Future of Mobile Communications 2020+

On 26 June 2014, the TCCA and PSCE hosted a one-day seminar on the Future of Mobile Communications 2020+. The seminar was organised to facilitate a discussion on the future changes in the mobile communications society, and the consequences for the mission critical communications requirements of public safety organisations and critical infrastructure operators.

Event hosts were Manfred Blaha, Chair of the PSCE User Committee and Technology Advisor at the Austrian Ministry of Interior, and Hans Borgonjen, Vice-Chairman of the TCCA and Senior Coordinator, International Standardisation for National Police Netherlands.

The day was introduced by Manfred Blaha as a focus on future broadband for critical communications users – to get an idea from the users' perspective as to how communications will look from the year 2020 and beyond. We all know that communications will be faster, but we don't know much else. This event was designed to catalyse creativity in the user community, and to give attendees a glimpse into the crystal ball to see the shape of things to come in 2020 and beyond.

Presentations from visionary representatives from Airbus, Cisco, Extend Limits, Microsoft and Motorola Solutions were followed by a panel discussion.

Attendees were asked to note their thoughts on the key points made by each speaker, and this input is summarised in the Appendix.

First Presentation: The Internet of Things ... Beyond IT - Alain Fiocco, Senior Director, Cisco CTO office

We were born with IP. We're known for injecting IP in all markets, and creating new markets with IP as the DNA. For Cisco, the Internet of Things (IoT) is already a reality. The company is responsible for driving the new Internet address class IPv6. The current IPv4 defines an IP address as a 32-bit value, whereas IPv6 addresses have a size of 128 bits and consequently a much greater address space.

The IoT is about connecting everything that isn't a human being – getting access to data and actioning directly. Cisco is looking to the Internet of Everything – connection humans, data, things, processes.

Access control is in place in the home, but is difficult for networks, with Internet connectivity increasing in manufacturing, oil and gas, safety, security, defence, smart cities, and across the whole business infrastructure.

The key criteria are to make data truly real time – we talk about big data but it needs to be fast data – and to have pervasive security, of devices, people, policies and supply chain.

What will it take to achieve this? Operational technology network transformation: from basic connectivity to a critical part of the enterprise infrastructure; from proprietary standards to open standards, and from disparate networks to converged, secure and collaborative operations.

IPv6 is mandatory to the IoT because it enables scale and simplicity: linking addresses with types – so infrastructure, devices, services can be provisioned based on the address

Most IoT platforms are leveraging the cloud, there are not many proprietary technologies. The presentation shows a comparison between what it takes to establish a connection between an application and device using IPv4 and IPv6. The IPv6 connection is much 'flatter' – still creating a domain of responsibility but not having to create all the links in the chain.

Leveraging 3G/4G architecture and extending it can create an IP network for old and new devices to connect over any of the available bearers to the service provider – this could be a public packet core or a private one running in a particular location – but still interconnect with the public one.

So taking smart grids as an example – they could put electricity back in the grid as well as consuming. This is achievable using IPv6 and is deployed today.

With open standards there are a lot of different accesses, but most important is the common network layer at the application level. Open standards at all levels ensure interoperability and reduce technology risk for utilities.

The difference between big data and fast data is the processing of that data. The cloud assumes high speed always-on connection for fast processing, so there is a need for distributed computing to process data – below the cloud – it's 'fog' computing.

This is the IoT model – data centre cloud then fog computing then devices, and in the process providing an aggregate point

There must also be underlying security principles, as the IoT means managing tens of millions of devices. The Internet of Everything is about connecting the 50 billion smart devices expected by 2020.

But we need to finish the race to connect the human internet – to redefine end-to-end IPv6-centric networking, and use for new infrastructure going forward.

Q & A for Cisco:

Q: What about lawful interception in the IoT – what tools are you giving the authorities to do what they have to do?

A: All the IP networks today are providing lawful interception capabilities, allowing fixed and mobile to intercept based on IP addresses.

Q: Can you expand on the concept of fog computing – about having a lower layer?

A: We want to make computing power available at a lower level than the cloud/data centre – it's a mistake for devices to do their processing in the cloud.

So – network equipments also have computing capacity for customers to drop any applications – provide a 'guest' operating system – we just provide the apis for the network.

Q: My understanding of IPv6 is mainly to have guarantee for data provisioning from a to b – but you are focussing on huge number range?

A: Any packet and any destination has an address.

Second Presentation:

Microsoft, What's Next in Mobile and Cloud- Harald Leitenmuller, CTO, Microsoft Austria

Cloud first ←→ mobile first

We are about the prioritisation of the innovation process – so for cloud, some products are only 'shipped' in the cloud. Mobile impacts design and usability – we are looking to provide access to services to everyone on any device on any platform.

Microsoft presented the New World of Work – NWOW. The social trend is access to assets as a community. For business, the cloud is a sharing economy solution.

There is a change of demography in the working population of Europe, it is getting older – meaning there can be four different generations working together.

People are now measured by results and the business impact brought to the company. The individual owns the responsibility to design and achieve the results expected – it's a very different work environment and very flexible work environment.

How do we measure the impact of the NWOW – the balance between work and family life? If you are flexible you will work harder as you can work on your own terms.

What does cloud mean? It is an enabler of this new world of work.

- People: culture based on responsibility and trust
- Place – environment optimised for your individual and collaborative contribution
- Technology – need enabling technology for time and place
- Cloud is the enabler – something you can trust

Cloud economics is all about economies of scale. Wholesale is cheaper than retail. Demand aggregation, across time zone, multi tenancy: design for the cloud

40 per cent of customers in Austria rely on old infrastructure – updating and maintaining is much more expensive than migrating to the cloud. Yet using the cloud is 8x cheaper than running your own infrastructure and this puts a huge pressure on industry. If one jumps on the cloud, it has huge impact on competitors, as happened in the banking industry.

Microsoft are the data centre guys: 200+ cloud services in 120+ data centres. Running the cloud means automation and self-service. Servers have a maximum three-year lifespan, so the software can have a higher availability than the IT infrastructure beneath.

We invest a lot in finding new solutions for new problems, including security/privacy. The common key trends affecting security are:

- The consumerisation of IT
- Targeted attacks
- Identity-centric environment
- Cloud computing
- Regulatory/compliance issues

In terms of government access to data, the role of government to data is complex. With the digital transformation of society and the economy, we need new norms – technology innovation is so fast that the new norms cannot keep up – Microsoft has to go faster to protect our customers.

We cannot have just one strategy – how do we deal with cybercrime or economic espionage?

It's about security ...privacy...transparency....a trustworthy cloud initiative.

This is the year of encryption – but economy of scale in the cloud does not work if you encrypt everything. It's an ongoing transformation – we are not sure where this will lead, but it is a dramatic transformation.

Working together is much more interesting and powerful than working alone.

Third Presentation:

A world in transition - 'reset your mental software' - Tony Bosma: Futurist/Trendwatcher/Extend Limits

Tony Bosma presented a highly visual session, with clips from the Internet showing how the future is unfolding today.

He encourages us to challenge the status quo – and points to a technology-driven world where the smartest 'person' in the room will be the room itself.

Being really intelligent is questioning the things you know – we are conditioned from birth to look for the things we want to find. This is also true when we think about public safety and the changing role of public institutions within public safety. "We do not see things as they are, we see things as we are" (Anais Nin).

The changes we are now seeing are so fundamental that to think that we are in a temporary crisis is the biggest mistake we can make. This is also for public safety and crisis information. The future is already here. Technology combined with societal changes and new ways of communication demand safety institutions to reset the way they think about their future roles and way of working.

"We have to make a fundamental change, transition to a new world that is not real-time but pre-time – where technology knows what we need before we do - shifting from a world where people are serving structures to where networks are serving people."

Communication in crisis situations is becoming totally different and will change more with the continuous rise of people having access to technology. The growing impact of artificial intelligence and calculating power; increasing connectivity, and the growing usage of intelligent sensors. But it is not all about technology. Keep in mind who we trust. Our personal peer groups become more important as our trust in institutions still declines. Technology is changing exponential from predictive data to autonomous drones, pervasive surveillance, robotics and even the merge of technology within the human body. We need to unlearn what we have learned to understand the impact of today and tomorrow's technology. The presentation gave examples of what is already possible and what is coming.

But we must beware of dependence on technology. Are we making the past more efficient, or preparing for a fundamentally new world?

Everyone has access to data and communications. The future will see the death of the search engine – the smart mobile device will already know what you need. It's predictive and contextual. Finally we create a world where technology isn't dependent of us humans any more. In this new future world it is all about the smart usage of enormous amounts of data provided by smart algorithms. It is also about the empowerment of citizens and engagement in citizen communication.

Prepare for a world where your organisation is able to act 'pretime' by the usage of smart analytics and algorithms. The way to act on future developments which happen today is by intensifying cross border collaboration. Be technology driven but be always aware of total dependence.

Organisations working on public safety have to be more on top of developments that are happening right underneath their own eyes. Learn to monitor and translate those developments. Too many organisations still wonder why certain developments have happened instead of wondering why they haven't happened yet. That's the key in preparing for the future.

Q & A for Tony Bosma:

Q: How will we as humans react when technology or networks fail in that world?

A: We'll fall back to the traditional way of thinking. US Defense Secretary Leon Panetta said the US was facing a 'digital Pearl Harbor'. Most countries and governments are not aware. Do not throw the anti-digital world away.

Fourth Presentation:

Technology Trends: Back Office Data Mining Big Data - Paul Steinberg, CTO, Motorola Solutions

There are three basic wheels in motion: Societal change; business evolution, and technological evolution.

Social media has become a source of input important for people to pay attention to. There is lots of data – what do we do with it?

"The world has changed from careful collection, rationalisation and databasing of information, to one of storing everything, because we can."

Of the data stored today, only half a per cent is analysed, and 70-80 per cent is improperly secured.

How do we lessen the amount of cognitive effort required to analyse data? It's not about more data, it's about what you do with it.

Mission critical intelligence means helping people become informed and intelligent. Intelligence brings context, which brings more informed decisions.

Whether it's public safety LTE, shared between public safety, public, and/or private networks – the important thing is that the network has the capability to collect and operationalise data for mission critical applications.

The tools must be tailored and the data must be translated. Devices must be designed based on the user experience, to enable the user to make sense of the data. Technology has to be second nature – data analytics enables the user experience design.

When public safety users need the technology the most, they have the least cognitive capacity to be able to use it. Motorola refers to this as 'High Velocity Human Factors'. The experience is different for each user, so analysing the data enables the creation of a targeted user interface.

This will bring real time information to the public safety officer, who can see it and act in real time: this is bringing the right information to the right person at the right time in the right way, and leveraging the power of the data that the world is creating so prolifically. However, we are constrained – there are legal and civil barriers in the way of sharing information.

Q & A for Motorola Solutions:

Q: In the last few years pondering the mission critical broadband world, I have assumed that video is the killer app – but listening to analytics – is video the killer app or the distilled analysed data?

A: The killer app is not only video – the prolific bandwidth consumer is video and the way we treat it means we can't do the analytics at the optimum location. We need more intelligence at the edge – so we haul less back. Real time video – real time events when someone is watching – push that to the fog (see Cisco section) – a localised environment. For analysis of an incident, the uplink and downlink bandwidth required is roughly equal.

Fifth Presentation:

'Augmented Reality' - Herve Mokrani, Head of External Funding France & Europe, Airbus Defence and Space

Augmented reality combines real and virtual information, pre time and 3D. Why do we need it? We need it to provide public safety officials with relevant information.

This could include mapping, monitoring user health, monitoring environmental conditions – fire, water, reduced vision due to smoke. Wearable technology is already available, with integrated sensors.

There is 'attitude monitoring' where sensors on the responder transmit the state/status of the responder back to the control room. Trials of wearable technology for monitoring body temperature have been held over TETRA and Tetrapol.

We have to take into account the weight and flexibility of the user equipment, such as head-worn gear to take pictures to transmit back to base, or an oxygen monitor integrated into a diving mask.

In the future, vehicle navigation systems could have a holographic personal assistant showing the blue light responders the best route to an incident – the route with the least traffic lights and traffic congestion. The most requested application is help with indoor navigation from the fire community.

The control room of the future will have some 3D capabilities – for example 3D models may exist for all buildings to help a command officer to be virtually on the field and interact with the responders during an incident.

Today, augmented reality deals mainly with vision, but could incorporate all the senses to alert first responders to heat, cold, smooth or rough surfaces, and smell to alert presence of gas and HAZMAT.

"The issue today is not a technological issue. These capabilities all exist. The barrier is user and citizen acceptance. This can have a huge impact and we have to change mindsets. "

Q & A for Airbus:

Q: Do you have any plans to influence calls for augmented reality?

A: Airbus may develop some end user applications – public safety application scenarios are being developed to show management of priorities. There are not as many apps as the consumer world – we need a public safety app store – customised to end-users.

Interactive Round Table— Questions and Answers
Moderated discussion about Consequences for Mission Critical Services Communications

Speakers and audience

The panel session was opened by Hans Borgonjen. The audience contributed with comments about what they had heard so far, and a lively discussion ensured, with some statements/questions and answers captured below:

"Our near future is more moderate - our future is not so fast as presented."

"The next way of getting information is not government or public safety; it comes from the people – with information coming from multiple massive sources."

"Public safety infrastructure used to be isolated – now it will not be, it will be pressured from external sources, and will need to adapt and expand and strengthen to manage the data deluge."

"Just four per cent of internet users worldwide are using IPv6."

"TETRA and TEDS will be around for several years to come – any new networks need to incorporate the specific needs and resilience required by public safety."

"Public safety and PPDR need to lean into the developments while retaining the fall back and mission critical reliability."

"We can't hold back progress. It's not about replacing existing stuff, it's about integration."

"Anything that will allow public safety to spend more time in the field and less time at a desk will be embraced."

"How do we handle the information deluge? One general difference between the 'normal' world and the operational world is that the' normal' user just bombards the net with information for everyone. Public safety has to have pre-processed useful information otherwise it's pointless."

"Public safety is traditionally very conservative and learns from others' experiences – but change will come – we need new kids on the block in our communications centres."

"We are now in a situation where the gap between user needs and the technologies we are able to offer are growing fast because we do not have secure broadband."

“Bricks, bytes, behaviour – the first two will come – it’s getting people into the right mindset.”

“The public safety arena is slower in the uptake.”

“How do we deal with the data flood – how do we make our data interoperable? It’s a challenge between protection of the data itself and how we share it.”

‘It always has to work, but there are legal principles. BYOD is not easy for public safety.”

“Try something in a safe environment – iterate on it with the technology providers and evolve it. We need agile technology development.”

“Will we as public safety government people be able to trust the cloud from a security viewpoint?”

“Access to data will depend on how critical that data is – whether it needs to be secure.”

“How do we deal with the bad guys? With the private phones of the public safety guys having data collected by Google etc – should this be dealt with at the mobile operator level?”

“Big data, fast data, - how do we deal with all this data and make it useful?”

“First you have to validate the veracity – securely capture the data with multiple databases. The barriers need to be broken down and the data processed to extract intelligence. That intelligence needs harnessing, then it’s about how it is presented. Right information, right people, right time, right place.”

Q: “We are listening to all the speakers – data, data analytics – but the question is, even today we have mobile users and mobile phones – but we don’t use the functionality because of coverage, battery usage and cost. So all about IP etc – but what is happening to TETRA and Tetrapol?”

Cisco response: “My opinion is that standardising on a single layer of technology is not realistic. We would be stupid not to leverage wi fi etc.”

Motorola Solutions response: “Not a harmonised layer 2 - and coverage is different with data. So TEDS will augment TETRA and probably be the only real wide area mission critical data bearer (resiliency, coverage) for the next 5-20 years. Big data doesn’t have to equal big bandwidth – all the stuff we talked about, except high definition video, is possible on TEDS. Then as broadband becomes more prevalent there will be a combination. TETRA will be here for a long time to come.”

“We will have to manage the spectrum issue – having control over spectrum access is essential.”

“Technology development speed is exponential. We have to encourage people to move from their comfort zones and be more rapid and agile in their decision-making.”

“We have already done good work on technology – LTE is the choice for broadband so we know we will have high speed data.”

“It’s about the applications – it’s about the public safety user and the Internet of Things, data mining, video – imagine those services.”

“Is LTE, broadband and spectrum the right way to go – yes. You’re not going to get a quarter of these things for public safety in a mission critical context – and they are requirements that also protect public safety users.”

“It’s very difficult to have a common platform – users have a different speed of adoption.”

“Take a suggestion - develop an application – and unleash an ecosystem of third party developers to create public safety applications.”

“How can we connect people?

“Suggested action for TCCA Applications Working Group: A Public Safety application ecosystem needs to be cultivated and prioritised (APIs, mobile application management, application certification, application store, cybersecurity standards etc.).”

Press Release

Following the event, a press release was issued summarising the day. The press release can be read here: http://www.tandcca.com/about/article/22169

Presentations

The presentations can be downloaded from here:

https://www.dropbox.com/sh/6rth4svzkxep429/AAAYL667bw3TzCG4g0h0Q0nna?n=46179626

Appendix

Delegate notes

At the beginning of the day, delegates were asked to note key points from each speaker's presentation.

It is clear from the notes that the main messages from each speaker were heard loud and clear.

- Big data, fast data, 'fog' computing will help the cloud and IPv6 will drive the Internet of Things and the Internet of Everything.
- The New World of Work – how to utilise a flexible working environment to enhance productivity, and the increasing use of cloud computing to achieve economies of scale.
- Technological change is indeed rapid so how do bureaucratic governments keep pace?
- The management of data – it's not what we have, it's how we analyse it, extract the relevant intelligence, and use it to maximum advantage.

However ...

The most common reference in the delegate notes was about security, and how this future world of cloud, massive data, furious technology advances and futuristic inventions can still ensure that security of communications remains as robust as it is today.

Comments about security include:

- How do we manage the security of data centre in another country (from emergency services point of view)?
- Would like to hear more about security – particularly placement of applications/SCADA/electricity grid etc
- Mobility – in the new world of work - how do we ensure security? New data plants integrated into the power plant – how do you secure?
- If we are moving to a collaborative society what to expect when working with sensitive information in the public domain
- Mobile – IP is essential → the need for reliable broadband services for LTE → challenge for high security systems
- Prioritization of services how is it done? For instance in the security domain (mission critical applications)
- IoT: Challenge: Making an Internet/Network of things mission critical; resilient; secure/verifiable; predictable
- Cloud security issues and access reliability
- Microsoft: How is the regulation regarding Data Handling is accomplished? Regarding risks and mitigation strategies for companies entering the cloud have you integrated the CSA matrix or intend to?