Policy Language (MSPL), at least one per involved SMD. This HSPL to MSPL refinement profits from trustworthiness scores calculated via smart-contracts and taking advantage of the historical behavior of the system among others (5,6).

The solution selected (7) needs to be enforced on the different SMDs, which in turn are responsible of the infrastructure. The Orchestration MSPLs are refined onto Domain MSPLs while taking care of possible dependencies as well as conflicts between them (8,9,10). Similarly to the trustworthiness score-based solution prioritization done at E2E level, at this level not only the possible solutions are valued (11) but also the infrastructure on which they are going to be deployed. As a result of this process the precise

interactions with the infrastructure elements (12) are obtained and the system's behavior is altered (13).

The behavior of the system is constantly monitored, in particular looking for security flaws, and events are reported to the Security Analytics Engine. When an anomaly is detected, Decision Engine at the SMD level is informed (16).

AI techniques are employed to generate a mitigation in MSPL form again inspected for conflicts with the already enforced policies (17a,18a). Finally (19a,20a) the SMD loop is closed by providing the Security Orchestrator with the new policy that is altering the system's behavior again.

Alternatively, or by explicit decision, E2E Security Analytics Engine is informed (17b) of the anomaly and the countermeasure decided, if any. The E2E Security Analytics Engine will inform the E2E Decision Engine (18b) that again may decide to provide a countermeasure but probably affecting neighboring SMDs via the E2E Security Orchestration (19b) therefore closing the E2E loop.

Conclusion

The realization of secure and trustworthy 5G systems is crucial for a firm digital transformation.

To this end, the INSPIRE-5Gplus project is focused on developing a state-of-the-art software-defined security orchestration and management framework for future connected systems (5G & beyond) and pervasive services. The designed architecture empowers zero-touch security services for protection, trustworthiness and liability in managing 5G & beyond systems across multiple domains leveraging emerging techniques, including ZSM, AI/ML, DLT and TEE. The foundations of this security architecture is based on enabling an intelligent closed-loop of security operations that takes into account the constitution of multi-domain architectures and the need of multi-level loop termination. INSPIRE-5Gplus establishes the basis for intelligent, secure and trustable 5G deployments by addressing the key security challenges through vertical applications applying the described closed-loop and HLA.

Further information

INSPIRE-5Gplus website –
<https://www.inspire-5gplus.eu>

Military use of 5G

Advantages of 5G from a defence perspective



Kennet Nomeland
Norwegian Defence
knomeland@mil.no



Pål Grønsund
Telenor Research
pal.gronsund@telenor.com

Military experts foresee that 5G will play an important role in future military operations, and 5G is today a hot topic in NATO. Ubiquitous connectivity, high bandwidth and low latency opens for many new use cases and military organizations all around the world are today experimenting with 5G and plan to use public 5G networks providing good

coverage in combination with military-operated private 5G networks.

Ongoing 5G pilots in Norway

The Norwegian Defence has since 2018 participated in the EU-funded project 5G-VINNI coordinated by Telenor Research. In 5G-VINNI we try to adapt public 5G networks to military requirements while conforming to the standards from 3GPP as well as ETSI NFV.

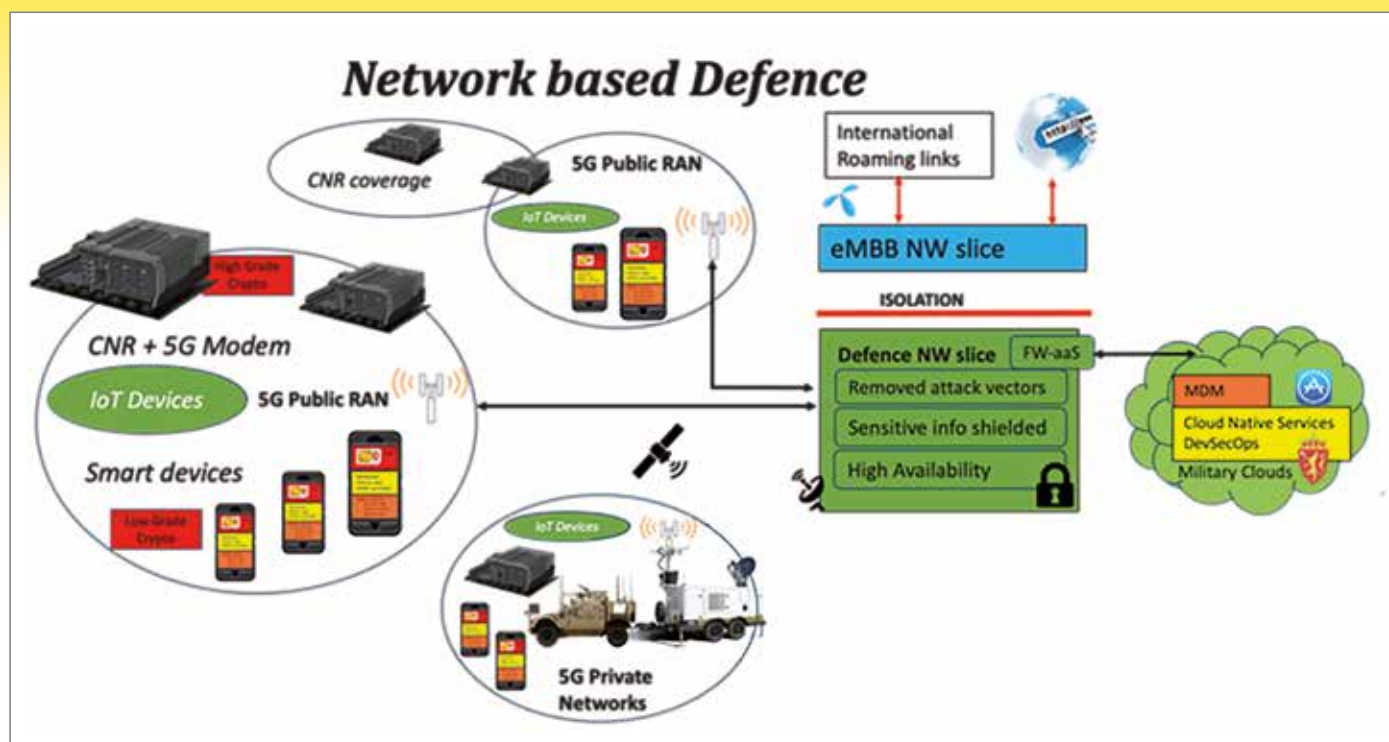
A dedicated defence network slice tailored to military needs has been implemented in the 5G-VINNI pilot network. On Rygge military air station a 5G base station and an enterprise edge computing node have been installed. The Norwegian Defence is exploring 5G MIMO and beamforming capabilities. Range, capacity and robustness in both C-band and mmWave are analyzed to discover in what scenarios 5G New Radio (NR) can be useful to military use.

In September 2020, the Norwegian Defence joined a second EU-funded 5G project, FUDGE-5G. In FUDGE-5G the Norwegian Defence explores the use of private 5G networks.

What is so special about 5G?

From a technical perspective there are several areas that make 5G more interesting for military use compared to earlier generations:

5G New Radio: New frequency bands and new antenna technology are introduced with 5G NR. Massive MIMO and beamforming techniques are of particular interest for military organizations. In addition to the increased capacity that opens for many new military use cases, beamforming may also make the communication more robust against interference. The Norwegian Defence has done trials to measure range and capacity in both C-band (3,4-3,7 GHz) and mmWave (26 GHz). Recently the Norwegian Defence Research Establishment has performed electronic warfare testing to see how robust the 5G NR waveform is against intentional jamming. Integrated Access and Backhaul (IAB) was introduced in Release 16, and in 2022 we are planning to test it in our 5G pilots. We want to find out if IAB can give us a flexible solution when we want to fast extend the 5G coverage.



How a combination of private and public 5G networks could serve military needs in the future

Network slicing makes it possible to create your own virtual network on the same physical infrastructure of a public 5G network. With a dedicated network Slice, you can set your own security policy, priority mechanism, etc. In the 5G-VINNI pilot Telenor Research created a dedicated Defence network Slice with focus on security and where the traffic has been completely isolated from any public or Internet traffic. Roaming has also been disabled. To achieve maximum separation and control of the metadata we have configured a separate 5G Core in the Defence Network Slice. A firewall with Machine Learning capabilities that monitors the traffic and other security functions is applied to the Defence Slice.

IMSI-Catching: Researchers have previously demonstrated how an attacker may use an IMSI catcher to obtain the identity of a subscriber in the form of an International Mobile Subscriber Identity (IMSI) in 4G networks. In 5G standalone (SA) networks it is possible to eliminate the threat from IMSI catchers by using the Subscription Concealed Identifier (SUCI) instead of IMSI. Together with our partners we have verified that when a phone is locked to 5G SA, it will not expose the IMSI. A closed Defence Slice running in a public network may be set up in a mode called 5G SA support only. Practically, this will be possible in a few years from now when Dynamic Spectrum Sharing (DSS) provides a seamless 5G experience of 5G NR in all frequency bands. In addition, SA support is needed in the military handsets, and roaming outside Norway must be blocked. In a commercial eMBB slice this will be difficult, hence this is a good example of the possibilities we have with network slicing.

Autonomy: Edge computing means installing datacenters at the edge of the network close to the users. Using edge computing nodes, it is possible to achieve local autonomy in strategically important areas. In the 5G-VINNI pilot we have a dedicated edge inside Rygge Air Station. This edge is running a complete 5G core network as well as selected application functions. Even with outage of backhaul (both fiber and satellite communication) to the central 5G Core data center in Oslo, the pilot can still provide full autonomy and provide military services to the users in the air-base.

In the FUDGE-5G project we address private 5G networks. A private autonomous 5G network is installed on a trailer (Cell on Wheels) so the armed forces can establish 5G in local areas of interest. From a network perspective we want to utilize both private and public 5G networks, and from a service perspective we want to test how we can utilize both centralized military clouds, 5G and edge computing nodes to create better and more robust services.

Securing 5G for military use

Securing 5G for a military use is complex. We need experts in 5G radio, cloud technology and security. In 5G-VINNI and FUDGE 5G the Norwegian Defence Material Agency is working closely with Telenor Research, the Norwegian National Security Authority and the Norwegian Defence Research Establishment. We have adopted an agile methodology where we perform tests and demonstration and learn as we go, since the learning curve is steep.

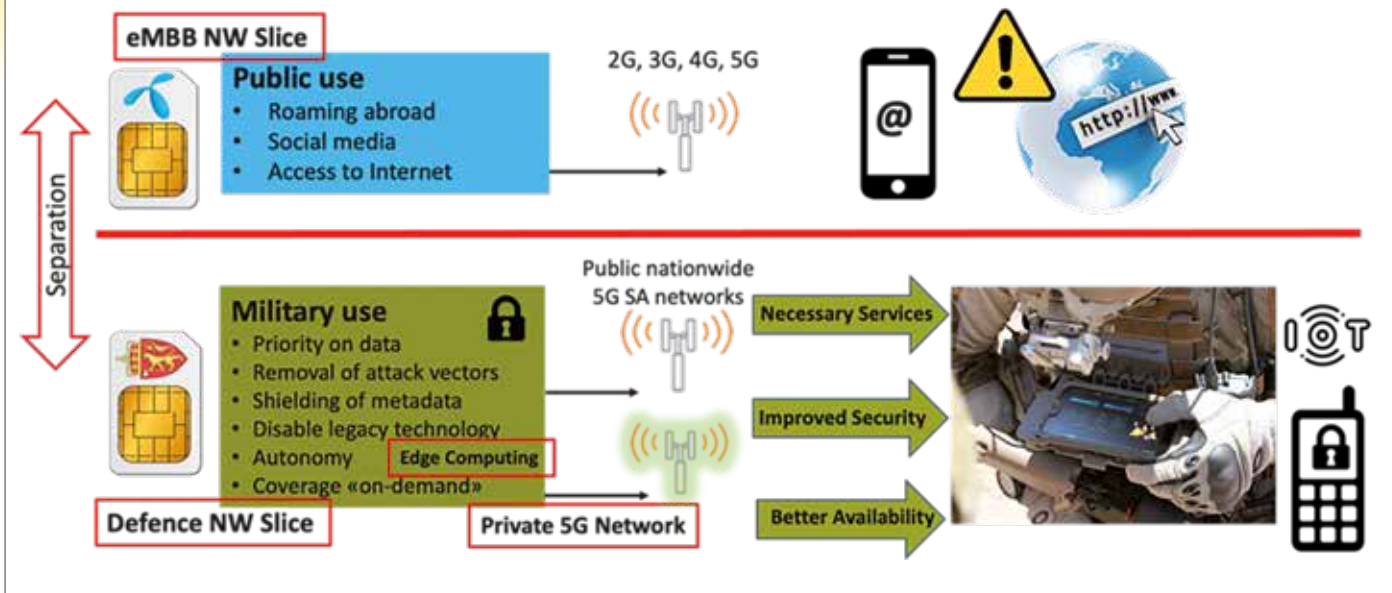
Military organizations have in general good mechanisms to ensure confidentiality and integrity of the data before sending it over a commercial network. An important principle to secure confidentiality in 5G networks is multiple layers of encryption terminating in different places. The encryption provided by 5G (SIM card + IPsec encryption in the transport from the gNodeB to the 5GC) is terminated in the 5G network. Application-level encryption and VPN can add additional security beyond what is provided by the 5G network.

Control of terminals via mobile device management solutions and control of the operating system in the smart devices is also important, if the user equipment is used for classified information.

Modern smartphones support multi-factor authentication (MFA) that is currently not supported by traditional military Combat Net Radios (CNR). A combination of something you know (e.g. password), something you have (e.g. NFC card/ FIDO support) and something you are (e.g. biometry) is today possible on a smartphone.

No military organization will “put all the eggs in one basket” and solely depend on 5G. To be able to communicate in all kinds of scenarios, military organizations will always have different ways of communicating, like satellite communication and CNR. However, we believe that 5G can be used in many scenarios such as in collaboration with public safety agencies. The Norwegian Defence often participates in missions related to natural disasters, refugee crises, terrorism, pandemic diseases, etc. Hybrid warfare targets the whole society, not just the military. The

Network Slicing to separate Public and Military traffic



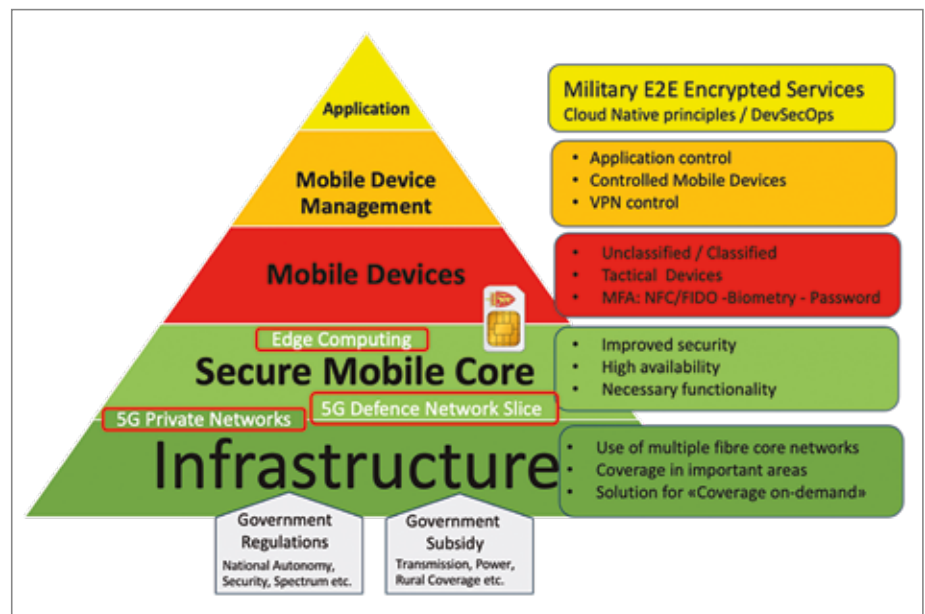
The figure illustrates how military and public traffic is separated by network slicing

need to collaborate in the public safety context is more crucial than ever. With the use of 5G networks, collaboration between public protection and disaster relief agencies and the Norwegian Defence will be easier.

To secure high availability of the public mobile networks, the Norwegian government provides funding to ensure robust transmission, power-supply and 5G coverage also in rural areas. In the future an increasing part of the critical communication in the society will traverse public 5G networks. In 2023 the area coverage of public 5G networks in Norway will reach 90%.

Conclusion

5G provides many advantages over previous generations and we will soon see use of 5G also in military organizations. The 5G projects 5G-VINNI and FUDGE 5G are giving the Norwegian Defence a unique insight in the 5G possibilities and limitations. The main focus for the Norwegian Defence at the moment is to create a target architecture where network slicing, edge computing and private 5G networks will be part of the solution to secure the mobile value chain. Securing 5G for military use will be a continuous work that will never end so that a long-term collaboration with the private commercial stakeholders endures long into the future.



Securing 5G for military use is complex and it requires competence in many areas

Further information

5G-VINNI project - <https://www.5g-vinni.eu>

FUDGE-5G project - <https://fudge-5g.eu>

Security threats and strategies for 5G and Beyond

Interview with cybersecurity experts from ENISA

The changing threat landscape has impacts on security and trust of current and future networks in Europe and worldwide. Eurescom message editor-in-chief Milon Gupta asked three cybersecurity experts from ENISA, the EU Agency for Cybersecurity, about the status, trends and strategies to deal with security threats: Goran Milenkovic is cybersecurity expert in the Policy Development and Implementation unit of ENISA, and he is primarily responsible for the telecom sector and for 5G security; Marnix Dekker leads the work of the Agency in the area of telecom security, cybersecurity breach reporting, and the security of cloud and digital infrastructure under the NIS Directive; and Apostolos Malatras, is Team Leader of ENISA's Knowledge and Information Team, in charge of the cybersecurity of emerging technologies, threat landscapes and foresight.

What are the major threats for current mobile networks including 5G?

Goran Milenkovic: Most of the major incidents coming out of the EU-wide incident reporting process are software bugs and hardware failures. Additionally, because a mobile network is a large, partly underground partly above-ground ICT infrastructure, there is exposure to natural phenomena, cable cuts, power cuts and battery theft. 5G networks will have even more complex software, featuring machine learning, edge computing, network function virtualisation, and rely on cloud services for the core network and outsourcing. Therefore, it will be a challenge for telecom providers to manage the new 5G technology and keep it secure. ENISA has worked over the last couple of years on 5G threat assessment and mapping the relevant landscape.

How will the growth of Cloud and IoT usage change the threat landscape in the next years?

Marnix Dekker: With IoT and 5G we are witnessing a diffusion of computing, shifting from traditional centralised cloud architecture to the edge and closer to the end users. 5G also changes how critical network functions are being imple-



Goran Milenkovic



Marnix Dekker



Apostolos Malatras

mented and deployed. Besides numerous technical security aspects that have to be considered, this shift means providers will have to rely on suppliers, but also additional players, like cloud service providers and system integrators. Overall the network setup will be more complex and there will be more dependencies, more outsourcing and a more complex supply chain landscape. At the same time there will also be changes on the side of the subscribers and the devices they connect to the networks with the arrival of IoT. These new IoT devices connected to the mobile networks will bring new risks for the availability and resilience of the networks.

How will the changing threat landscape impact security and trust of 5G and beyond networks?

Apostolos Malatras: The threat landscape is always changing. As we have seen recently, attacks by nation-state actors are a growing concern, especially for telecom providers. And novel technologies such as 5G also involve new risks and threats, but it is important to underline that 5G also brings important benefits, including several security improvements, like better encryption and better authentication. At the moment, the technical specifications are still being developed and a lot will depend on how they will be built into products and used by the operators. And that is not always as straightforward as it may seem. And let's not forget complexity. Complexity is the enemy of security and in the case of 5G networks this is perhaps more evident than ever. One of the key risks identified in the EU coordinated risk assessment for 5G is the lack of cybersecurity skills and expert personnel on the side of the providers, to deploy 5G networks securely.

What will be the impact of technological dependence and efforts toward technological sovereignty on security and trust in the European 5G and beyond domain?

Goran Milenkovic: Indeed, 5G not only brings more technological complexity, it also changes the overall ecosystem and the telecom supply chains. There will be many new players, integrators, managed service providers, software vendors, etc. Because mobile networks are so critical for society, it is important to consider the different technology dependencies in order to avoid the risks of relying on one single supplier for our network equipment. The 5G cybersecurity toolbox includes specific measures and concrete recommendations to mitigate such risks, both at national level as well as at EU level by stepping up efforts for maintaining a diverse and sustainable 5G supply chain, and further strengthening EU capacities to develop 5G and post-5G technologies.

Which elements of the EU cybersecurity strategy should be implemented with priority?

Marnix Dekker: The EU cybersecurity strategy announced in December 2020 is a broad package containing new Commission initiatives, legislative proposals and also funding to secure Europe's digital market in the near future. It contains for example a proposal for a revised NIS Directive, called NIS2, which will cover also the telecom sector. The strategy also explains the next steps on cybersecurity of 5G. It is not easy to pick some of these elements over others, but one of these worth mentioning is the issue of supply chain security, which is the subject of a growing concern, as we saw with the recent SolarWinds case.

New EU Cybersecurity Strategy

The new EU cybersecurity strategy was presented in December 2020. It contains concrete proposals for regulatory, investment and policy initiatives, in three areas of EU action: 1. Resilience, technological sovereignty and leadership; 2. Building operational capacity to prevent, deter and respond; and 3. Advancing a global and open cyberspace through increased cooperation.

Under the new EU cybersecurity strategy, Member States, with the support of the Commission and ENISA, are encouraged to complete the implementation of the EU 5G Toolbox, a comprehensive risk-based approach for the security of 5G and future generations of networks.

Further information

https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391

SolarWinds Case

In spring 2020, SolarWinds, a major US information technology firm, was the subject of a cyberattack that spread to its clients and went undetected for months. Hackers had secretly broken into SolarWind's systems and added malicious code into the company's network management system, a software



called "Orion" that monitors the various components in the networks of its 33,000 customers. In December 2020, The Washington Post reported that the IT systems of several government agencies were breached via the Orion software. Russian hacker group Cozy Bear, which is said to be working for the Russian Foreign Intelligence Service, was reported to be behind the attack. In January 2021, CRN reported that the attack could cost cyber insurance firms at least \$90 million.

The SolarWinds case showed an advanced level of sophistication and the kind of impact cyberattacks on supply chains can have. According to ENISA, supply chain attacks are constantly increasing their presence in the threat landscape and will require a step-up in defenses, also in Europe. The EU 5G Toolbox has a specific focus on supply chain security, and it is also an important focus area in the new EU cybersecurity strategy.

CELTIC News 1/2021

The newsletter of EUREKA Cluster CELTIC-NEXT

CELTIC Chair's Corner
The Eureka Clusters Programme

Events
AI-NET Kick-Off Event

Public Authority Profile
Spanish Centre for the Development of
Industrial Technology – CDTI

Table of Contents

CELTIC Chair's Corner

The Eureka Clusters Programme – A New Era of Joint Thematic Calls 3

Events

AI-NET Kick-Off Event – CELTIC Flagship Project for Intelligent Network Automation 4

Public Authority Profile

Supporting the Telecommunications Area in Spain through CELTIC-NEXT – Centre for the Development of Industrial Technology (CDTI) 6

Project Highlights

5G-PERFECTA – 5G and next generation mobile performance compliance testing assurance 8

Update from the CELTIC Office

Relaunch of CELTIC-NEXT in revised Eureka Clusters Programme 10

High number of proposals in Eureka Clusters AI Call 2021 11

6 new projects received CELTIC-NEXT label 11

IMPRINT

CELTIC Office
Xavier Priem
CELTIC Office Director
c/o Eurescom GmbH
Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989 381
Email: office@celticnext.eu



Join the Industry-Driven Research Programme for a Smart Connected World

CELTIC-NEXT Call for Project Proposals – Deadline: 22nd November 2021

Do not miss the opportunity to participate in CELTIC-NEXT, the industry-driven European ICT and telecommunications research programme under the umbrella of EUREKA. Submission deadline for the next call for project proposals is 22nd November 2021.

CELTIC-NEXT projects are collaborative private-public partnership R&D projects. All EUREKA member countries and associated countries can financially support them. More information on public funding and national contacts per country can be found on the CELTIC-NEXT Public Authorities Website. Please talk to your national contact early in the process.

Easy proposal process

Preparing and submitting a CELTIC-NEXT project proposal is easy. Just register on the CELTIC-NEXT online proposal tool, fill in the Web forms, and upload your proposal in pdf. Access to the proposal tool and to a proposal template is available via our Call Information page (<https://www.celticnext.eu/call-information>).

Benefits of participating in CELTIC-NEXT

- You are free to define your project proposal according to your own research interests and priorities.
- Your proposal is not bound by any call texts, as long as it is within the ICT/ telecommunications area – see CELTIC-NEXT Scope and Research Areas.
- CELTIC-NEXT projects are close to the market and have a track record of exploiting their results soon after the end of the project.
- High-quality proposals have an excellent chance of receiving funding, with an average success rate higher than 50 %.
- The results of the evaluation will already be known in January 2022.

If you have any questions or need help, do not hesitate to contact us; we are pleased to help you.

Contact:

CELTIC-NEXT Office
office@celticnext.eu
Xavier Priem
priem@celticnext.eu
Website: www.celticnext.eu



The Eureka Clusters Programme – A New Era of Joint Thematic Calls



Jari Lehmusvuori
Nokia, CELTIC-NEXT Vice-Chair
jari.lehmusvuori@nokia.com

Many steps have been taken and many milestones reached in 2021 both in CELTIC-NEXT and jointly with the other Eureka Clusters. We are experiencing an inspiring time of both facilitating the well-known industry innovation projects, as well as planning the new Eureka Clusters Programme (ECP) jointly with the other innovation Clusters in Eureka. With the launch of the ECP in the 2nd half of 2021 a new era with both the bottom-up Calls and thematic Calls will be available as opportunities for the innovations on the next generation communications in the CELTIC-NEXT community. Therefore, it is worthwhile here to summarize the baselines as an early introduction.

The traditional CELTIC bottom-up calls in spring and autumn are not affected by the additional ECP processes. The Joint Thematic Calls under the ECP's Multi-Annual Programme (MAP) are additional commitments from both Public Authorities and Clusters to work together on common and cross-Cluster topics. The current CELTIC-NEXT projects are performing well, and as a highlight, the new CELTIC-NEXT Flagship project AI-NET is now also up and running.

Thematic joint project calls by Eureka Clusters Programme

The planning and organization of the Eureka Clusters Programme (ECP) started in October 2020. It has continued under the lead of Eureka and with a strong contribution by the CELTIC Office. While not yet approved, the first call for projects may be introduced in late 2021 with a closing date in spring 2022. The ECP Calls follow the concept of joint calls of multiple Clusters, which enables widening the scope and competences available to a project.

Each of the Calls have a theme agreed between the industry and the funding Public Authorities of the countries. The ECP provides project opportunities to both large companies and small and medium-sized companies, and the public authorities funding according to their national policies. Each of the supporting countries assign an indicative and viable budget outlook for a thematic Call which, among the other new features, will provide improved predictability on funding. In addition, the schedule of funding decisions from idea to start is the goal. All these main features of the thematic joint calls of ECP make them a new innovations project instrument to the CELTIC-NEXT industry community, which is complementary to the single-Cluster bottom-up calls.

Celtic-Next in the ECP

The Multi Annual Plan (MAP) sets out the commitments of the public authorities and the Eureka Clusters. They jointly determine which RDI communities can be integrated in the MAP as Eureka Clusters, what the expected funding level will be, and what potential thematic areas for collaboration are. Each RDI community wishing to join the ECP applies for a period of 4 years to operate as a EUREKA Cluster. CELTIC-NEXT as such a community has submitted the application to Eureka as of 1st July 2021. Being a part of this ECP MAP approval process it has enabled us to update our CELTIC-NEXT Roadmap together with the MAP. As a Eureka Cluster the communications industry community of CELTIC-NEXT will have the opportunity for the future thematic joint calls that set out the challenges of sustainability and autonomous mobility as examples. The themes and a description of the calls to be launched in the coming year, including the budget commitments of the participating Eureka countries are given on the Annual Operational Plan of ECP.

Eureka Clusters AI Call 2021

As a preliminary step towards the joint calls, the Eureka Clusters AI Call 2021, to which CELTIC-NEXT substantially contributed, was organised with a submission deadline of 28 June 2021. This is an opportunity for the companies in the communications area to set up cross-innovation projects with a large network of organizations in the area of Artificial Intelligence with flexibility in the topics.

Celtic-Next Autumn 2021 Call

CELTIC-NEXT is continuing as the communications and applications Cluster in Eureka. The Celtic Autumn Call 2021 will be launched with the submission date in November 2021. It is a bottom-up Call with flexibility in the scope for the projects. Proposals for new innovations projects are welcomed. A brokerage event is foreseen for pitching of project ideas and partnering.

Celtic-Next Flagship project AI-NET

The new industry-led CELTIC-NEXT Flagship project AI-NET (Accelerating Digital Transformation in Europe by Intelligent NETWORK Automation) started in mid-2020. It is targeting automated resilient networks for economy and society. The project brings together partners from seven European countries and three fields of technology: Communications Networks and Technologies for 5G and Beyond, Near-Use Data Centers, and Artificial Intelligence (AI). Novel solutions for network automation are expected in the forthcoming two years.

Change in the CELTIC-NEXT Management Team

Xavier Priem has started as the new CELTIC Office Director. He has a strong track-record, both in innovation management and business development, thus providing an excellent background for industry innovations. Please join me in welcoming Xavier to the lead in the times of new challenges. He took over from Peter Herrmann, who retired in spring after having dedicated 15 years to CELTIC. As the CELTIC Office Director since 2014 he relentlessly drove the Cluster for the benefit of the European telecommunications industry innovations. Please join me in thanking Peter.

AI-NET Kick-Off Event

CELTIC Flagship Project for Intelligent Network Automation



Milon Gupta
CELTIC Office
office@celticnext.eu



Prof. Dr.-Ing. Ina Schieferdecker, Director-General for Research for Digitalization and Innovation at the German Federal Ministry of Education and Research (BMBF)



Darja Isaksson, Director General at Vinnova, Sweden's Innovation Agency

On 1st June 2021, CELTIC flagship project AI-NET was officially launched at a high-level online event. Representatives from the public authorities of Germany, Sweden and Finland as well as representatives of the AI-NET project consortium, comprising major players from industry (large and SMEs), research organisations, and academia, presented the visions and goals of the ambitious European project to an audience of more than 150 participants.

AI-NET aims at 'Accelerating Digital Transformation in Europe with Intelligent Network Automation'. The project is addressing the

challenge that the current centralised cloud infrastructure is not adequate for serving the requirements of the digital transformation in Europe. AI-NET is built on the premise that three technologies need to be combined to shape a new secure service and application platform: 5G, edge-centric computing, and artificial intelligence.

The main goal of the AI-NET project is to provide enablers and solutions for high-performance services deployed and operated at the network edge. AI-NET is using artificial

intelligence for complementing traditional optimisation algorithms, in order to manage vastly increased network complexity.

The kick-off event was opened by Prof. Dr.-Ing. Ina Schieferdecker, Director-General for Research for Digitalization and Innovation at the German Federal Ministry of Education and Research (BMBF). She said: "AI-NET is an important step for Germany and Europe towards technological sovereignty."



Milon Gupta - Eur... Celtic Meetings Dominik Flick [Fraunhofer] Jan Ja... Viewing David's screen

Towards a Solution for European Data Sovereignty

- **GAIA-X** for a European federated data infrastructure.
- **International Data Spaces** for secure, controlled and trustworthy data exchange across the federation.
- **AI-NET** provides the communication technology supporting low latency and European rules.

Next step:

- **Distributed Multi-Provider Cloud Edge Continuum (IPCEI-CIS).**

The diagram illustrates the Data Ecosystem and Infrastructure Ecosystem. The Data Ecosystem is centered around Data Providers, Data Consumers, and Data Sharing. It includes components like DAPS, Identity Provider, Federated Catalogue, Broker Service Provider, Vocabulary Provider, Data Processing or Storage Service, and Data Sharing. The Infrastructure Ecosystem includes Nodes, Interconnect, and various providers like Identity, Federated Catalogue, Broker Service, Vocabulary, Compliance, and Certification Body.

Fraunhofer ISST

Presentation by Prof. Dr. Jan Jürjens from Fraunhofer ISST

In the following presentations, the representatives of the funding agencies from Sweden and Finland – Darja Isaksson, Director General at Vinnova, Sweden's Innovation Agency, and Heikki Uusi-Honko, Head of International Networks at Business Finland – shared their views on the importance of AI-NET from the perspective of their national innovation strategies. While Ms Isaksson pointed out that "AI-NET is a cornerstone in Vinnova's strategy for digital transformation", Mr Uusi-Honko highlighted the importance of AI-NET for contributing to sustainable growth in Europe. CELTIC-NEXT Vice Chair Jari Lehmusvuori, Head of Department at Nokia Bell Labs, completed the session by presenting the European innovation perspective of Eureka Cluster CELTIC-NEXT.

The next session was dedicated to presenting the AI-NET sub-projects AI-NET-ANILARA, led by Ericsson Research, AI-NET-PROTECT, led by ADVA, and AI-NET-ANTILLAS, led by Nokia Bell-Labs. Magnus Frodigh, Vice President & Head of Ericsson Research, Sweden, Dr. Christoph Glingener, CTO ADVA Optical Networking, Germany, and Patricia Layec, Research Department Head, Nokia Bell-Labs, France, presented the ambition of AI-NET to connect critical in-

frastructures and data centres through enhanced transport networks and improved networking concepts that will result in reinforced overall security.

The event concluded with a panel discussion on how Europe can accelerate the digital transformation with intelligent network automation. Panelists in the session moderated by Eurescom Director and CELTIC Chairman David Kennedy were Dr. Mohsen Amiribesheli, Research Technology Manager at Konica Minolta Global R&D; Dr. Markus Ohlenforst, Managing Director at IconPro GmbH; Dominik Flick, Project Manager for Energy Performance Management at Stellantis / Opel Automobile GmbH; Dr. Timo Lehnigk-Emden, Managing Director at Creonic GmbH; and Prof. Dr. Jan Jürjens, Director Research Projects at Fraunhofer Institute for Software and Systems Engineering.

About AI-NET

AI-NET is a 74 million-euro public-private partnership project under CELTIC-NEXT, the EUREKA Cluster for next generation communications for a digital society. AI-NET comprises three sub-projects with 92 companies, research organisations, and universities from



Germany, Sweden, Finland, France, United Kingdom, Netherlands, and Poland. The CELTIC-NEXT flagship project is coordinated by ADVA Optical Networking SE, a European telecommunications vendor headquartered in Germany.

AI-NET is publicly co-funded by the public authorities of Germany (BMBF), Sweden (VINNOVA), Finland (Business Finland), and the United Kingdom (Innovate UK). The project will end in August 2024.

Further information

- AI-NET Kick-Off Event Page – <https://www.celticnext.eu/event/celtic-ai-net-kick-off-event/>
- AI-NET Project Page – <https://www.celticnext.eu/project-ai-net/>

Supporting the Telecommunications Area in Spain through CELTIC-NEXT

Centre for the Development of Industrial Technology (CDTI)



Juana Sánchez
CELTIC-NEXT representative
Centre for the Development of Industrial
Technology (CDTI)
juana.sanchez@cdti.es

The Centre for the Development of Industrial Technology is the main R&D funding agency in Spain.

CDTI is a public business entity, answering to the Ministry of Science and Innovation, which fosters the technological development and innovation of Spanish companies. It is the entity that channels the funding and support applications for national and international RDI projects of Spanish companies. Therefore, CDTI contributes to improving the technological level of the Spanish companies by means of implementing the following activities:

- › Financial and economic-technical assessment of R&D projects implemented by companies.
- › Managing and fostering Spanish participation in international technological cooperation programmes.
- › Fostering international business technology transfer and support services for technological innovation.
- › Supporting the setting up and consolidating of technological companies.

CDTI employs over 350 people, three quarters of whom are engineers and graduates. Even though the bulk of the CDTI infrastructure is in Madrid, the Centre offers to Spanish companies a strategic network of CDTI SOST (Spanish Office for Science and Technology) offices in ten countries: Belgium, Brazil, Chile, China, India, Japan, Korea, Mexico, Morocco and the USA to promote the Spanish technology at international level, mobilize global financial resources and detect international market opportunities for Spanish high-tech companies with the aim of fostering the transnational technological cooperation in International Programs at bilateral or multilateral level, with special focus in the European programs, like Horizon Europe or Eureka.

Commitment with Eureka and CELTIC-NEXT – new funding procedure implemented

Addressing its international orientation, CDTI has strong support with the Eureka programme in general and with Eureka Clusters in particular. The bottom-up orientation of Eureka is fully aligned with CDTI's philosophy. CELTIC-NEXT, focussed on the telecommunications area, has become a Eureka Cluster with high interest in Spain. The Spanish CELTIC community ranges from large companies to small and medium-sized companies that regularly participate in its calls to improve their competitiveness. The impact of Celtic projects encourages Spanish companies to use this way to accelerate their potential business establishment in the telecommunications area.

In order to accelerate the time to contract of CELTIC projects, CDTI has a new funding procedure that forces Spanish companies to apply for funding as soon as Celtic projects are labelled. Spanish funding application is done in two phases: First, the leader of the Spanish sub-consortium applies a 'Eureka request' after the deadline of each CELTIC-NEXT call (margin: 15 days). Second, once the projects are labelled, each company involved in la-



CDTI premises in Madrid





E3 medical test video sequence

belled projects presents the full memory (national request) with a margin of 20 days. This improved process will avoid long-term funding procedures for CELTIC projects and will shorten time-to-contract.

Successful Spanish CELTIC project E3

The E3 project is a good example of CELTIC success based on three principles: OPEN platform that guarantees access EVERYWHERE for EVERYBODY. E3 has designed, implemented, tested and validated with final users (patients and professionals) an E2E (End-To-End) video-

conference platform able to allow EVERYBODY (low-cost high-quality video conference & e-health services reusing in-home infrastructures) access to e-health services EVERYWHERE (both rural & urban areas, both patients and professionals) thanks to bandwidth adaptation techniques that allow simultaneous multipoint conferences with SD and HD.

These developments were tested and validated by doctors in 15 use cases over one common OPEN platform (adapted to point-to-point videoconferences and STB/HDTV functionalities), able to reuse in-home infrastructure (professional-to-patient scenarios and patient-to-patient scenarios).

E3 is a cross-domain project that uses Open Innovation to allow external partners (6 Spanish SMEs, 1 Polish SME, 1 Polish medical institution and 3 French medical institutions) to collaborate from project definition to test and validation easing go-to-market fit that has allowed to generate 12 new products and improve 14 products generating over 26.5 million euro revenue with 5.2X ROI since end 2020.

The main impact on Spanish partners has been on CALBOQUER SL (ASMEDIT) which launched Face-to-face+E3 developed solution to its 10 million customers with a 3 million euro revenue yearly increase. ASMEDIT is using STARFLOW (CLEVERNET) WAN Optimization solution to guarantee its professionals working from home connectivity, reliability and data in motion security.

Three start-ups have been created to commercialize E3 project developments, including SMART Health TV solutions in Spain which is participating in the ESA Space COVID19 Response Initiative as provider of tele-care technology for CNR (Consiglio Nazionale delle Ricerche).



E3 project: User-friendly experience / Videoconference at Home TV

The E3 project has received 8 awards including: CELTIC-NEXT Innovation Award Winner (Heidelberg, 2020), EUREKA Excellence Award Winner (EUREKA Stakeholders Conference Amsterdam, 2019) and CELTIC-NEXT Excellence Award Winner (CELTIC-NEXT Event at EuCNC in Valencia, 2019).

Conclusion

CELTIC-NEXT is a strategic Eureka Cluster for Spanish companies that offers an excellent framework to improve their competitiveness in the telecommunications area at interna-

tional level. Spain has many successful projects that have helped companies to establish as a reference in such competitive markets. CELTIC's support is key for participants. Besides, its Core Group offers high level orientation to participants.

CDTI, aligned with CELTIC-NEXT and with Eureka Clusters in general, has optimized the funding procedure with CELTIC calls to accelerate the time-to-contract of CELTIC projects. This new procedure has already been implemented in the CELTIC-NEXT Spring Call 2021.

> Further information

- > CDTI website – <https://www.cdti.es>
- > E3 project page – <https://www.celticnext.eu/project-e3/>

5G-PERFECTA

5G and next generation mobile performance compliance testing assurance



Antonio Cuadra-Sánchez
Indra Minsait
acuadra@minsait.com

ity of 5G networks is aligned with the expectations of bandwidth, latency and other key performance indicators. A series of innovation activities have been settled in order to establish a reference architecture for supervising 5G networks by means of monitoring techniques that measure 5G performance indicators to evaluate the real performance of 5G networks. The consortium, led by Indra Minsait, gathers 16 partners from Industry & Telco, Research Centers, Academia and SMEs of Poland, Portugal, Spain, Sweden, and Turkey.

user data rate and End-to-End latency of < 1ms. This new high-performance network needs to be effectively tested to assure that 5G technology is actually offered with high quality levels. For this purpose, we have developed a 5G performance compliance testing assurance solution that calculates KPI (Key Performance Indicators) to show the real behavior of 5G network and services. In addition, we have developed automated processes, tools and mechanisms ensuring 5G service quality, based on data processing and analytics approaches.

The 5G-PERFECTA project has developed a 5G performance compliance testing assurance solution that measures the KPIs to show the real behavior of 5G network and services.

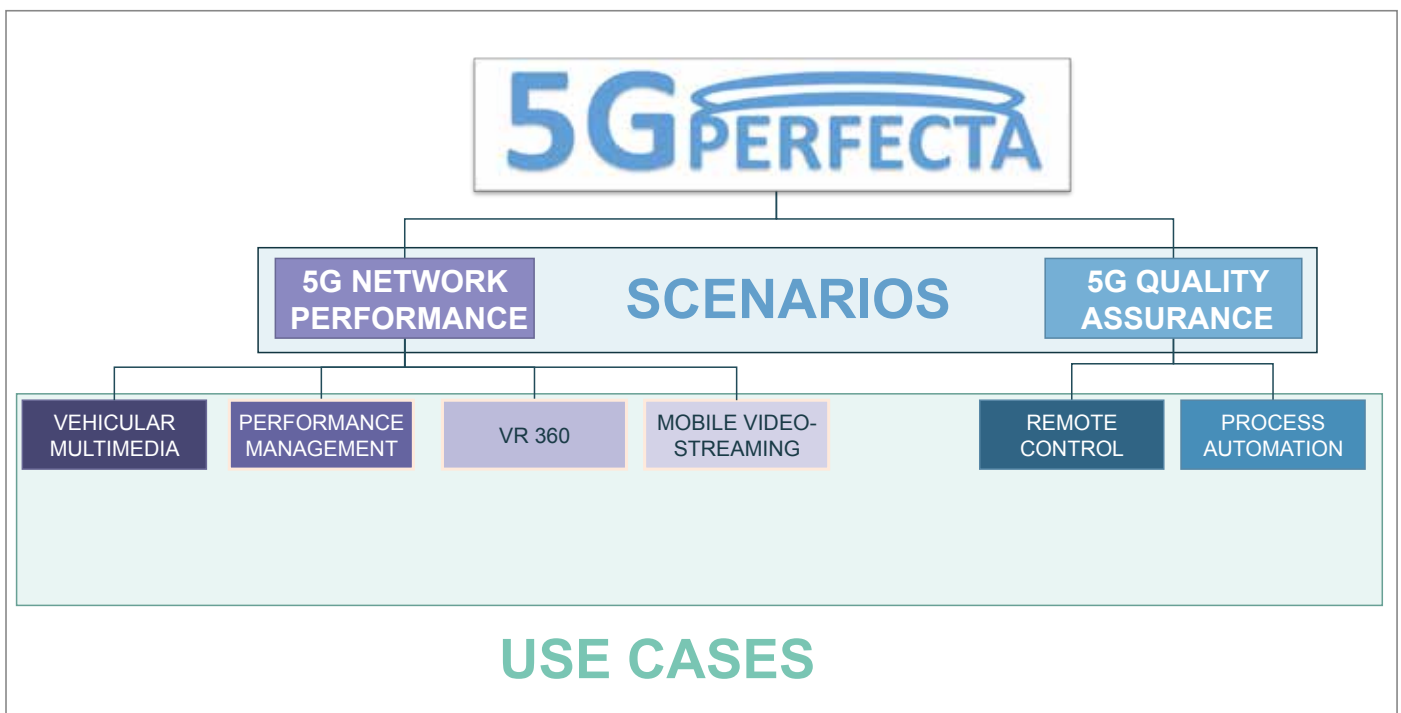
The challenge of CELTIC-NEXT project 5G-PERFECTA has been to develop the technology to assure the 5G service quality based on data processing, that is, to guarantee that the qual-

Motivation

The 5G infrastructure will deliver solutions, architectures, technologies and standards for the ubiquitous 5G communication infrastructures of the next decade. The following parameters are indicative of the new network characteristics to be achieved at an operational level: 10 times to 100 times higher typical

Scenarios and use cases

We have defined two main project scenarios and six use cases. The 5G Network Performance scenario provides the performance monitoring information and includes the test-bed and measurement scope for 5G network performance analysis. The 5G Quality Assurance scenario provides the quality of service



5G-PERFECTA scenarios and use cases

monitoring information, including the time-sensitive networking mechanisms, the deployment of critical services with performance guarantees, and the QoS observability for 5G. See in figure 1 the project scenarios and use cases.

Impact

The 5G performance compliance testing assurance solution will help the digital providers (operators, service providers, applications providers, etc.) to evaluate how next generation services are performed on the 5G networks for different purposes: measuring of 5G network performance, validating the services on 5G networks, monitoring the QoS and QoE, launching of new applications, etc. In addition, there is a very strong focus on end users in 5G PERFECTA, since they are the ones who really benefit from the correct behaviour of the 5G network. For this purpose, we have considered the end-user perspective in the analysis of the performance of services on 5G networks.

Conclusion

The project will provide capabilities that improve efficiency in content delivery by means of user-oriented quality assurance capabilities, which will be able to impact a significant part of the 5G revenues expected for the following years. The outcomes of this project will allow network and service providers to deploy the right 5G infrastructure to run the most advanced video technology business cases before final 5G standardization is complete.

5G-PERFECTA will provide a monitoring platform that delivers real measurements of several new feasible services over the new generation networks, including beyond 4G and the 5G network, tested on a real infrastructure. These performance indicators will allow to determine the suitability of new mobile infrastructures, including 5G to support next generation applications in mobility, such as remote driving, medical care, logistics, retail, Smart Cities, Industry 4.0, etc.

You can find more information on 5G-PERFECTA at <https://www.celticnext.eu/project-5g-perfecta/>.

Public Authorities

This project has been co-funded in Spain by the Centro para el Desarrollo Tecnológico Industrial (CDTI), in Sweden by Vinnova, in Portugal by Portugal 2020, in Poland by Narodowe Centrum Badań i Rozwoju and in Turkey by Tübitak.

Relaunch of CELTIC-NEXT in revised Eureka Clusters Programme

Ambitious roadmap for 2021 – 2025



Xavier Priem
Director CELTIC Office
priem@celticnext.eu

CELTIC-NEXT has been relaunched with a new, ambitious roadmap as part of the revised Eureka Clusters Programme. The relaunch is very timely in a world of dramatic change that requires novel ICT solutions addressing the economic, societal, and environmental challenges the Eureka member states and the world as a whole are facing.

The revised Eureka Clusters Programme

The CELTIC-NEXT Cluster application for the four-year period 2021-2025 was accepted, together with the Multi-Annual Plan for the Eureka Clusters, on 18th June 2021. This concluded a relaunch process that had started in June 2020. The new Eureka Clusters model is meant to encourage industry-wide collaboration and the forming of new innovation ecosystems. The revised Eureka Clusters Programme aims to align and synchronise the Clusters' processes.

Since June 2020, the Eureka Clusters had already intensified their joint and synchronised activities, most visibly through two jointly organised AI calls in 2020 and 2021, which both mobilised a substantial number of excellent project proposals.

Updated CELTIC-NEXT roadmap for 2021 – 2025

The theme of CELTIC-NEXT for the new period is: "Next-Generation Communications for a secured, trusted, and sustainable digital society". All topics identified in the strategic roadmap of CELTIC-NEXT for the 2021-2025 period have been aligned under this theme. These topics are neither comprehensive nor prescriptive. In line with the bottom-up approach of CELTIC-NEXT, projects are free to explore



Topical areas of the CELTIC-NEXT Roadmap 2021-2025

any subject, as long as it is related to ICT and telecommunications.

A core part of the roadmap relates to the evolution of communication networks. The roadmap identifies the ongoing digitisation and automation of many aspects of our lives as fundamental drivers for transforming the communications network architecture and functionality. The shift to automation of everything is driven by current enabling technology trends like cloud-based services with dynamic, adaptive scaling, extensive virtualisation, novel software-defined automated solutions and ever-increasing wireless connectivity with a great promise of 5G, Beyond 5G, and the nascent 6G, and will require a redefinition of networking concepts and a new digital infrastructure involving radical shifts in technologies, architectures and business models to meet future digital needs.

The roadmap highlights a number of important trends and requirements expected to shape the projects and results of the CELTIC-NEXT Cluster in the coming years, including: pervasiveness, almost infinite network capacity, imperceptible latency, tera-scale things, cognitive operations, and perpetual protection.

Addressing the digital needs will require significant changes in network architecture and technology. Nine dimensions are identified in the roadmap towards an end-to-end convergent network architecture: 1. Massive-scale access, 2. Converged edge cloud, 3. Smart network fabric, 4. Universal adaptive core, 5. Programmable network operating system, 6. Network slicing, 7. Augmented cognition systems, 8. Digital value platforms, and 9. Dynamic data security.

Further related areas of the roadmap beyond communication networks in the narrow sense include: cybersecurity, artificial intelligence and big data, ICT solutions for sustainability, ICT-enabled health and wellness, new solutions for consumption and production, smart cities and smart territories, smart transport, smart energy, smart agriculture, smart home and smart building, digital enterprise and digital education, content, entertainment and gaming, fintech, and digital life services.

Many of the topics identified in the roadmap go across several Eureka Clusters, which is intentional, as ICT is at the core of innovation in all vertical sectors. In line with the concept of the revised Cluster Programme, CELTIC-NEXT will use these cross-Cluster topics as opportunities for creating synergies and increasing

impact across the whole programme. Only in this way can CELTIC-NEXT and the other Clusters in the programme continue delivering top-level industry-driven innovations addressing the needs of economy, society and environment. In line with this cross-Cluster collaboration spirit, CELTIC-NEXT is one of three Core Technologies Clusters, together with partner Clusters ITEA (software) and Xecs (hardware). As a Pillar Cluster, CELTIC-NEXT supports the two more application-based Clusters EUROGIA2020 (low-carbon energy technologies) and SMART (manufacturing).

Excellence targets

CELTIC-NEXT has defined a set of excellence targets in order to keep its activities focused on achieving substantial measurable impacts. These targets are divided into three areas:

1. Technical excellence targets

- › Accelerate the deployment and take-up of new advanced end-to-end ICT services, employing the new network concepts of 5G and leading to the implementation of 6G in Europe
- › Actively facilitate the adoption of those ICT technologies by all targeted Verticals into their communities, business models and processes

2. Economic excellence targets

- › Consolidate the position of European ICT manufacturers and service providers within Europe and on the global market
- › Contribute to all Eureka Communities tackling the technological and socio-economic challenges in a holistic way by considering the end-to-end perspective of new communications solutions

3. Societal and environmental excellence targets

- › Investigate where advanced communications can reduce carbon footprints for many vertical sectors
- › Assist European nations and industry to access the societal benefits and returns of being at the forefront of the new digital society
- › Consolidate the European sovereignty in ICT technologies and services as well as other critical infrastructures relying on ICT infrastructures, like the Energy Grid

These targets are highly ambitious and require close collaboration between the private and the public sector. The revised Eureka Clusters Programme provides the structure and the ecosystem to achieve them.

High number of proposals in Eureka Clusters AI Call 2021



The second Eureka Clusters AI Call, which was launched on 1st March, has attracted a high number of project proposals. By the deadline of 28th June, 43 proposals had been submitted. These proposals represent a total commitment of 2,518 person years by international researchers and developers from large enterprises, SMEs, research & technology organisations, and academia.

The aim of this Call is to boost the productivity and competitiveness of European industries through the adoption and use of AI systems and services. 14 Eureka countries have allocated budget to support ground-breaking Artificial Intelligence innovations. The Call has been jointly organised by the following Eureka Clusters: CELTIC-NEXT, EUROGIA, ITEA, PENTA-EURIPIDES, and SMART. For 9 of the submitted proposals, CELTIC-NEXT has been selected as the primary Cluster. For 6 additional proposals, CELTIC-NEXT has been selected as the secondary Cluster. This means that CELTIC-NEXT has been selected in more than a third of the proposals among the 5 Clusters.

The proposals are now being evaluated. Results are expected to be known by the end of September.

› Further information

Eureka Clusters AI Call website - <https://eureka-clusters-ai.eu>

6 new projects received CELTIC-NEXT label



In the CELTIC-NEXT Spring Call 2021, 10 validated proposals submitted by 12th April 2021 got selected in the evaluation process, and out of them 6 new projects received the CELTIC-NEXT label.

The labelled projects are now eligible for funding by the project partners' national funding bodies.

The consortia of the six projects include a total number of 76 partner organisations from 12 countries, ranging from leading industry players to SMEs and academic institutions.

The six projects include the following topics:

- › 6G for Connected Sky
- › Massive IoT over High Density LoRaWAN Networks
- › Ultra Scalable Wireless Access
- › AI-Powered Communication for Health Crisis Management
- › Federated AI Platform for Industrial Technologies
- › Cloud-based Online Access to Computational Fluid Dynamic Simulations

As soon as the funding for the new projects is confirmed and they are ready to start, each of them will be presented on the CELTIC-NEXT website (www.celticnext.eu).



About CELTIC-NEXT

CELTIC-NEXT is the EUREKA Cluster for next-generation communications enabling the inclusive digital society. CELTIC-NEXT stimulates and orchestrates international collaborative projects in the Information and Communications Technology (ICT) domain. The CELTIC-NEXT programme includes a wide scope of ICT topics based on new high-performance communications networks supporting data-rich applications and advanced services, both in the ICT sector and across all vertical sectors.

CELTIC-NEXT is an industry-driven initiative, involving all the major ICT industry players as well as many SMEs, service providers, and research institutions. The CELTIC-NEXT activities are open to all organisations that share the CELTIC-NEXT vision of an inclusive digital society and are willing to collaborate to their own benefit, aligned with their national priorities, to advance the development and uptake of advanced ICT solutions.

www.celticnext.eu



Demonstration of 5G end-to-end validation platform

Final 5G EVE webinar



Milon Gupta
Eurescom
gupta@eurescom.eu

In the final 5G EVE webinar on 26th May 2021, the project consortium presented the major achievements in the development and use of the 5G EVE validation platform to an audience of 60 participants. As a highlight, the 5G EVE team demonstrated live the multi-site capabilities of the platform.

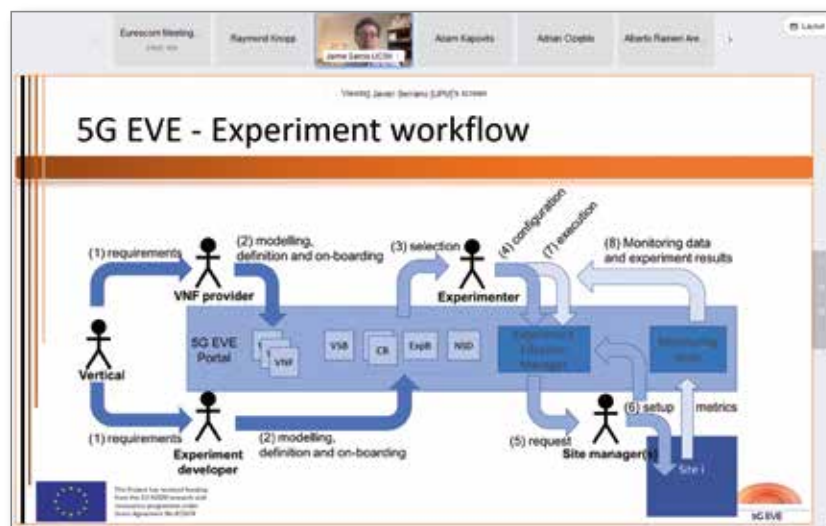
In addition, experts from the consortium presented new platform features like, for example, performance diagnostics, and demonstrated the 5G EVE gaming use case as an illustration of the multi-site capabilities of the 5G EVE platform.

In a short training session in the last part of the webinar, experts from the four 5G EVE sites shared practical knowledge on platform usage, which will be useful for the utilization of the platform beyond the duration of the project.

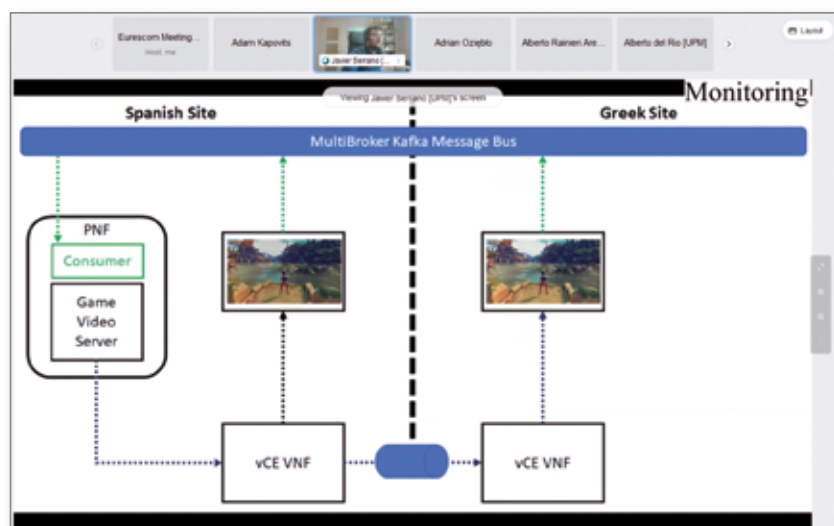
The webinar was particularly aimed at current and future 5G EVE platform users from 5G PPP use case projects and innovative SMEs, who would like to test and validate their 5G solutions in the most effective way.



Presentation of the 5G EVE multi-site gaming use case by Luis Contreras from Telefonica



5G EVE experiment work flow for vertical multi-site use cases, presented by Jaime Garcia-Reinoso, University Carlos III de Madrid



Demonstration of the 5G EVE multi-site gaming use by Javier Serrano from UPM



Demo of the 5G EVE performance diagnosis for vertical use cases by Yannis Chondroulis from Wings ICT

Further information

Slides and videos of the presentations are available on the webinar page – <https://www.5g-eve.eu/event/final-5g-eve-webinar-validation-platform-achievements-and-multi-site-use-case-deployment/>

On the Road to 6G

Joint EuCNC & 6G Summit



Milon Gupta
Eurescom
gupta@eurescom.eu

The theme of the 2021 Joint EuCNC & 6G Summit from 8th to 11th June 2021 was “On the Road to 6G”. The event, which was originally planned to take place in Porto, Portugal, was held in virtual format, due to the COVID-19 pandemic. It included the conference as well as the exhibition.

The conference focused on a wide array of telecommunications aspects ranging from 5G deployment and mobile IoT to 6G exploration and future communications systems and networks, including experimentation and testbeds, and applications and services. The dominant topic in many sessions was 6G respectively Beyond 5G. However, many topics discussed were relevant for both 5G and 6G. This included particularly security.



Joint EuCNC & 6G Summit website

Workshop on Automated and Intelligent Security

On the first day of the event (8th June), the FAST workshop 'From 5G to 6G Automated and Intelligent Security', which was co-organised by 5G PPP project INSPIRE-5Gplus, addressed important cybersecurity risks.

Experts from a number of EC projects and a keynote speaker from IEEE explored innovative concepts for security management of 5G networks and beyond from a holistic high-level architecture perspective. Crucial topics discussed at the workshop for reaching a fully-automated and secured 5G infrastructure included the adoption of a set of emerging trends and technologies, namely, Zero-touch network and Service Management (ZSM), Software-Defined Security (SDSec) models, Artificial Intelligence/Machine Learning (AI/ML) techniques, Distributed Ledger Technologies (DLT), Zero Trust models, and Trusted Execution Environments (TEE).

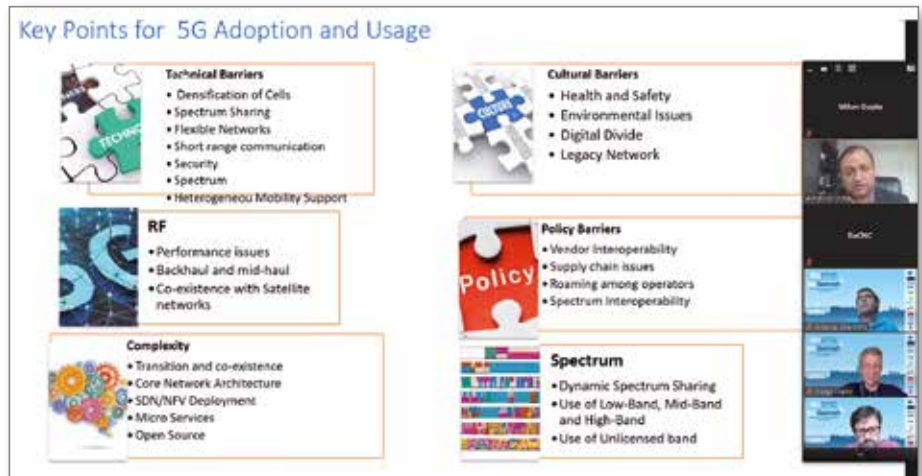
The workshop was opened by Pascal Bisson from Thales and Antonio Skarmeta from University of Murcia. It was organized around a set of key thematic areas structured in four sessions, with the participation of 13 5G projects and a prominent keynote speaker.



Ashutosh Dutta, IEEE Communications Society Distinguished Lecturer & Co-Chair for IEEE Future Initiative

Session 1 was dedicated to 'Security and Trust Architecture for Beyond 5G Networks' and included presentations on related aspects, from the definition of a security management closed-loop to security and trust mechanisms and outlier detection for 5G security.

Session 2 explored 'Automated and Intelligent (smart) Security network management'. The presentations covered topics like 'ZSM Security Orchestration for Multi-Tenant 5G Networks', 'On-demand deployment of security services', 'Hardening Interdomain Vertical Services with Moving Target Defense', and 'Security Challenges on 5G CCAM Scenarios'.



Online presentation at the FAST workshop 'From 5G to 6G Automated and Intelligent Security'

In the keynote following this session, Ashutosh Dutta, IEEE Communications Society Distinguished Lecturer & Co-Chair for IEEE Future Initiative, presented key points to be considered for secure adoption and usage of 5G.



Session 3 discussed 'Security Beyond 5G Networks and Services'. It included presentations on 'Trustworthy Networking Beyond 5G' and 'Cloud-Scale SDN Network Security in TeraFlow'.

Session 4 finally explored 'Security Enablers for Beyond 5G Networks and Services'. The presentations covered topics ranging from 'Machine Learning Applied to 5G Network Cyber Range', 'Security and Trust in NetApp Deployment and Operation', '5G Embedded Trust', and 'Practical Autonomous Cyberhealth for Resilient Micro/Small/Medium-Sized Enterprises'.

The FAST workshop gave an excellent overview on the status of research on automated and intelligent security in 5G and highlighted the challenges on the road towards 6G.

Smart Networks and Services JU

In a workshop on the final day of the event (11th June 2021), the objectives and structure of the new European Joint Undertaking (JU) on Smart Networks and Services (SNS) were presented. The envisaged budget volume of the SNS JU is 900 million euro, according to a statement published on the 5G-IA website.

The goal of the SNS JU partnership will be to define and implement the research, innovation and deployment roadmaps that will enable Europe to take a leading role in the creation of the next generation of smart network technologies and services, also known as 6G.

The SNS JU partnership will focus on facilitating the full digitization of European society including vertical industries and public administration services. The 6G SNS solutions will be designed and implemented in such a way that European values like security and privacy are safeguarded, and that European technological sovereignty is further strengthened. The SNS Partnership targets to have a perceptible positive impact on the quality of life of European citizens and a noticeable boost in the European data economy by 2030.

Further information

Joint EuCNC & 6G Summit website –

<https://www.eucnc.eu>

FAST workshop page –

<https://www.eucnc.eu/workshops/workshop-8/>

SNS Partnership –

<https://5g-ia.eu/sns-horizon-europe>

Accountability and Liability for 5G and Beyond

INSPIRE-5Gplus workshop



Milon Gupta
Eurescom
gupta@eurescom.eu

On 16th June 2021, the INSPIRE-5Gplus project held a full-day online workshop on accountability and liability for 5G and beyond. It brought together more than 30 researchers and practitioners from several domains, including actuaries, lawyers, and researchers in networking and multi-agent systems. They presented challenges and approaches for liability management in multi-party 5G ecosystems and digital services, with a forward-looking perspective on Beyond 5G systems.

The main purpose of the workshop was to share, compare and disseminate best practices, approaches, tools and methodologies for identifying, formulating, and managing liability in 5G systems. The workshop addressed crucial topics such as formalization of commitments and obligations, contractualization, monitoring & supervision, evidence collection & analysis at runtime, as well as post-mortem evidence collection & forensics for identifying liabilities in case of disasters, security incidents, or regulation violations.

The workshop moderated by Gürkan Gür from Zurich University of Applied Sciences started in the morning with presentations by INSPIRE-5Gplus partners, covering topics from the Manufacturer Usage Description (MUD) standard and Liability-Aware Security Management (LASM) to Root Cause Analysis (RCA).

This was followed by presentations covering a variety of multi-disciplinary aspects. Sylvie Jonas from AGIL'IT Law explained how liability management based on contracts works in a 5G environment. Carmen Fernandez Gago from University of Málaga talked about accountability in the cloud. And Samia Bouzefrane from the National Conservatory of Arts and Crafts (Cnam), France presented a trust-based recommendation system.

In the afternoon session, Jacques Kruse-Brandao from SGS presented challenges, approaches and concepts for 5G device security certification.



Gürkan Gür (Host)



Sylvie Jonas

Arthur Van Der Wees from Arthur's Legal talked about trustworthy and accountable digital ecosystems. And Claire Loiseaux from Internet of Trust presented responsibilities and certification in cybersecurity space.

A round-table discussion with the speakers, moderated by Gürkan Gür, concluded the workshop. The panel discussed questions like: What is the major challenge for multi-party liability management? Who has to manage liability between parties? And what would be nice to have for multi-party liability management? While the speakers provided knowledgeable answers to these questions, many aspects of liability management require still plenty of research and multi-disciplinary discussion. In view of the growing economic and societal importance of 5G applications and services, finding technical, regulatory, and legal solutions for the topics highlighted at the workshop will be of high importance for the success of 5G and 6G.

Further information

Workshop page – <https://www.5g-eve.eu/event/final-5g-eve-webinar-validation-platform-achievements-and-multi-site-use-case-deployment/>

News in brief

European Green Digital Coalition established



On 19 March 2021, 26 CEOs of companies, including 13 European telecom CEOs, signed a declaration to support the Green and Digital Transformation of the EU. They formed the European Green Digital Coalition, committing on behalf of their companies to take action in the following areas:

- To invest in the development and deployment of greener digital technologies & services that are more energy and material efficient,
- Develop methods and tools to measure the net impact of green digital technologies on the environment and climate by joining forces with NGOs and relevant expert organisations, and
- Co-create with representatives of others sectors recommendations and guidelines for green digital transformation of these sectors that benefits environment, society and economy.

The European Green Digital Coalition will help not only the tech sector to become more sustainable, circular and a zero polluter, but also to support sustainability goals of other priority sectors such as energy, transport, agriculture, and construction while contributing to an innovative, inclusive and resilient society. Its members will work closely with the European Commission and others to deliver on their commitments and will report regularly on progress made. In 2022, the first available results and progress reports will be presented. 45 SMEs and startups support the European Green Digital Coalition, and many will take the sustainability commitments to join in the near future.

Further information

EC news release: <https://ec.europa.eu/digital-single-market/en/news/companies-take-action-support-green-and-digital-transformation-eu>
 Joint Statement by ETNO and the GSMA: <https://www.etno.eu/news/all-news/8-news/702-telcos-egdc.html>

Over 580 million 5G mobile subscriptions by the end of 2021

5G mobile subscriptions will exceed 580 million by the end of 2021, according to a projection by Ericsson. This trend is driven by an estimated one million new 5G mobile subscriptions every day.

The forecast from the latest edition of the Ericsson Mobility Report supports the expectation that 5G will become the fastest adopted mobile generation. About 3.5 billion 5G subscriptions and 60 percent 5G population coverage are forecast by the end of 2026.

However, the pace of adoption varies widely by region. Europe is off to a slower start and has continued to fall far behind China, the U.S., Korea, Japan and the Gulf Cooperation Council (GCC) markets in the pace of 5G deployments.

5G is expected to surpass a billion subscriptions two years ahead of the 4G LTE timeline for the same milestone. Key factors behind that include China's earlier commitment to 5G and the earlier availability and increasing affordability of commercial 5G devices. More than 300 5G smartphone models have already been announced or launched commercially.

This commercial 5G momentum is expected to continue in coming years, spurred by the enhanced role of connectivity as a key component of post-COVID-19 economic recovery.

North East Asia is expected to account for the largest share of 5G subscriptions by 2026, with an estimated 1.4 billion 5G subscriptions. While North American and GCC markets are expected to account for the highest 5G subscription penetration, with 5G mobile subscriptions comprising 84 percent and 73 percent of all regional mobile subscriptions respectively.

Data traffic continues to grow year on year. Global mobile data traffic – excluding traffic generated by fixed wireless access (FWA) – exceeded 49 exabyte (EB) per month at the end of 2020 and is projected to grow by a factor of close to 5 to reach 237 EB per month in 2026. One exabyte (EB) comprises one billion gigabytes (GB). Smartphones, which currently carry 95 percent of this traffic, are also consuming more data than ever. Globally, the average usage-per-smartphone now exceeds 10 GB/month and is forecast to reach 35 GB/month by the end of 2026.

The COVID-19 pandemic is accelerating digitalization and increasing the importance of – and the need for – reliable, high-speed mobile broadband connectivity. According to the latest report, almost nine out of ten communications service providers (CSPs) that have launched 5G also have a fixed wireless access (FWA) offering (4G and/or 5G), even in markets with high fiber penetration. This is needed to accommodate increasing FWA traffic, which the report forecasts to grow by a factor of seven to reach 64 EB in 2026.

Massive IoT technology (NB-IoT and Cat-M) connections are forecast to increase by almost 80 percent during 2021, reaching almost 330 million connections. In 2026, these technologies are forecast to comprise 46 percent of all cellular IoT connections.

Further information

Reference website: <https://www.ericsson.com/en/press-releases/2021/6/ericsson-mobility-report-more-than-half-a-billion-5g-subscriptions-by-the-end-of-2021>



© AdobeStock

The dark side of data

How data garbage hurts business and the environment



Milon Gupta
Eurescom
gupta@eurescom.eu

Everyone is talking about big data. There is indeed a large potential for extracting economic and societal value out of huge amounts of data. By feeding algorithms with data, machine learning could provide solutions to almost everything. So much about the bright side. However, in the shadows of the big data vision lurks a less pleasant reality: huge piles of data garbage, gazillions of data files lingering unused on servers around the world – dark data.

According to the “Databerg Report” published by information solution provider Veritas in 2015, organisations in Europe, the Middle East and Africa hold on average 14% of identifiable business critical data, 32% ROT (redundant, obsolete and trivial) data, and 54% dark data.

According to market research firm Gartner, dark data is defined as “the information assets organizations collect, process and store during regular business activities, but generally fail to use for other purposes.” These other, more productive purposes could be, for example, analytics, business relationships and direct monetisation.

How dark data is produced

The critical question is, how dark data comes into existence in the first place. There are various causes and reasons. One of the underlying enablers of dark data is that data storage is seemingly cheap and abundant. Thus, all data that could possibly be useful is stored, whether they are actually used or not. And once data is stored, there is usually nobody who cares about checking and reducing data amounts.

On the production side, there are many contributors. Organisations often retain dark data for compliance purposes only. That is ironic, as in some cases storing data could cause bigger compliance risk than benefits, just think of private data and the risks of violating data privacy regulations.



© AdobeStock

While in the past, dark data was mainly produced by humans, nowadays the biggest share of dark data is produced by machines, including information gathered by sensors and telematics. According to an estimate by IBM from 2015, roughly 90 % of data generated by sensors and analogue-to-digital conversions never get used. It is doubtful, whether this has improved in the last six years. I wouldn't be surprised, if it is even worse now.

Some organisations seem to believe that dark data could be useful to them in the future, once they have acquired better analytic and business intelligence technology to process the information. While this is theoretically possible, in practice I find it hard to believe that a lot of value will be generated in ten years from analysing dark data generated by humans and mostly machines today. Even if a small amount of today's dark data could be pure gold in ten years' time, the question is, whether it would be worth the problems dark data already creates today.

Why dark data is a problem

Given that cloud storage is cheap, the question is, why dark data should be a problem at all. The answer is in the huge scale of dark data. Once the amount of dark data exceeds a certain level, storage cost is no longer cheap. The “Databerg Report” from 2015 predicted that dark data could cause 891 billion dollars of avoidable stor-

age and management costs by 2020, if left unchecked. I have not seen any recent study on the amount and cost of dark data. However, I have a strong suspicion that the real cost might be even higher today.

As storing huge amounts of data consumes a lot of energy and material for the data centre infrastructure, there is not just a financial cost, but also an environmental cost in the shape of carbon-dioxide emissions.

One of the reasons why the problem persists and might actually grow over the coming years is that most companies probably have no idea about the volume and cost of dark data.

What can be done about dark data

In my view an important part of the solution can be derived from a famous quote by Lord Kelvin: “If you can not measure it, you can not improve it.” Applying these words of wisdom to dark data, you could say: if you can measure dark data, you can remove it. Even if removing dark data is not always the preferred solution, for example because of compliance needs or expected value to be derived in the future, it would be a good start to be aware of the scope of the problem and to know, which data on an organisation's server is dark. Maybe the machines that increasingly generate dark data could also help to remedy the problem through the use of machine learning in weeding out useless data.



Effective Tools for European Research Projects

EuresTools is a modular suite of Cloud-based software tools which facilitate controlling and reporting and enable distributed project teams to communicate and manage information effectively. Over 200 successful European research projects and initiatives have already benefited from **EuresTools**.

Contact us at services@eurescom.eu to get further information.

<http://www.eurescom.eu/EuresTools>



EURESCOM message

The magazine for telecom insiders

Get your free subscription of Eurescom message
at www.eurescom.eu/message

EURESCOM

European Institute for Research
and Strategic Studies
in Telecommunications GmbH
Wieblinger Weg 19/4
69123 Heidelberg, Germany
Phone: +49 6221 989-0
Fax: +49 6221 989 209
E-mail: info@eurescom.eu
Website: www.eurescom.eu

Innovation through Collaboration

Eurescom is the leading organisation for managing collaborative R&D in telecommunications. Our mission is to provide efficient management and support of R&D projects, programmes, and initiatives for our customers. We offer more than two decades of experience in managing large-scale, international R&D for major industry players, the European Commission, and EUREKA Cluster CELTIC-NEXT. What distinguishes Eurescom is the combination of a secure, reliable infrastructure for collaborative work, a large European network of experts, and internationally outstanding project management skills.



QR code to the
online edition of
Eurescom message