International Telecommunication Union

ITU-T

Technical Paper

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

(09/2020)

XSTP-sgstruct

Strategic approaches to the transformation of security studies

Summary

Quite early in the 2017-2020 study period, ITU-T Study Group 17 (SG17) faced a number of problems:

– On the one hand the strong and fast evolution of security caused by many external forces leading to a number of innovations, prompted SG17 to consider if it had the right structure for the future.

– On the other hand, resources not being infinite, SG17 shall consider offering an efficient structure for the future.

In many ways, a Study Group is like a company whose product is called a 'Recommendation'. They also need to understand how to structure their 'portfolio' in the right 'business units', which are essentially Working Parties and Questions. As in a company, success is heavily dependent on how the organization is structured, and how leaders are allocated to this organization. As such it became essential to pay particular attention to the future structure of security studies.

To support this effort, a correspondence group for the transformation of security studies was established by SG17 during the course of this study period. It was opened to any delegate interested in this issue and regrouped a significant part of the SG17 management team, member states, sector members, associate and academia participants, and sometimes, civil society. It successfully delivered a significant number of creative results such as the establishment of an incubation mechanism to support innovation, the processing of hot topics with TSAG (Telecommunication Standardization Advisory Group), the changing of a number of Questions half way through the study period, and models for new structures, candidates, and even an alternate story/narrative for the study group. It also became apparent that the long-term strategic thinking allowed some hidden realities to be revealed and helped other communities including member states to influence the transformation of their own national cybersecurity strategy.

This knowledge spanned through a period of 3 years and consisted of a large number of TDs and Contributions. The members of the correspondence group recognized the value for the future leadership teams to regroup the knowledge already produced into this document and offer a vehicle to help the SG17 community develop a strategic approach to the transformation of security studies.

Keywords

Strategy, transformation of security studies.

Change Log

This document contains Version 1 of the ITU-T Technical Paper on "Strategic approaches to the transformation of security studies" approved at the ITU-T Study Group 17 meeting held in Geneva, 24 August to 3 September 2020.

Table of Contents

Page

Technical Paper ITU-T TP.SG-SCTRUCT

Strategic approaches to the transformation of security studies

1 Scope

The scope of this Technical Paper is the synthesis of all the results delivered by the correspondence group on transformation of security studies under the mandate of ITU-T SG17 from August 2017 to August 2020.

It includes the contextualization of this work and the methodological aspects considered.

It describes the strategic thinking that the correspondence group developed.

It covers the short, mid and long-term aspects of the transformation of security studies.

2 References

None

3 Terms and definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Technical Paper

This Technical Paper defines the following terms:

3.2.1 digital service providers: A categorization of all the service providers in the digitalization era (offering digital services).

3.2.2 question coverage: Question coverage is an attribute to whether the current Question coverage is within the mandate or if it expands outside of its mandate. Question coverage can take values: Fit or Expands.

3.2.3 question density: Question density is the number of sub-items it must cover in its mandate. Question density can take values: Small, Medium or Large.

3.2.4 question granularity: The granularity of a Question is the size of the scope of its mandate. Question granularity can take values: Small, Medium or Large.

3.2.5 question load: Question load is the work-load activity of a question. Question load can take values: Light, Medium or Heavy.

4 Abbreviations and acronyms

This Technical Paper uses the following abbreviations and acronyms:

AI	Artificial Intelligence
B2B	Business To Business
B2B2C	Business To Business To Consumer
B2C	Business To Consumer
CACAO	Collaborative Automated Course of Action Operations
CDC	Cyber Defence Centre

CERT	Computer Emergency Response Team
CG	Correspondence Group
CG-SECAD	Correspondence Group Security Architecture Development
CG-XSS	Correspondence Group Transformation of Security Studies
CNPD	Cloud Network Platform Device
CSIRT	Computer Security Incident Response Team
CSB	Cloud Service Broker
CSP	Communication Service Provider
CTO	Chief Technology Officer
DLT	Distributed Ledger Technology
DSP	Digital Service Providers
EDR	Event Data Record
ENT SP	Enterprise Service Provider
ETSI	European Telecommunications Standards Institute
EU	European Union
FAIR	Factor Analysis of Information Risk
FG	Focus Group
GDPR	General Data Protection Regulation
GSI	Global System Integrator
GSMA	Global System for Mobile Communications Association
ICT	Information Communications Technology
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IoT	Internet of Things
IPTV	Internet Protocol Television
ISG	Industry Specification Group
ISO	International Organization for Standardization
ISP	Infrastructure Service Provider
IT	Information Technology
JTC	Joint Technical Committee
KPI	Key Performance Indicator
M2M	Machine To Machine
MSP	Managed Service Provider
NBT	Next Big Thing
NEP	Network Equipment Provider

NFV	Network Function Virtualization
NWI	New Work Item
OASIS	Organization for the Advancement of Structured Information
OID	Objet Identifier
OTT	Over The Top
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PP18	ITU Plenipotentiary 2018
QKD	Quantum Key Distribution
RG-SS	Rapporteur Group Standardization Strategy
SC	Sub Committee
SDG	Sustainable Development Goal
SDN	Software Defined Network
SDO	Standard Defining Organization
SG	Study Group
SGLA	Study Group Leadership Assembly
SOC	Security Operation Centre
STEEP	Social Technological Ecological Economical Political
SWOT	Strength Weakness Opportunity Threat
TD	Temporary Document
TP	Technical Paper
TR	Technical Record
ToR	Terms of Reference
TSAG	Telecommunication Standardization Advisory Group
UN	United Nations
WI	Work Item
WP	Working Party
WTSA	World Telecommunication Standardization Assembly
ZTM	Zero Touch Management

5 Executive summary

SG17 recognized the need for a structural transformation and established a correspondence group on transformation of security studies.

This correspondence group attracted more than a hundred participants and met over a 3-year period from August 2017 to August 2020.

The correspondence group delivered a significant number of outcomes at short, mid and long-term which provided many benefits for SG17 and its members such as the pioneering of a new incubation mechanism, allowing innovation to flow in the study group, supporting changes in Question texts, addressing of hot topics, and proposing of alternatives in the structure of the study group.

As a result, from a strategic thinking approach, a new area of development was identified based on the recognition of the need for an increased security architecture development (now a new correspondence group) and an opportunity concerning operational security.

This work proved helpful to several member states in their own transformation of their national security strategies, as well as adding to the maturity of the team over time as it addressed more complex and valuable horizons.

As such other organizations seeking to perform a transformation of their security approaches could consider the approach taken in this technical paper and/or the lessons learnt on how to create the right conditions to allow change to happen.

This document regroups the knowledge accumulated to allow current and future SG17 delegates as well as connected communities and member states to prepare their own transformation of security studies for ITU-T or for their own purposes.

6 Introduction and overview

SG17 realized quite early in the study period 2017-2020 that given a rapidly changing overall context, it was necessary to consider how to transform security studies in the short, mid and long-term.

– By short-term, we mean the time between two SG17 meetings as a way to resolve the tension between:
  - mandates established for four years which, from a cybersecurity perspective, is an eternity, and
  - the need from the industry to standardize on recognized innovations and for which no reserve was made in any question text. In WTSA-16, the terms *Quantum*, *AI* and *DLT* were not even listed in Resolutions.

– By mid-term, we mean a two-year period, basically matching the middle of the study period and a good moment to potentially tune and change some of the question texts.

– By long-term, we mean:
  - the end of the study period and what matters to its transformation, however,
  - as the next study period is engaging for another four years, we recognize the need to consider longer intervals by the end of the next study period,
  - which means long-term, meaning here 5-8 years depending on how the correspondence group has progressed over time.

6.1 Who participated?

A correspondence group for the transformation of security was established after the 2nd SG17 meeting and was asked to pursue its mission over the current study period.

Through a large number of teleconference calls and a growing community of more than 100 participants, the correspondence group worked incrementally and delivered abundant documentation.

Participants were:

– members of the SG17 management team (Vice Chairmen, Working Party Chairmen and Vice Chairmen, Rapporteurs and Associate Rapporteurs)

– member state delegates

– delegates from sector members and associate participants

- delegates from academia
- sometimes delegates from civil society

6.2 Assumed audience of this document

This document is directed to anyone interested in the transformation of security studies and is not limited to within ITU-T SG17.

- This document is to provide future SG17 management and leadership teams with an approach to the transformation of security studies, showing a methodology, a strategic thinking approach and how to resolve short, mid and long-term aspects.
- This document has been used by other communities, e.g., by some member states to influence their own national cybersecurity strategies. Its general applicability has shown that it can be of value to others who have to transform their own fields.

6.3 A maturity curve

As most of the team had apparently never been exposed to such an exercise, it had to go through a significant methodological effort to allow transparency and neutrality before being in a position to propose alternatives and expressed views at each step of this project.

Given the output, it was deemed worth capturing this experience in this document as a synthesis. It delivered significant influence and results to support the short, mid and long-term problems facing the study group. It allowed delegates to influence their own affiliations in near real time. It transformed the participants themselves in various dimensions. The participation increased as significantly as the team maturity itself, both between co-convenors and between participants.

6.4 How is this document organized?

This document is organized to provide a synthesis of:

- The general context
- The methodology used
- The strategic thinking followed
- The short-term impact of the study group
- The mid-term impact of the study group
- The long-term impact of the study group

7 General context

Study Group 17 is responsible for security aspects of the overall information communications technology (ICT), with the addition of over the top (OTT) technology after ITU PP18. All of its current and future work supports a large fraction of the world's security systems, based on voluntary contributions.

Yet, this world has never before undergone such an unprecedented transformation due to the implacable pressure of digitalization. Whilst this transformation is leading to disruptions in every constituent of today's world, leading and self-accelerating every aspect of innovation, the world is also facing an unprecedented threat from the cyber security attacking landscape.

As illustrations of the above, this transformation leads to:

- The return to the spotlight after 25 years of artificial intelligence (AI) with all of its associated unknowns;
- The fractal impulse of crypto currencies to promote the distributed ledger technologies (DLT);

- Incentives to create Quantum computer capabilities;
- Incentives to create new robotics markets;
- Support for new intelligent transport systems;
- A radically new way to approach finance;
- The redefinition of Government functions, and any other verticals; and
- Innovative ways to improve the place of humans in a digital world from the growing field of digital humanities.

Unfortunately, todays' world also witnessed "Wannacry", one of the first worldwide attacks on 150 countries in 'one go' in May 2017, which was followed by the "NoPetya" attack, and the constant attacks on crypto currencies which led to hundreds of millions of value lost and these attacks are evolving everyday with current significant concerns about the security of 5G. In addition, geopolitics is showing new frontiers fuelled by the spectre of a mounting set of cyber weaponry from cyber security attack units to disinformation. These are 'just' milestones in an increasingly prevalent attack landscape. This means that:

- attacks are now getting close to the individual level and are increasingly targeting the organizational level potentially preventing an individual from getting surgery or a ship from leaving a port with the potential of a real materialization of the impact,
- our encryption capabilities will be ruined by the next generation of Quantum computing capabilities within a horizon of 10-15 years.

To summarize this long introduction:

- The security ecosystem as we know it today is evolving erratically[1] through changes in vertical industries, innovation technologies and core security technologies. These trends have far-reaching impacts beyond just SG17 and global standardization.

On the one hand, given its mandate of security, SG17 is under pressure from global forces such as:

- An arms race between attackers and defenders leading to a large range of innovations;
- A fundamental singularity moment approaching, called post-Quantum;
- Digitalization mega-trend driving general innovation (AI, DLT, etc.) which fuels both the attackers and the defenders weaponry but, also in many ways created a huge inflation of the attack surface;
- Increased business awareness of the importance of security and the need to invest;
- ICTs, which scope the work of many Study Groups, are undergoing strong transformations;
- Nation state positions on security have evolved domestically and internationally, which leads to impactful changes in the policy and regulatory frameworks at country and regional levels;
- Civil society as a counterweight to security with privacy centric concerns;
- Academia which has matured a lot and opens new frontiers for security;
- A shortage of skills, talents, resources and professionalization, which accelerates the need for best practices and standards to simplify the jobs.

On the other hand, the domain of the ITU is being transformed incrementally. The new ecosystem is better described as the digital service providers (DSP) ecosystem.

- ITU recognized the OTTs as part of its applicability as per PP18 Resolution 207,
- 5G will seal the change in focus from B2C, to B2B and B2B2C which means:
  - verticalization is becoming an essential pillar of the new ecosystem;

[1] By erratically we mean fast, tectonically and disruptively, making it hard to predict when to 'double down' on which new categories will appear, consolidate, or disappear.

- verticals themselves will become service providers in many ways, augmenting the new ecosystem of digital service providers; and
- this is happening due to the same forces listed for security, the general mega-trend of digitalization is driving business actor changes.

Whilst SG17 has evolved incrementally over the past 15 years, the magnitude of the above changes triggered a situation, which led SG17 to set up a correspondence group for the transformation of security studies with one of its goals being to propose long-term future SG17 structure alternatives.

As there was no model or guidance on transformations, it was through a set of incremental steps in the thought process that the team patiently crafted an analysis, a creative method and then a number of out of the box solutions to this new problem.

Indeed, a key driver of this thought process was to compare the Study Group with a company for which the Recommendations are like company products and services and the structure of the Working Parties, and Questions are like the Business Units and organization of a company.

It is very clear that designing a Study Group structure that can meet the long-term requirements, limits and constraints of this new reality will provide the conditions for success should success be defined.

7.1 Problem statement

In the above context, the problem that this document aims to resolve is:

> Why and how to establish a short, mid and long-term strategy for the transformation of security studies? Once established, what can this process propose as good solutions and alternatives for short, mid and long-term strategy?

7.2 Why the need for new long-term SG17 structures alternatives?

Much like in a company, transforming and/or designing an organization structure for a Study Group must be done carefully taking into account many requirements, constraints and limits. As this process takes time, resources, strategic thinking, decisions, internal and external communications, politics, selection of leadership and appointments, measurement, etc. it is essential that its design phase is executed with a high degree of quality so that it can provide organization structure alternatives that the stakeholders can decide on and then appoint the right leadership to this structure.

7.3 Why is this a problem now?

SG17 evolved incrementally over the years but security issues evolved at a much faster pace due to a number of global forces as mentioned previously. There are additional signs that SG17 is in need of a change, such as:

- Increase in the number of questions
- Increase of requests for creating new questions
- Difficulty in managing some meetings under the pressure of contributions
- Difficulty to 'read' the Study Group structure to allocate New Work Items
- Increase of cross questions meetings
- Efficiency issues
- Perspective of WTSA-20

7.4 Outcome and results

The outcome and results of this process are summarized in Table 1.

Table 1 – Summary of outcome and results

Term	Deliverable	Impact
Short-term	Incubation mechanism	A premier in the history of ITU Allowed innovation to be accepted in SG17, e.g., quantum key distribution (QKD), etc. Changed the approach to the work and re-valued TPs and TRs to allow all participants to be on the same level of information
Mid-term	Supported the change of a number of Question texts	Allowed SG17 to adapt at mid-term of the study period
	Support to Hot Topics analysis and rationale for Q1	Allowed SG17 to answer TSAG Allowed TSAG RG-SS to improve format and improve its approach to Hot Topics
	Identified Next Big Things	Inputs to workshops, changes of question texts, etc.
Long-term	Several proposals for new SG17 structure	Input to the WTSA preparation correspondence group. Gave several creative alternatives, defined specific terms to qualify the potential changes of structure
	A modelisation of SG17	Helped rationalise neutrally and find potential creative alternatives which would impact Working Parties and SG17 meetings
	A massive gap on operational security	Operational security seems to be a new frontier which is under-represented today. It would allow a significant gap for Recommendations as well as of collaboration and coordination with other SDOs
	The beginning of a root cause analysis and an industry analysis	Helps guide the SG17 in potentially many directions including: which actors to hire for contribution, which actors to influence, to interview for feedback, etc.
	A new correspondence group on security architecture development	Provide a new instrument to improve quality, composability, harmonization and increase focus on more technical Recommendations
Methodology	Identification, development and practice of methodologies adapted to SG17 case	Gave a methodology to the correspondence group which was used as the instrument for the transformation as well as allowing the maturity of the team to be increased
	Established strategic thinking as a practice	Allowed a core of delegates to develop Strategic Thinking views which are influencing and enriching beyond the core team and disseminating in SG17
Community	Influenced the national cybersecurity of some countries	This helped some of the delegates to consume the work for their own advantage but also gave validation and additional inputs to some of the assumptions as the strategic thinking could be tested in the field to some degree.

Table 1 – Summary of outcome and results

Term	Deliverable	Impact
	Lead a number of administrations to contribute, influence and support	Several administrations participate actively and engage in the development of this transformation at short, mid and long-term, again helping the overall maturity and transformation of the team itself for improving the conditions of SG17

8 Methodology followed

8.1 How to find good alternatives to the long-term structure of SG17?

Finding an organization structure is the result of:

- a very delicate design process that will produce the alternatives with the right rationale/strategic thinking, and
- a design process that needs itself to be established with the right governance in place.

8.1.1 Establishing the design process

Study Groups are a community, so it became very obvious that the design process leading to the alternatives to the long-term structure of SG17 must be:

- transparent to everyone,
- neutral to all expressed-views, and
- consensus based.

The correspondence group took the following analogy: The design process is like resolving an equation, which it needs first to establish. Yet this equation can lead, in our case to three possible situations that are described in Table 2.

Table 2 – The three possible ways the design process can end

Alternative	Comments	Examples
ALT1	There is no way to improve the situation and there are no alternatives because there are too many constraints	The politics, resources and rules in the Study Group are too coercive
ALT2	There is only one alternative to improve the situation	There is a path but the controversy is so strong that we can only find one way to improve the Study Group structure.
ALT3	There are multiple alternatives to improve the situation	For example, a conservative, a moderately innovative and a radically innovative alternative structure.

Therefore, the question that comes to mind is:

From which equation are these solution types coming?

Now the design process is about organization transformation, which can be approached in various ways [b-Incubation]:

- A bottom up approach which consists in starting from the existing structure to infer the next candidates.

- A top down approach which consists in creating an ideal big picture against which all constituencies need to converge.
- A combination of both approaches.

Here we considered a combination of both approaches, which led to the following process of defining the "future story" and establishing the requirements, limits and constraints of the future structure. This will lead to the development of our "future story", a narrative of a shared vision for SG17.

8.1.2 Obtaining and organizing input

Obtaining and organizing input for such a transformation is a complex task considering:

- the variety of roles inside and outside the ITU,
- the diversity of cultures:
  - by countries from all over the planet,
  - by ITU roles from contributors, editors, rapporteurs, leaders, etc.,
  - by member types from member states, sector members, etc.,
  - by profession from researchers, architects, consultants, etc.

Each input sheds light on some facets and so highlighted the need for a Strategic Thinking process.

With this in mind, the goal was to triage the input into essentially the following categories:

- requirements
- limits
- constraints
- structure
- story

8.2 Requirements

The correspondence group never rigorously codified the requirements which is certainly a limitation on the work of the correspondence group itself. This could be improved in future study periods, yet as requirements were considered, the transformation of security studies shall:

- correctly represent the industry dynamics;
- include as appropriate innovation under any of its forms (hot topics, next big things, etc.);
- consider societal aspects (such as the sustainable development goals);
- deliver a mid-term and long-term structure alternatives that provide a good efficiency;
- provide a good return of investment for the industry;
- identify fruitful gaps for new work items in a long-term approach based on well thought out and reasonable strategy; and
- reduce the current silo approach and move to a shared vision approach, allowing Recommendation composability and harmonization;
- foster and encourage collaboration and coordination within and outside of the ITU-T.

8.3 Limits and constraints to the future structure of SG17

The correspondence group did not rigorously split the limits and the constraints and this is an area of potential improvement for future methodology for the transformation of security studies.
SG17 should consider the limits and constraints identified in Table 3.

Table 3 – Limits and constraints

Constraint	Potential complication	Description
C1	ITU rules	WTSA-16 approved SG17 mandate with detailed Question description. Although ITU rules are there to allow for adjustment and evolution of a SG and its working areas in between WTSAs, changing the structure could be misperceived as 'outlaw' SG17 by not fulfilling its mandate, facing scope creeping, loss of focus and missed targets. To prepare for the next WTSA in October 2020 we must propose a new/revised SG17 structure by October 2019. This means that in the March 2018 meeting of SG17 we will be left with 18 months to find a consensus and be prepared. In fact, given the difficulty/complexity of this task, we do not have a huge amount of time ahead of us.
C2	Resource limits	The SG17 community is a growing community but the linear expansion of Questions is causing exponential entropy increase to simply follow the Questions, ensure quality outcome, increase risks of cross Questions coordination, create rooms and logistic issues, etc. By no means can the current resources from member states, sector members, academia, etc. match this.
C3	Resource allocations	Management positions were given to specific people across SG17 and this is bound to commitments from participating organizations which include resources time, travel costs and membership costs. Changes in the structure will inevitably redistribute positions which may potentially create breakages in back to back agreements and therefore create a political risk.
C4	Dependencies	There are many explicit, implicit and perhaps even forgotten dependencies within SG17 and outside of SG17 both within and outside ITU. Within SG17: Questions from joint collaborations, correspondence groups, Resolutions, JCAs Within ITU: SG17 and SG13, SG15, SG20, FG-DLT, FG-DPM, etc. Outside ITU: ISO/IEC JTC 1, ETSI, IETF, IEEE, OASIS, etc. A good example is the mandate given by ISO SC6 to Q11 to deal with any work related to Blockchain and PKI.
C5	Legacy and history	SG17 comes from a specific history and some of its structure is still carrying some of this history at several levels: – Certain Questions today might have to be re-named/re-interpreted as they come from a past where security had a certain context which has completely evolved. – Existing Recommendations might potentially require a severe review and update and this may prove to be a herculean task. – Current Work Items categorization might have been ambiguously allocated to Questions while others would have been more relevant to host the work item. – The history of SG17 itself can also perhaps teach us some lessons on how new Questions or working parties were created.

Table 3 – Limits and constraints

Constraint	Potential complication	Description
C6	Alignment	What is the 'horizontal' or 'vertical' alignment of certain Questions and even the Study Group itself? By horizontal we mean an entity which offers a shared capability to the others, by vertical we mean an entity which offers a capability for a specific business, industry, organization. As such Q1, Q6, Q13 are good examples of vertical Questions and Q2, Q3, Q4, Q5, Q7, Q8, Q9, Q10, Q11, Q12, Q14 are good examples of horizontal Questions. Today the Study Group is certainly designed horizontally to support the other Study Groups. However, current experience of the Study Group shows that cross SG coordination is also challenging on cross Study Group issues such as on IoT Security. Security is a business by itself and 500 companies are delivering products to customers directly not counting the digital service providers that are also embedding or delivering security products. This means that the verticality of the Study Group itself delivering direct value to this world was neglected or even forgotten, and the whole 'Security as a Service' aspect was by and large neglected (which leads us to the next point).
C7	Direct and indirect reach	Most of the work done is about directly protecting a construct. The idea for example that the digital service providers are the gateway to the security of the markets was massively ignored and it is only recently that Security as a Service work items started to appear or 5G Security for the customers rather than the security of 5G itself. Perhaps the current 'security by design' doctrine should be extended to incorporate the kaleidoscope view of a direct and indirect channel to make this global adoption faster with less friction and a good seamless security experience.
C8	Ossification	Ossification is about the risk that each Rapporteur trying to improve its current Question for good reasons might in fact contribute to the ossification of the current structure, creating a natural inertia to change with the risk that the potential new structure might be too conservative.
C9	Speed	The speed of delivery of good standardization in this context is an enormous problem given the speed at which the security landscape is evolving.

SG17 should also consider the limits of:

– the current work-load of existing Questions to ensure capacity is available to carry out the required work;

– the availability of the required skills to carry out the work;

– the small delegations who cannot span through an extensive structure;

– the leaders themselves (fatigue, mismatch of field domain vs evolved mandates, etc.); and

– work done by other standardization groups within ITU-T (SGs and FGs) and outside (e.g., ISO/IEC, ETSI, IETF, IEC, etc.).

9 Strategic thinking approach

It took many steps for the correspondence group to establish a strategic thinking approach and in particular for the long-term. Several approaches were trialled:

- First, the urgency of the short-term situation focused attention away from long-term strategic thinking in the early days of the correspondence group and a first analogy was urgently developed to help organize the thinking.
- Second, other methods from the industry were considered but it rapidly became apparent that some were too ambitious to apply to the case of SG17 and others were only revealed as adequate later.
- Third, it took time to realize that the pressure of hot topics (indirectly coming from TSAG) was not of a strategic nature and was not meant to constitute a strategic thinking approach.
- Fourth, it was only when the correspondence group started to look at the industry forces and analysed the situation from proven and efficient outside-in methods according to the 5 forces from Michael Porter, that progress started to be made in strategic thinking.
- Finally, the ITU-T Study Group Leadership Assembly of autumn 2019 was the trigger to unlock genuine strategic thinking when the group asked the question what is the present state of cybersecurity?

9.1 The 'company' analogy

While it came very slowly and involved a lot of steps, the strategic thinking sustaining this work came from an analogy with what companies do when they want to establish their own future transformation and story.

The first typical approach that a company would take is the so-called SWOT (strengths, weaknesses, opportunities and threats) approach. This is typical 'inside out' approach which usually peers with a bottom up approach of interviewing the main leaders of the current organization.

Only a partial SWOT approach on the weaknesses (as per Annex A) was carried out by the correspondence group. Though it is a demanding exercise this is another area for potential improvement for any future work on transformation of security studies.

In addition to the initial approach to compare SG17 with a company, another approach emerged to consider ITU-T as a company and, in keeping with the analogy, SG17 being one of its 'company divisions'.

Both approaches are meaningful but the second one could have been better formalized as there are aspects that SG17 does not control but its parent entity does. This was hinted at through the hot topics situation but it is much bigger than that (WTSA-20 preparation and many other aspects).

9.2 'Outside-in' tools

What is under consideration in a major 'outside in' read of the real world and what it means for the organisation. Methods such as STEEP (social, technological, economic, environmental and political), are systematically used to get design transformation teams through a number of considerations that framed the genesis of the transformation story.

Therefore, the first implication is that the answer has to be at least checked if it does not come from the outside world, meaning in our case: the business and the users of the Recommendations.

The correspondence group learnt that just approaching external stakeholders to engage in an intelligible discussion was a task in itself. Indeed, it requires a developed narrative to make sure the interviews are efficient and of value for both sides and to ensure that the correspondence group delegates do not lose credibility during the interviewing process.

Carrying out a complete "STEEP" landscape description is a full consultancy job that is very demanding in resources and commonly offered by very costly specialized companies. For this reason we recognize that, like any design it will be carried out with a lot of partial information and assumptions.

9.3 Hot topics are tactical

With this in mind we realized (and it took a lot of time to realize) that the internal ITU SG17 and ITU-T level strategic thinking was polarized on hot topics as a way to incrementally approach transformation.

It is recognized here that whilst the identification and qualification of hot topics is important, dealing with Hot Topics does not constitute a strategy. Hot topics are tactical topics that appear, develop, merge and disappear.

9.4 Analysis of the key forces

Taking a step back, what shapes standardization can be summarized by the interaction of (most of the time hidden) forces:

– Business and market forces

– Geopolitics

– Research competition

– Civil society influence

We therefore re-position here a strategic approach which:

– Starts with an analysis of the evolution of the market dynamics

– Is modularized, limited and constrained by the member states' mandates

We concentrated on these aspects at this stage. In doing so we established some limits to our own design method.

Once these are established, then Hot Topics can be factored-in.

9.5 The hidden elephant discovery – The major breakthrough

The strategic thinking journey accomplished with the help of the former sections allowed delivery of the core essential alternatives to the short, mid and long-term of the study group structure.

Only once these core essential alternatives had been delivered, and with a now very mature team, we were able take a second major step back and ask ourselves some more fundamental questions as listed in Table 4. Table 4 expresses the views of the co-conveners on which the team later reflected.

Table 4 – The co-conveners' expressed views on long-term strategic thinking

#	Expressed view	Comments
EV01	The considerations we need to explore to inform the strategic discussions are significant	What for example does "Readiness" mean for Quantum or AI or other innovations We are missing a huge aspect concerning how we fit these in human society's long-term future: – Lead a discussion on STS Forum: stsforum.org – Japan Society 5.0 – UN sustainable development goals (SDGs) and their consequences[2] We are also missing recognition concerning counterfeit products in general.
EV02	Implications from EV01 on cybersecurity	How does this translate in terms of cybersecurity

[2] We had a very good remark from Mrs. Oh who met a UN representative attending ISO JTC1 SC27 on DLT and how it will affect self-employed people including fishermen, farmers, notarial, etc. and how it will decrease jobs and how it is a problem for Korea for example.

EV03	Current state of cybersecurity	Which we think is in regression: – M. Taddei's exposed some aspects in his presentation at the SGLA. – M. Kadobayashi's note on Youngsters regressions on coding practices, etc. using Javascript, back stepping almost daily. Also his considerations on the need for simplification (Which echoes some aspects developed in M. Taddei's presentation). – Mrs. Oh also noted the difficult constraints on privacy vs PII and its implications back on SDGs and how we fit the EV01 or not.
EV04	The concern to get answers within SG17	It is difficult to get answers at this level from SG17 delegates in general but we are hopeful. Yet, we need help elsewhere in other fields, e.g., Pharmaceutical with their successes and failures and in general we need 'more expertise'.
EV05	National general approaches	We also need to recognize and openly discuss that certain countries are on the edge of this thinking (e.g., Japan) whilst other countries are trying to be more pragmatic and follow more proven routes (e.g., Korea).
EV06	It is not just SG17, there are intersections with other SGs and potentially things to discuss/learn with ITU-R	We need to communicate with the other SGs (on the same trend observed at SGLA, especially pushed by the SG2 chairman, but as well on some other aspects which came out at TSAG through e.g., the coordination discussion during the ad-hoc sessions on quantum computing).
EV07	The requirement for a focus on Design and Architecture to have a solid foundation strategically in the long run	We discussed the proposal by M. Taddei at the last TSAG as per C99 and consider it is a good input for the work of this CG. Specifically we are all concerned by the state of the X.800 series but it could also help EV01 to offer the SDGs (See C99 again) as systematic criteria (non-mandatory) for recommendations development.

Finally this allowed us to undertake a proper strategic approach to innovation, to the actors, and to what SG17 is missing, and also to understand that we had a major issue namely Operational Security that was basically not defined. Indeed, we have observed a general abysmal lack of operational security knowledge, especially in the context of standardization. This probably explains why the plethora of strategies, capacity building initiatives, certifications and frameworks are in the best cases under-performing and in the worst cases simply failing.

If the purpose of security is to reduce risk, without yet going into these aspects, as per *Hubbard/Sieresen, Factor analysis of information risk (FAIR), The Duty of Care Risk Analysis Standard (DoCRA)* [b-DOCRA] any improvements we can make to operational security will help reduce risks.

Taking a pragmatic approach to operational security it can be broken down into the 4 required constituencies listed in Table 5.

Table 5 – The four constituencies of operational security

#	Required constituency	Description
1	People	We need security specialists who are able to proactively and reactively monitor, detect, incident response and security manage the problem.

		This includes proactive risk assessments, audits, security architecture work, etc. and involves a range of cyber defence centres such as security operation Centres (SOC), computer emergency response teams (CERTs), computer security incident response team (CSIRT), etc.
2	Knowledge	What is the 'recipe' we need to use to fix the problem? This is called the playbook and to fix a problem you might need different playbooks, some being very aggressive but at the expense of a loss of business key performance indicators (KPIs), and other less aggressive playbooks that do not necessarily resolve the problem, but preserve the business KPIs.
3	Security products	All the potential weaponry of security products on endpoints, network and platforms: endpoint security products, firewalls, proxies, data centre security, orchestration, integrated cyber defence, identity management, identity, encryption, data loss prevention, messaging security, etc.
4	Assets	Assets are the artefacts that need to be protected: the networks themselves, the endpoints and the things whatever they are at any scale, the data, the people, their expertise, the organizations, etc. Each artefact may exhibit an intrinsic security capability fuelled by the push for 'security by design' and now 'privacy by design'.

However the current reality looks more like Table 6 that indicates the real state of the four constituencies of operational security.

Table 6 – The real state of the four constituencies of operational security

#	Required constituency	Current state
1	People	We are probably missing over 2 million security specialists globally based on previous estimates by IDC. A simple check within the network of colleagues shows heavy shortages of candidates in research in Germany, in Switzerland, etc. so this is not just a developing country issue, no-one is immune. On top of being quantitative, the issue is also qualitative. Paradoxically security is a non-professionalised area, most of the jobs being vocational today, with few exceptions. Education globally is not providing the licensed and certified curricula that would be required. One cannot go to e.g., Geneva university and ask to hire 5 incident responders, 3 crisis managers, etc. Of even more concern, the entire service domain lacks common and implementable definitions in managed security services, cyber defence centres, CERTs, CSIRTs, etc. As a result every player comes with its own definition without properly measuring the underlying spectrum of sub-services that need to be developed, and the impact of that on the maturity curve and business expectations. If the services are undefined, then jobs cannot be defined either. FIRST has done a great job on incident response, and ITU has started X.framcdc as an overall definition of cyber defence centres and all their variations, but this is all still work in progress.
2	Knowledge	Playbooks do not exist today as a defined agreed standard. Period. After a difficult situation at IETF and a year lost, the proponents repatriated the working group at

Table 6 – The real state of the four constituencies of operational security

#	Required constituency	Current state
		OASIS and it started its work now (known as CACAO). Yet this is still in the first steps with various disagreements in the background. For example, some network equipment providers (NEPs) are wondering why they should share what they consider to be their "magic sauce".
3	Security Products	The product stack is a cacophony of products from companies each of which are in the belief – or the dream – that they are setting the de facto standard. There is no integration agreed, no orchestration agreed, there is no formal architecture of the product stack, it is all ad hoc. Some work though is encouraging like OASIS openc2 on the orchestration stack, or ITU's work in SG17 to revisit its X.800 foundation, with first approaches on integrations with schemas of data security products for interoperability, etc. Yet so much is still lacking in this space, considering the privacy/security split and extremist positions taken, the wrong impression that encryption = security, the innovation in security like AI which in fact increases the attack surface for security itself, the advent of distributed ledger technology (DLT), the advent of Quantum, etc. Innovation has benefits but no one seems to be willing to recognize the complications it brings with a severe lack of maturity, let alone any ethical approach, not to mention the strong lack of human factor considerations at any level (user experience, anthropology, etc.).
4	Assets	Unfortunately the intention of security by design was mistranslated as stakeholders understood it to mean that if you are secure by design, you are secure. Sadly this is not true. Current security capabilities cannot have interoperable managment by an exogen security stack. To make things worse, the current approach taken by the industry leads to a major Frankenstein effect, which, due to the hyper convergence and scalability of platforms, is actually potentially multiplying the attack surface. This is fundamentally due to the lack of a multi-factor design including dimensions such as security as a design essential, not as a "patch" in the design. If done correctly, by optimizing costs, most of the time an optimized multi-factor will help other design criteria such as inferred by UN SDGs and will hace the add on effect of helping the companies. This means that the minimization of the attack surface becomes a major problem and as maturity model levels are very mediocre, the tension in the supply chain further exacerbates the issue. For some specific areas such as 5G, consider the example of a city like Tokyo with 10 million inhabitants. Assuming 100 'IP addresses' per person, Tokyo would have to manage a 5G platform for 1B objects. Reckoning that a network slice will consume from 100 to 1000 containers in a serverless SDN/NFV cloud architecture, this basically means having to manage 1T containers. As this cannot be done manually, AI will be indispensable. But then how to protect 1T containers if we factor in the additional attack surface generated by AI, which requires a very powerful security stack, which again itself requires more AI, which needs to be protected, and so on? Ultimately who guards the guards? And this is just 5G, without even looking at the 5G elements themselves. What about the security of new SIM models, what about side channel attacks on radio and all the rest?

The root cause analysis led to identifying the deep and somewhat hidden difficulties, between the four main stakeholders: governments, business, academia and civil society but more importantly it opens:

- A positive perspective on a vast opportunity for standardization;
- Several standardization organizations should seize this opportunity with good coordination;
- ITU-T SG17 is already playing a role and could grow significantly while resolving this key problem;
- It shows both expressed views of the key roles that SG17 and ITU-T should play:
  - Terminology and high-level concepts.
  - A requirement to become a more technological place with the support of a renewed architectural and design culture.

The correspondence group estimates that this analysis reveals a major opportunity for standardization in ITU-T and with other SDOs and that this work should be exposed to a larger community to get feedback and both amend, confirm and develop a powerful new approach in a very shared security standardization ecosystem.

10 Short term impact to SG17 structure

The correspondence group identified immediately and with a great sense of urgency the requirement to address innovation in SG17 with the paradox that mandates are set for a 4 years study period, an eternity in terms of developments in cybersecurity.

The correspondence group developed what is now called the incubation mechanism. The goal is to allow innovative new work items to develop in an incubation queue allocated to a question carrying this mechanism so that it would decrease the pressure to arbitrarily and randomly change current question texts. This will allow the correspondence groups to develop a mid and longer-term strategy.

The incubation mechanism was subject to much debate but managed to start at a time when quantum key distribution and other quantum contributions arrived at SG17.

The pilot started at a high cadence and one by one tested all of its aspects over a period of 2 years.

This pilot had been successful beyond all expectations providing a number of benefits for the delegates and the study group itself, allowing for much more consensus in SG17 meetings as it helped to streamline correctly the process for innovation in a very organized and lean way.

It also allowed a number of new ideas to flourish while giving credit and importance to the development of Technical Papers and Technical Reports before any fully normative work, allowing an entire community to be on the same page and allowing a much better development process.

The whole incubation mechanism is detailed in a dedicated Technical Paper [1b-Incubation].

11 Mid-term impact to SG17 structure

Once the short-term approaches were put in place and while they were being developed, time marched on to the mid-term of the study period and a new urgency arose to seize the opportunity to change Question texts. Changing Question texts requires time and TSAG approval.

The correspondence group worked to support a number of rapporteurs in the transformation of their Question texts.

The fact that the long-term strategy period was nearing at the same time allowed things to be put in perspective, posed some hard questions, and influenced significantly Questions strategies.

Q2, Q4, Q5, Q6, Q8 Question texts were changed with the support of the SG.

Another mission that the correspondence group accomplished was to support Q1/17 in preparing the answers to TSAG regarding the Hot Topics Liaison Statements which showed:

- The importance of hot topics as they impact mid-term changes in questions as rapporteurs want to seize potential opportunities for standardization development.
- The tactical nature of hot topics on the long-term strategy.
- A number of issues at TSAG level which were then being addressed through a specific story based on SG17 experience (not to be covered in this document but showing it had other transformation side effects).

12 Long-term impact to SG17 organization structure

The long-term impact of SG17 structure took multiple steps and collected several approaches and expressed views.

12.1 Different structure models

Some definitions of elements of Questions are provided in Table 7.

Table 7 – Questions' on granularity, density, load and coverage

Question	Definition	Values	Examples
Granularity	Granularity of a question is the size of the scope of its mandate	Small Medium Large	Q4/17 has a very large mandate and so has a large granularity Q5/17 has a very narrow mandate on spam and so has a small granularity Q6/17 has a large mandate on networks and so has a large granularity Q7/17 has an extra-large mandate on application security: large granularity Q8/17 has a narrow mandate so has a small granularity Q14/17 has a narrow mandate so has a small granularity
Density	Density refers the number of sub-items it must cover in its mandate	Small Medium Large	Q4/17 has a medium density Q5/17 has a small to medium density Q6/17 has a large density, it has to cover a lot within its mandate Q7/17 has a medium density, its mandate is very lose Q8/17 has a medium density Q14/17 has a very large density and needs to address a lot of aspects
Load	Load is the work-load activity of a question	Light Medium Heavy	Q4/17 has a light load Q5/17 has a light load Q6/17 has a heavy load Q7/17 has a medium load Q8/17 has a medium load Q14/17 has a very large load
Coverage	Coverage corresponds to whether the current coverage is within the	Fits Expands	Q4/17 coverage fits Q5/17 coverage fits

	mandate or if it expands outside of its mandate		Q6/17 coverage expands in several ways as it supports work items that are at the border of its mandate Q7/17 coverage fits Q8/17 coverage expands as it now carries Big Data Infrastructure work items which are not part of its mandat3e Q14/17 coverage fits but with risks of expansions

The current structure is given a hard limit in terms of the number of questions and if the number of cybersecurity next big things to cover is increasing then the direct consequence is that:

– The granularity of questions will need to increase.

– This will certainly increase the density of questions which are under low density at the moment.

– This will increase the work-load AND the coordination between questions.

– But will keep coverage back under control.

Deriving a prototype under these assumptions will be called the high granularity class of prototypes.

But a radically different view exists, noting that today due to hidden dependencies:

– Questions are the focus of SG17 versus Working Parties.

– We run SG17 meetings, not Working Party meetings.

– In a typical 8 days meeting we allocate.

  - 3 days to opening plenary, working party reports and closing plenary.
  - 5 days to run all the questions in parallel.

The new thesis here is that:

– Questions could run in less days and therefore decreasing the granularity of questions could allow for more questions in SG17 say 20 but which would then run in 2 batches of 10 questions in parallel for 2 ½ days and another 10 in 2 ½ days;

– Optionally there could also be Working Party meetings separate from SG17 meetings (which to some degree has been pioneered in the interim question meetings).

Whilst it is allowed to have Working Party meetings there is an interesting context-based ITU knowledge. There are in fact 2 types of Study Groups:

– Very technical Study Groups can run Working Party meetings without issues.

– Very policy and member state driven Study Groups can be run only by Study Groups meetings.

SG17 is neither one nor the other and is actually unique in ITU as it has both aspects equally represented. So having Working Party meetings to help redistribute the work would cause a problem to government administrations to sustain more meetings.

Yet the Working Party level of SG17 is under-represented and might be called to play a bigger role in the future.

We can certainly develop a creative prototype here and ask ourselves critical questions to obtain useful data points on whether such a prototype could help.

As clear benefits we would end up with:

– More questions but with a smaller granularity;

– With the implication of less coordination between questions;

– A reasonable density and therefore a reasonable load; and

– A more controllable coverage.

It adds other advantages in that it can allow new leadership positions and therefore invite more external experts to complete and augment SG17.

For example, in the same vein of DLT being its own question, we may expect to have questions dedicated solely to:

– AI/ML

– Quantum

– 5G security

12.2 The high granularity model – A first attempt to change the structure

Based on this new way to read the situation as per above, a High Granularity Prototype Class was proposed for SG17 as a first attempt to change the structure with a few remarks:

– This analysis showed that in whatever scenario Q8 owning big data infrastructure was a stable decision.

– Conversely the discussion of Q4, Q5 shows that the revision texts of both are not stable yet.

Both above remarks show how the long-term discussion can help the mid-term discussion too.

We note also that the question on whether Q11 should own the work on blockchain and PKI is relevant as ISO SC6 working group mandated Q11 to conduct this work which shows the importance of understanding the requirements, limits and constraints under which SG17 operates.

12.3 The CNPD model

The cloud network platform device (CNPD) model was established with the intention to keep the structure of the study group close to a technological decomposition called CNPD, see Annex D.

12.4 The 'army' analogy model

This model (see Annex E) was made on a military analogy by which:

– Working party levels are like high level army forces (air force, navy, ground forces, etc.);

– Questions are like an army base;

– Work Items are like a military task.

It implies that

– Working parties are very stable;

– Questions are more volatile;

– Work Items are projects with a lifecycle.

It also suggests the recognition of a main/"mother" question in each Working Party.

12.5 The 'house' analogy model

See Annex F.

12.5.1 Establishing the story

Establishing the story was possible only after having gone through the previous logical structure and strategic thinking. It also created a level of credibility in prompting business executive leaders of CSPs and OTTs to get their feedback. In essence the question to them was:

What 'story' would give you the appetite to join or come back to ITU-T SG17?

This question is actually valid concerning any constituent of the DSP ecosystem.

12.5.2 The proposed new story

Considering all the above methodological and analysis work, and after consultations and debates, the proposed new story was established as:

SG17 should produce coherent and high quality technical standards that ensure that end customers have trust in the digital service providers (DSP) services that they receive and can be offered security value if they require it in a constantly evolving arms race with cyber adversaries. SG17 should create these standards in an efficient, effective process focused on the needs of the participants without gaps or overlaps between the work items

13 Conclusions

It delivered a significant number of outcomes for short, mid and long-term which provided many benefits for SG17 and its members, pioneering a new incubation mechanism, allowing innovation to flow in the study group, to support changes in question texts, to address hot topics and to propose alternatives in the structure of the study group.

As a result from a strategic thinking approach a new area of development was identified based on the recognition of the need for an increased security architecture development (now a new correspondence group) and an opportunity concerning operational security.

This work helped several member states in their own transformations of their national security strategies, as well as increasing the maturity of the team over time to address more complex and valuable horizons.

As such other organizations seeking to perform a transformation of their security approaches could consider the approach taken in this Technical Paper and/or the lessons learnt on how to provide the right conditions to allow change to happen.

Annex A

Inputs to strategic thinking

This annex regroups a number of inputs to the Strategic Thinking.

About SWOT approach

Establishing a strengths, weaknesses, opportunity and threats (SWOT) approach helps drive the strategic thinking and we note the following contribution at TSAG RG-SS that establishes the 'weaknesses' component of the SWOT study for ITU-T based on observations at SG17.

Identified 'weaknesses' include:

- Lack of product architecture skills:
  - There is a disproportion of researchers and member states at the expense of very few product architects.
  - As a consequence, current Recommendations are mostly at framework or guidelines level but rarely are there any Recommendations at product specifications level.
  - This has major consequences on how Recommendation users recognize or do not recognize the value of ITU development.
- No feedback loop on the Recommendations and no user representation:
  - There is a complete under representation of the users of the Recommendations with NO FEEDBACK loop. It does not seem possible to have proper measures on how and where the recommendations are being used, if they are good or not.
  - If a Study Group was a business this would be an absolute NOGO.
  - We assume too that if a user would like to leverage several Recommendations from within the same Study Group and across Study Groups the feedback would be:
    - Syntaxes are not necessarily aligned
    - Semantics are not aligned
    - There are overlaps
    - There are contradictions
  - There are a few good examples though such as in security: X.509, PKI, OID, X.500, etc. but we have no concrete codifications of these successes that are used extensively.
- How to address composition and the lack of a Chief Technology Officer (CTO) function and design methods:
  - A fundamental issue is the problem of composition. How to compose Recommendations that are volunteer contribution driven in nature and may overlap or even conflict.
  - Because the process is bottom up coming from Recommendations it is extremely difficult to do arbitrations because there is no 'mechanism' to support this.
  - There is a lot of parallelism with normal business here and in general arbitrations are managed by CTO offices and this is done through proper design methods at architecture level.
  - Such a top down approach could force contributors and editors to consider a set of design criteria for their Recommendations that will generate:
    - Systematically addressing the criteria with many benefits for the Recommendations.
    - A fair method to 'neutralize egos' and allow teams to concentrate on fighting together for the right and optimized solution.

    - As new information often arrives, generate new abstractions, this can reveal hidden dependencies, create new interfaces and in other words generate new value.
  - A good example of Design principles is found in TD1954 of SG17 though Symantec will generalize them in a contribution for the SG17 August meeting.
- What is success?
  - There is no clear and perhaps even worse wrong measurement of success.
  - This is perhaps due to the fact that the Study Group real work is under-represented at PR and marketing level and so the only success points are the subliminal messages that Study Groups are addressing to other SDOs or even within ITU about 'look we created a new question'.
  - A clear definition of success and measurement is required and should be enforced in order to 'raise the bar' and help:
    - Provide and formalize more guidance on New Work Items acceptance
    - Improve the development of Recommendations
    - Provide Excellence Standards
- A deficit in perception:
  - We also observed a gross deficit in perception with too many negative messages propagated.
  - Symantec Corporation does not think this is correct, or justified, or even fair but at the same time recognizes that the communication on what is the true nature of the work is completely absent from a public relations and marketing perspective.
- There is a lack of alignment between ITU-T and ITU-D:
  - If and when ITU-T and ITU-D can be properly aligned on what should be the 2 pillars of the ITU-D, i.e. projects and capacity building, this would potentially be of huge benefit for the ITU.
  - We are asking ourselves a lot of questions on how a given Recommendation can generate projects and capacity building and positively impact all the parties.
- From ideology to reality:
  - Where is the win/win/win between companies, ICT+OTT and end markets?
  - Failing to recognize this link will lead the strategy to ITU-T, to a solely ideological approach and we believe, will make it irrelevant.

About interviewing rapporteurs

Mindful of the C3 constraint, the team tested and evaluated a method to get feedback from rapporteurs and associate rapporteurs in a spirit of transformation by design.

Indeed a few individual interviews were carried out and proved extremely valuable for obtaining intimate feedback with rapporteurs and associate rapporteurs. They gave very useful suggestions for their Questions but also revealed information on new skills they had learned over time, new areas and many other experiences of leadership in other SDOs.

In order to better leverage this experience capital, it was agreed that it would be of significant value to SG17 to conduct interviews. Currently SG17 management are running such interviews, which take 1h30 to 2h on average and may require multiple calls to allow people a chance to understand their own position.

A proposed 'interview script' could be reviewed by SG17 management and if there is consensus on the approach, the proposal is that these interviews would be run by a Working Party leadership team, properly documented and then presented back to the SG17 management team for analysis in an aggregated report.

See Annex C

About market dynamics

There is no doubt that the ICT ecosystem has been evolving and transforming at a high cadence under pressure from a monumental mega trend called digitalization over the past few years. Whilst this mega trend can trace its infancy and genealogy in a multi-decade history, we will concentrate here on a model to help guide our strategic thinking.

Let us start with a few definitions first:

Digital service provider (DSP): an organization delivering a digital experience as a service to others.

The DSP ecosystem is composed of constituencies that are in heavy co-competition and that themselves evolve in this ecosystem to a degree that some constituencies could grow, while others could disappear. Table A.1 describes constituencies of the current DSP ecosystem.

Table A.1 – Constituencies of the current digital service provider (DSP) ecosystem

Acronym	Definition	Comments	Example
CSP	Communication service provider	In other words, operators, MNOs, etc.	AT&T, DT, China Mobile, etc.
NEP	Network equipment provider	Also referred as 'the vendors'	Ericsson, Nokia, etc.
GSI	Global system integrators		'Telco divisions' of IBM, HP, etc.
OTT	Over the top	Another word: Business Platforms	Facebook, Google, Alibaba, etc.
ISP	Infrastructure service providers	Meaning IaaS, Public Clouds	AWS, Microsoft Azure, etc.
MSP	Managed service providers	3000 in Germany, 1000 in France, etc.	Business Connexion, etc.
CSB	Cloud service brokers	Niche category which will probably fade but enabled a critical capability of Market Places	Ingram, AppDirect, Bearing Point, NEC Netcracker, etc.
ENT SP	Enterprises Service Providers	Enterprises who must become service providers because of their OT business under the pressure of digitalization (IoT, etc.)	Oracle entering 5G, Car companies looking at 5G for their cars, Train companies, etc.

What we observe is that over the past 10-20 years the ecosystem evolved as shown in Figure A.1

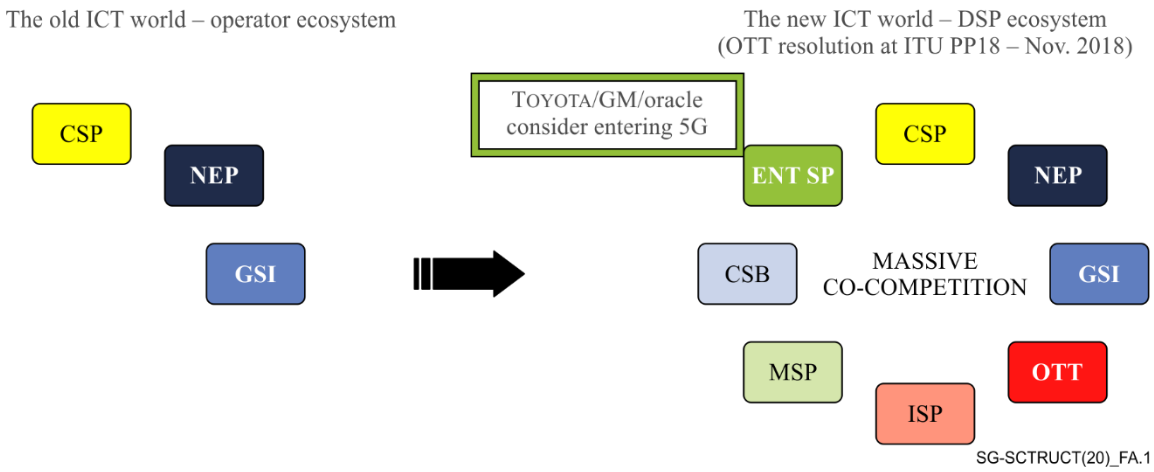


Figure A.1 – Industry dynamics

Now if we take an analogy with astronomy, a good analogy would be the one of a solar system establishing itself with several gazillion giant planets and tectonic planets formed or forming while some collisions are destroying some others and while numerous planetoids are still finding their own course.

Yet we need another instrument to help us see the market dynamics as now we only have an external view of 'the system'. This is with an old-school business analysis tool from Michael Porter also called the '5 forces' where when we move the referential of observation to one of the constituents, for example here the CSPs (the operator) we can now see the picture as shown in Figure A.2.

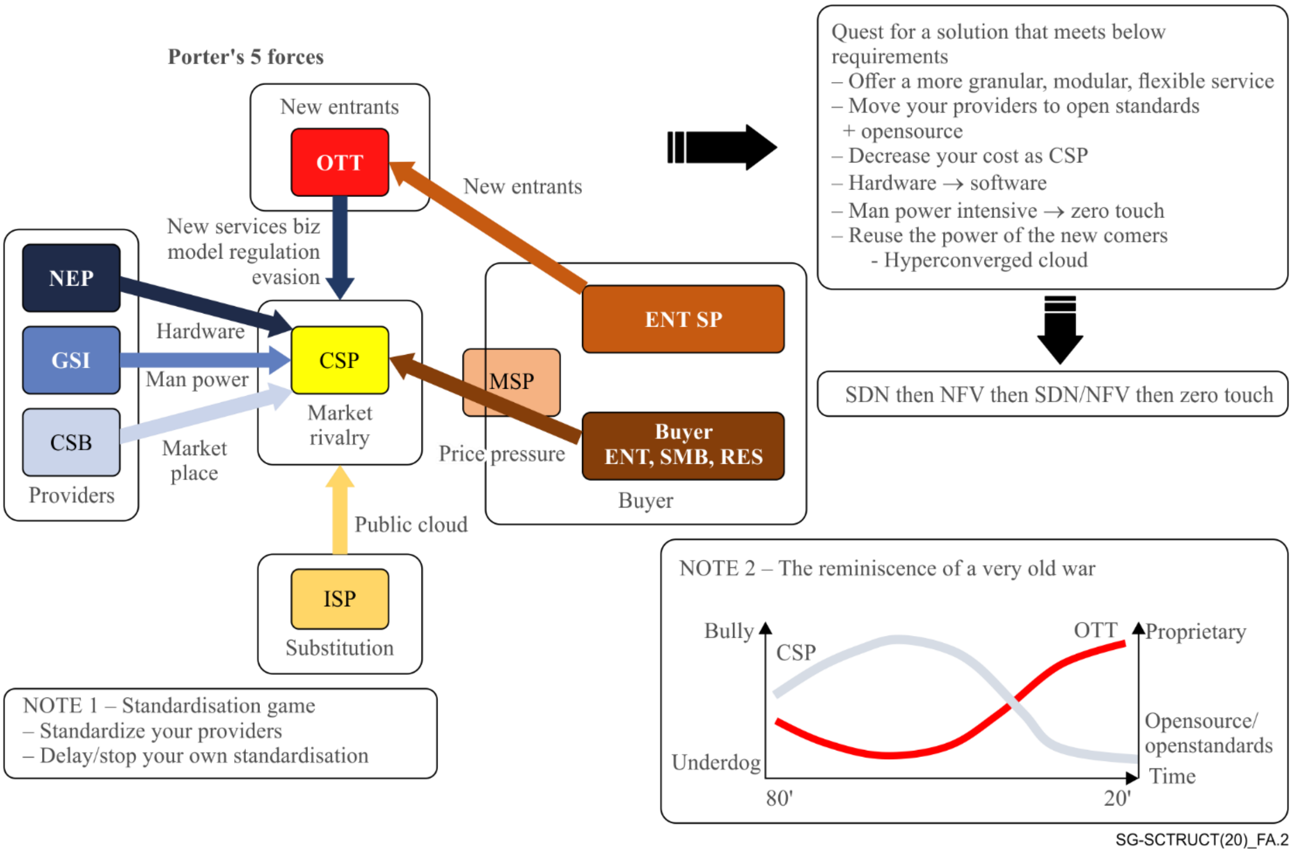

Porter's 5 forces
New entrants
OTT
New entrants
New services biz
model regulation
evasion
NEP
GSI
CSB
Providers
Hardware
Man power
Market
place
CSP
Market
rivalry
MSP
ENT SP
Buyer
ENT, SMB, RES
Buyer
Price pressure
Public cloud
ISP
Substitution
Quest for a solution that meets below
requirements
– Offer a more granular, modular, flexible service
– Move your providers to open standards
+ opensource
– Decrease your cost as CSP
– Hardware → software
– Man power intensive → zero touch
– Reuse the power of the new comers
- Hyperconverged cloud
SDN then NFV then SDN/NFV then zero touch
NOTE 1 – Standardisation game
– Standardize your providers
– Delay/stop your own standardisation
NOTE 2 – The reminiscence of a very old war
Bully
CSP
OTT
Proprietary
Opensource/
openstandards
Underdog
Time
80'
20'
SG-SCTRUCT(20)_FA.2

Figure A.2 – Porter's 5 forces applied to the new DSP ecosystem; centred on CSPs

This picture provides us with a lot to consider as we observe:

- the implicit democratization of technology and inevitability of 5G at a much more accelerated rate than it was with all previous network generations;
- an example (SDN, NFV and ZTM) of technical heavy transformation critical for CSPs to reinvent themselves at, to some degree, the expense of NEPs and GSIs in both their fight and their collaboration with OTTs;
- the growing role of verticalization in a world where the ICT focus will move from B2C to B2B and B2B2C which will accelerate the change for verticals from customers to new entrants as they are also by default service providers;
- the fundamental genealogy of why this is happening, not by accident in cycles that started nearly 40 years ago.

How impactful is it for standards? And specifically, for security standards:

- It is very impactful because we see a massive set of interoperability problems between these constituencies already materializing on the key issue of business onboarding.
- When 2 businesses such as a CSP and an OTT agree to make a joint delivery, it requires an onboarding of technical capabilities which needs to be aligned a huge amount of cybersecurity requirements between the 2 parties, as well as compliancy requirements.
- We see too that as this market grows, standardization could also be toxic, and regulators could make mistakes or civil society might be too dogmatic so there is a delicate balance.

About hot topics

Hot topics matter as they inform the tactical aspect of the transformation leading to concrete developments and decisions on the structure.

In recent years, ITU-T Study Group 17 has been devoting a significant part of its management resources to coordinate and prepare necessary structures for next gig things (NBTs).

Specific instantiations of NBTs such as cloud computing, big data, Internet of things, ITS, EDR and blockchain (see Annex B for a more complete list) changed from time to time and were the source of intense Liaison Statements between SG17 and TSAG which could help SG17 to consider potential new hot topics.

Since many of the NBTs have profound technical and economic impact, SG17 came up with inventive uses of management structures to deal with each of them, including the creation of new Questions. It is also worth noting that specific NBTs of interest shifted from time to time within SG17.

However, from a cybersecurity point of view, it could be considered that these NBTs are simply different instantiations of the same set of modular building blocks:

- Endpoints
  - as defined by being both end points of a communication and therefore covering, the user equipment or the things with which the user interacts, as well as the hosts in any form, from physical to server-less;
  - as modelled in a uniform way with their processor, memory, etc.
- Communication protocols
- Software and applications
- Human interfaces
- Sensors

If this is the case, then those Questions which are modular in nature should try to remain agnostic to specific technical instantiations as much as possible and remain a reliable contact point and source of expertise for multiple study periods. We believe that good technical Recommendations should be applicable to any of the NBTs over the course of their technical evolutions, as they are built with the same set of building blocks.

Likewise, other good standards from Q10/17, Q11/17 can be applied to any of the NBTs over the course of their technical evolutions – they remain a reliable contact point and source of expertise for respective technical topics, e.g., identity management, digital certificate and object identifiers.

Good technical standards are modular, and they are meant to be able to be composed for particular technical instantiations by subject matter experts who understand the target technical domain as well as the suite of standards.

What we learn here

When considering new areas for study, SG17 should consider all options, which might include the work being consolidated in a single existing Question, the creation of a new Question or the work to be carried out in a coordinated way across multiple Questions.

Annex B

List of potential next big things

Table B.1 provides a list and descriptions of potential next big things (NBTs).

Table B.1 – List of potential next big things

NBT	Short title	Description
NBT01	Artificial intelligence (AI)	Artificial intelligence is one of the deepest and most disruptive innovations that has resurged after 25 dormant years, with considerable impacts on our societies that will be visible imminently, with job losses for thousands of people. Currently, artificial intelligence and security can represent multiple dimensions: – Security for artificial intelligence – Artificial intelligence supporting security solutions – As counterpart to the above, the implications of artificial intelligence supporting cyber-attack weaponry (against the above) – Artificial intelligence to conform to security conditions We should also consider here the critical intricate topic of privacy and finally both security and privacy together. This will span the entire end to end journey of a user from when he or she is not even connected, to the user experience (direct or indirect, device or thing), to the digital persona(s) accessing an application which generates sessions across an entire infrastructure with boxes and middleboxes to finally reach a server to which is attached big data with analytics, and artificial intelligence. Artificial intelligence will not just be in the final data lake, it will be across all the constituencies of the experience. To a degree it could be the backbone of the entire security and privacy defence line.
NBT02	Quantum resistance	Quantum safe cryptography and Quantum key distributions are essential to the long-term resistance of any digital life. This is a major problem to be addressed within a 10 year horizon, yet is facing the challenges from the high incentives of the Quantum computing 'attack' weaponry to succeed sooner. The are several implications e.g., firstly on how to decrypt stockpiled encrypted data by adversaries and then on architectures and necessary middleboxes between the various segments of encryption will lead to interesting risk management considerations.
NBT03	Digital humanities	In academia there is a growing momentum to understand the position of the human being vs digital experience and how today the current solutions to ensure both individual security and privacy are limited, often with priorities put on privacy at the expense of security. This hides the whole question of how to bring back a truly seamless security and privacy user experience that would enable a respectful and visible trust in the future digital world.
NBT04	Robotics	Robotics will become more prevalent because the incentives to resolve todays problems in all the verticals including support for dependent people (elderly, affected by cognitive illness) to mitigation of severe threats to the viability and sustainability of our societies. At the same time robotics pose considerable societal issues, the first of which is like AI the fear of seeing a raise in

Table B.1 – List of potential next big things

NBT	Short title	Description
		unemployment rates. The hundreds of billions of funds being raised by certain organizations right now are simply providing the tone. Unfortunately, recent stories showing small robots 'assassinating tomatoes with a screwdriver' are showing the potential of the nightmarish 'Chucky doll movie' to the reality of robots. Clearly, the prophetic books of Isaac Asimov are now becoming a real problem that will require a number of security and privacy principles to be put in place. Again, how do we secure a robot and how a robot can be used as a (cyber) security weapon or conversely how it can help in defence, while respecting privacy.
NBT05	Cyber insurance	Selling anyone on the idea of adopting / acquiring / buying a security solution is hard. However if you turn around the problem rather than saying 'do you want to buy this door locker or this security surveillance' to 'do you want to have an insurance against this risk' the discussion is suddenly much easier with insurance companies using this discourse for a very long time. With the right skills, the right business models, the expertise, the know-how to measure risk, etc., coupled with the trend in regulatory places to push for significant certification programs for cyber security, this will result in a massive incentive for cyber insurance. Basically, cyber insurance solutions all have the same problem: How to measure the cyber risks and how to access the right data and therefore there are significant interoperability issues for exchange of data. We can expect various requests for standardization here.
NBT06	Big data	Big data is now solidly anchored in a growing number of organizations. Big data is maturing and the need to understand how to get it secured as well as how it can help to support the tools that allow securing of other constituencies makes it a core topic for study. Of course, the key question is what guarantees can we expect from big data providers, and how can we prevent for example the 8B identities that were stolen in the 8 years prior to 2016 from happening again. Besides the analytics part that causes all sorts of issues concerning the nature of how this is implemented today. If today this is not in itself an NBT it is still a topic that needs to find its proper place and guidance within SG17.
NBT07	Cybersecurity services	Cybersecurity from the point of view of tooling has been comprehensively addressed for a long time by Q4/17 and other SDOs, however cybersecurity services where people are actually managing the various security products and processes to deliver a security service with a customer providing recommendations for mitigations and analysis is an area that needs to be addressed in a Question and that can offer good matter for standardization. In fact, as this is the highest level of security and is really the pinnacle of the protection, it of course leads to deep questions on how many cyber defence centres can we really raise given the severe problem of skills available today and in the future. Requirements for standardization are there as a matter to decrease as much as possible labour intensive aspects as to be honest the world will never manage to train 1.5m or more cyber security specialists by 2019 as announced by IDC. In this sense cybersecurity services have no place in Q4/17. However, IF Q3/17 would be redefined as the Question supporting the overall

Table B.1 – List of potential next big things

NBT	Short title	Description
		area of services managed by people (and not the technology) we could then very easily agree that its place should be in Q3/17. This would therefore avoid the ossification constraint (see C8 in Table 3).
NBT08	SDN/NFV	Today SDN/NFV is becoming a reality and a condition for 5G security, however today it is one aspect of the Q6/17 charter. However, a close look at SDN/NFV would make it appear very close to a hyper converged cloud computing fabric (especially NFV) and is closer to Q8/17. In this example it is interesting to think that if Q8/17 would be re-chartered as an infrastructure Question in the future, a way to avoid ossification (see C8 in Table 3) would be to regroup these items.
NBT09	EDRs	Event data records (EDRs) are an interesting topic to study and a growing one, yet we should distinguish 2 elements here: – The EDR as a business EDR (the speed of an engine, the temperature of a pico tube, etc.) – The EDR as security event data record, meaning security data that can be generated and used by security products Both are important topics and require standardization and interoperability. Schemas agreed and shared would be a pre-condition to allow a real unified security strategy across security constituencies to reinforce a very loosely, if at all, coupled portfolio today in most organizations.
NBT10	5G security	5G security is in effect arrived in the market in 2018 and not in 2020 or 2021 as the EU requested. This is both an opportunity and a serious problem as a lot of issues were already an 'after thought' and as a well-known and respected standardization leader said: How can we offer a security standardization portfolio if we do not know the business model of 5G. This gives the tone of the challenges that we are expecting to encounter in this area and the significant issues in offering a decent security paradigm for 5G.
NBT11	Platforms	While today all the tech-giants are building proprietary platforms offering APIs and web services at the edge, we have not yet realized that perhaps this is an area that will require a significant amount of work in the future. The contrast with the operators who came from proprietary constructs from NEPs to an open digital market based on SDN/NFV is to be considered and it is possible that in the future that new regulatory requirements open the possibility to offer standards in this area, between big tech-giants' platforms and other participants in the overall digital service provider ecosystem. To start with (and this is not just an SG17 problem but an ITU problem) this NBT pauses the heavy semantically loaded Question of what is an operator today and what if a whole ecosystem of players under the banner of Digital Service Providers (CSPs, NEPs, GSIs, OTTs, MSPs, ISPs, CSBs, and Enterprises that are becoming service providers due to digitalization) force this definition to be revisited. It would certainly open a critically important way for security and privacy in order to allow this entire ecosystem to offer a frictionless security with automatic mechanisms for alerting, detecting, protecting and mitigating between themselves, making our societies much more truly resilient to attacks. A very minor but edifying

Table B.1 – List of potential next big things

NBT	Short title	Description
		signal was found in the consent of X.dsms at the last SG17 August meeting that in itself showed the painful constraint caused by of this lack of definition.
NBT12	IoT	Of course, IoT is a big topic and while it has started to be addressed security and IoT might require more focus.
…		

Annex C

Interview model for rapporteurs

Transformation concerns a number of aspects, such as organization, but it is also about leaders themselves and where they fit in the current vs the future organizational structure. A lot of knowledge, experience and vision lies in the organization leaders but was this information collected and assessed? The correspondence group developed and proposed an interview model for the rapporteurs.

At this stage, the team agreed that by no means, should interviews be, or be perceived to be, performance reviews.

The spirit of this interview is how rapporteurs and associate rapporteurs tell us about their own journey and to what they aspire, what is their view on their Question, what future they see for their Question and how they see their own role.

This is an inclusive method to help SG17 have a well-prepared team for when the discussion on WTSA preparation comes around.

With this in mind we propose the following draft script to be discussed at the next Special Session on Transformation of Security Studies at the SG17 January 2019 meeting:

To each Rapporteur and Associate Rapporteur.

– How has your journey been so far?
  - How long have you been working as Rapporteur at the ITU?
  - What other experiences have you on other potential leadership roles in other SDOs?
  - How have you aligned your role as a Rapporteur with your day job in your organization?
  - Have you learned anything new that is under leveraged by SG17?

– How do you see the current state of your Question?
  - Do you consider it is active/inactive? Is the associated work increasing/decreasing?
  - What are the three key positive aspects of your question?
  - What are the three things you would like to improve?
  - Do you use any of the following metrics: number of new work items (NWIs) in the new period, Number of WIs in the work program? Number of approved WIs, Usage of the block of time allocated during SG17 meetings, Attendance increasing/decreasing?

– How do you see the future of your Question?
  - Which are the main directions that the Question should take?
  - Should it stay the same? Should it be more focused? Should it be more generalized?
  - What would be your criteria for success?
  - What are you 'dreaming of' seeing for your Question?

– How do you see your role in the transformation and in the future?
  - To what level can you or are you willing to participate in the transformation?
  - Where do you see your role in the future structure?
  - Are you on the right Question or could we perhaps use some of your new skills more appropriately?
  - What is the support that you can rely on from your country/organization?

Annex D

Example of a potential new structure – CNPD

Figure D.1 shows an example of the potential new structure of the cloud network platform device (CNPD).

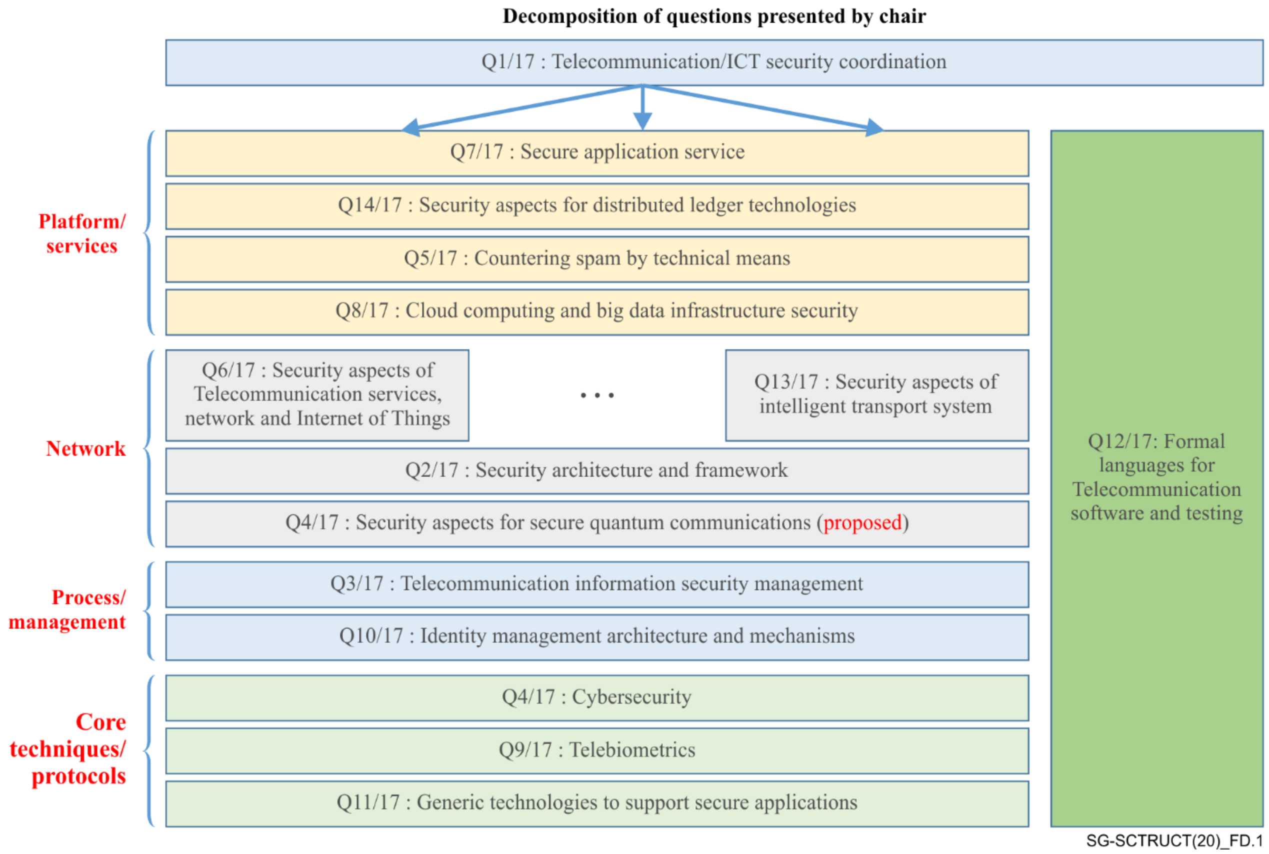

Decomposition of questions presented by chair
Q1/17 : Telecommunication/ICT security coordination
Platform/ services
Q7/17 : Secure application service
Q14/17 : Security aspects for distributed ledger technologies
Q5/17 : Countering spam by technical means
Q8/17 : Cloud computing and big data infrastructure security
Network
Q6/17 : Security aspects of Telecommunication services, network and Internet of Things
. . .
Q13/17 : Security aspects of intelligent transport system
Q2/17 : Security architecture and framework
Q4/17 : Security aspects for secure quantum communications (proposed)
Process/ management
Q3/17 : Telecommunication information security management
Q10/17 : Identity management architecture and mechanisms
Core techniques/ protocols
Q4/17 : Cybersecurity
Q9/17 : Telebiometrics
Q11/17 : Generic technologies to support secure applications
Q12/17: Formal languages for Telecommunication software and testing
SG-SCTRUCT(20)_FD.1

Figure D.1 – Example of a potential new structure - CNPD

Annex E

Example of potential new structure – The Army model

This model, shown in Figure E.1, was proposed by Mrs. Min Zuo in June 2019 as "Q6 in the big picture of SG17" with Q6 being the Question entitled: Security aspects of telecommunication services, networks and Internet of things.

Table E.1 maps the Q6 Terms of reference (ToR) vs identified hot topics

Table E.1 – Q6 ToR vs identified hot topics

Q6 ToR	Identified hot topics
Ubiquitous sensor network (including IoT, M2M)	IoT
Home network	
Security aspects using SDN/NFV	SDN/NFV (deferred to Q2)
Smart grid	
Mobile network (including NFC, eSIM, smartphone and 5G Networks)	5G security
Multicast network	
IPTV network	
PII protection issues in secure telecommunication services and networks	Security, privacy and trust PII protection

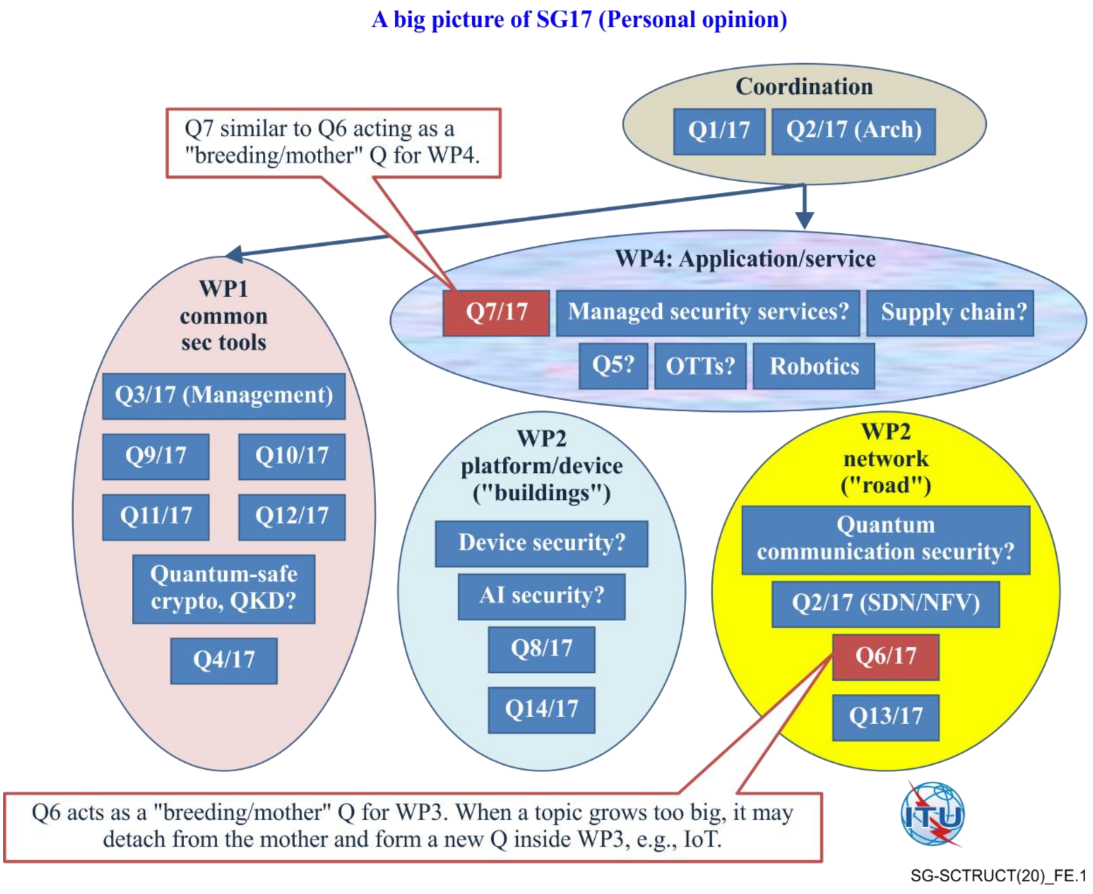

A big picture of SG17 (Personal opinion)
Coordination
Q1/17
Q2/17 (Arch)
Q7 similar to Q6 acting as a "breeding/mother" Q for WP4.
WP4: Application/service
Q7/17
Managed security services?
Supply chain?
Q5?
OTTs?
Robotics
WP1 common sec tools
Q3/17 (Management)
Q9/17
Q10/17
Q11/17
Q12/17
Quantum-safe crypto, QKD?
Q4/17
WP2 platform/device ("buildings")
Device security?
AI security?
Q8/17
Q14/17
WP2 network ("road")
Quantum communication security?
Q2/17 (SDN/NFV)
Q6/17
Q13/17
Q6 acts as a "breeding/mother" Q for WP3. When a topic grows too big, it may detach from the mother and form a new Q inside WP3, e.g., IoT.
SG-SCTRUCT(20)_FE.1

Figure E.1 – Q6 in the big picture of SG17

Some suggestions from Mrs. Zuo:

Keep WPs stable and straight forward and Questions flexible.

- Working Party
  - Analogy of army forces: navy, air force, marine, etc.
  - Should be stable but could change over quite a long time (e.g., someday there may be a space army, or a robotic army, etc.).
- Questions
  - Analogy of a military base.
  - Could be stable for a certain period but may very likely change over time (created, cancelled, moved to another place, etc.).
- Work Item
  - Analogy of a special team for a particular military task.

Annex F

Example of potential new structure – The House model

Elaboration of the potential "Big Picture" candidate for the future of SG17:

Recalling

a) Requirements for establishing a long-term future transformation of security studies as per

- The conclusions of TD669R1 Next Big Things
- The mandates a) and c) of the initial ToR TD782R1
- The continued mandates a) and e) of the ToR in TD1542 from previous CG-xss activities in the current study period
- The list of potential candidates Next Big Things (NBT) in Table 4 of the report of CG-xss TD895
- The special session on the TSAG LS on Hot Topics TD1540
- The LS/o/r on hot topics [to TSAG] TD1617
- Section 2.3 of TD1817
- The forthcoming SDG requirements coming and the feedback/concerns from Symantec on TSAG C53 as per C008 of RG-SS

b) Limits and constraints to the establishment of a long-term future transformation of security studies as per

- Table 1 – List of constraints of the first report of CG-xss TD895
- The limits in page 13 of the above report
- The difficulties to get sustained rapporteur engagement as per 2.1.3 of TD1417
- The generic questions paused by Symantec on the weaknesses part of the SWOT analysis at RG-SS level as per contribution to RG-SS number C007

Recognizing

a) The need for a long-term story as per

- Section 4.5 of the report of the special session of transformation of security studies TD842
- Slides 7-9 of TD1123

b) The vision for a long-term story as per

- Section 4.3 of the report of special session of transformation of security studies TD1268
- Section 2, 4th item and Section 3, 3rd item of the 2nd CG-xss report TD1300
- The entire Section 2.3 on first prototypes for the long-term of SG17 with a full analysis of the key dimensions on granularity/density and the models proposed with a FULL provocative example and 3 models: high granularity, small granularity or hybrid as per TD1417
- Slide 10 of supporting slides as per TD1432 and the associated section 2.5 of TD1433
- Slides 10-12 of supporting slides as per TD1566
- Section 2.4.3 of TD1817
- The further discussion on the 3 long-term models as per section 2.7 of TD1826

c) The specific discussions on the long-term for specific questions candidates for mid-term changes and more as per

- Q4/17 as per 2.2.2 of TD1415
- Q5/17 as per 2.3.2 of TD1415
- Q8/17 as per 2.1.3 of TD1415
- Q2/17 discussion as point 3 of section 2 of TD1716R1
- Q12/17 as per discussion point 6 of section 2 of TD1716R1

Recognizing further

a) The need to consider how to identify and input the rapporteurs views as per

- The need to conduct specific interviews as per item 4 and 7 of section 2 of TD1716R1
- The due considerations and caution of the co-conveners on the topic with the recommendation to get Working Party chairs to run interviews as per TD1827
- The proposed interview template as per TD1830

b) The need to consider the new market dynamics and not just the Hot Topics as per

- The difficulty to get any market data from analysts firms requesting huge fees as per action A06 (despite several attempts meetings and calls) of Table 5 of TD895
- The analysis in the co-convener meeting as per TD2200
- The reasoning with the help of a major operator as per TD2201

c) The need to consider feedback from the 'users' of our recommendations as per

- The co-convener meeting TD2200
- The discovery of the story with the help of a major operator as per TD2201

Concludes

a) The story as defined per a narrative with back to back agreements between the constituencies of the narrative to be moved to **"SG17 should produce coherent and high quality technical standards that ensure that end customers have trust in the digital service provider (DSP) services that they receive and can be offered security value if they require in a constantly evolving arms race with cyber adversaries. SG17 should create these standards in an efficient, effective process focused on the needs of the participants without gaps or overlaps between the work items."**

b) The above story recognizes implicitly:

a. The customer centricity vs the delivery organization

b. An end to end view by design for security

c. TRUST as the implicit existential requirement

d. The option to benefit from security added value services for premium delivery entities

e. The massive on-boarding requirements for security and compliancy services

f. The digital service provider (DSP) new ecosystem

g. The need for a balance between base standards to decrease costs and affordability and advanced standards to allow growth and differentiation

h. The requirement for smooth integration, easy testing and certification

i. To attach hot topics logically

j. To keep a mechanism for constant innovation like the current incubation mechanism

c) The story allows structuring of SG17 efficiently towards achieving this story and suggests a coherent 'house' analogy structure in 4 parts:

   a. the foundation questions;

   b. the enabling questions;

   c. the pillar questions on the core assets; and

   d. the roof questions that ensure the end to end guarantees expected by the customer centricity.

d) The story ensures that each Question rapporteur through the right interview mechanism proposes how his current or future Question can contribute to this goal in the above structure.

e) The story requires that for efficiency the right balance between the 3 potential models for the study group: high granularity, low granularity and hybrid and will prioritize stable high granularity questions with room for a limited set of low granularity questions for specific hot topics.

f) The story requires that the design of the new structure allows, by design, a smooth migration/transformation from the current structure to the new structure. For example a good number of current questions could be changed in a way which is an evolution and not a revolution by changing their long-term perspective.

g) The story also requires arbitrations between the Questions and this arbitration mechanism will be essential to reconcile this top down approach with any bottom up approach.

Recommends CG-WTSA20-prep and SG17

CG-XSS consensus

a) Aim for evolution, not revolution, in the reorganization of Questions.

b) Improve use of Working Party management.

c) Encourage active consultation process with digital service providers.

d) Encourage participation of digital service providers and their vendors in the Study Group meetings.

e) In order to simplify the delivery of technology, incorporate customer perspective and end-to-end perspective in addition to technology provider perspective.

f) Keep a mechanism for constant innovation like the current incubation mechanism in the next study period.

g) The work of CG-WTSA20-prep and CG-XSS should aim for convergence prior to the September 2019 SG17 meeting.

h) Question proposals should be designed to maximize their contribution to the story.

i) The future SG17 structure should reflect the ICT and OTT security market across industry verticals.

j) To recognize that:

   a. most Questions currently have 2 natures: A) They are about securing something B) they are about security itself;

   b. Questions of type A) are about:

      i. A.1) Threat landscape, etc. and security by design of what is under consideration and its limits.

      ii. A.2) How external security components, management and services can protect what is under consideration and therefore make clean interfaces with questions of type B) that will provide the core of the elements.

k) There is a need for a "CTO" function as harmonization, end to end architecture and integration of security that needs to be placed on one Question.

l) Provide specific roles and tasks to each SG17 vice chairs, such as:

  a) Working Party leadership

  b) Chief Technology Officer (CTO) function

  c) Liaison function

  e) Regional group representation

Expressed views in CG-XSS

Note: Many of the expressed views were left as they were originally input by their contributors for transparency. The apparent overlap with the above section is because some of the views were editorially changed. Consensus was not reached on all items.

a) Accommodate new topics without increasing the number of Questions or parallel sessions.

b) Aim for evolution, not revolution, in the reorganization of Questions.

c) Improve use of Working Party instrument to accommodate diversifying agenda.

d) Encourage the Study Group to engage in active consultation process with digital service providers in each Member State.

e) Encourage participation of digital service providers and their vendors to the Study Group meetings.

f) Incorporate customer perspective and end-to-end perspective in addition to technology provider perspective, in order to simplify the delivery of technology.

g) Keep a mechanism for constant innovation like the current incubation mechanism in the next study period.

h) The work of CG-WTSA20-prep and CG-XSS should aim for convergence at the September 2019 SG17 meeting.

i) Working Party should be static, in order to introduce dynamicity at Question level (ref. SG16), with the additional possibility of having one "mother"/innovation Question within each WP.

j) This structural approach should be maintained and stable throughout the Study Period.

k) This structural approach should be led by the story and Working Party and Question proposals should be designed to maximize their contribution to the story.

l) Considering the full-spectrum approach undertaken by the industry, each industry entity will need to infer its own perspective of SG17.

m) The structure for the next study period should take into account that the Question categorization of the current study period (2017-2020) is ambivalent.

n) To recognize that:

  a. Questions have 2 natures: A) They are about securing something B) they are security itself;

  b. Questions of type A) are about:

    i. A.1) Threat landscape, etc. and security by design of what is under consideration and its limits.

    ii. A.2) How external security components, management and services can protect what is under consideration and therefore make clean interfaces with Questions of type B) that will provide the core of the elements.

o) To make sure that Questions do not mix A) and B):

   a. and therefore recognize the need for a "CTO" function as harmonization, end to end architecture and integration of security that needs to be placed on one question.

p) Considering i-m above to align the house analogy structure as shown in Figure F.1:

   a. Roof of the house on the "alpha and omega" of security with a mission to ensure end to end security and therefore the above "CTO" function to support the trust in services of the story as well as to host the security services which carry the ultimate security SLA to the customer (refer to the "story". In addition, this part of the house will look at considering the legacy of X.800 and X.805, etc.

   b. Pillars on the market dynamics (because they are stable) and to consider 3 pillars:

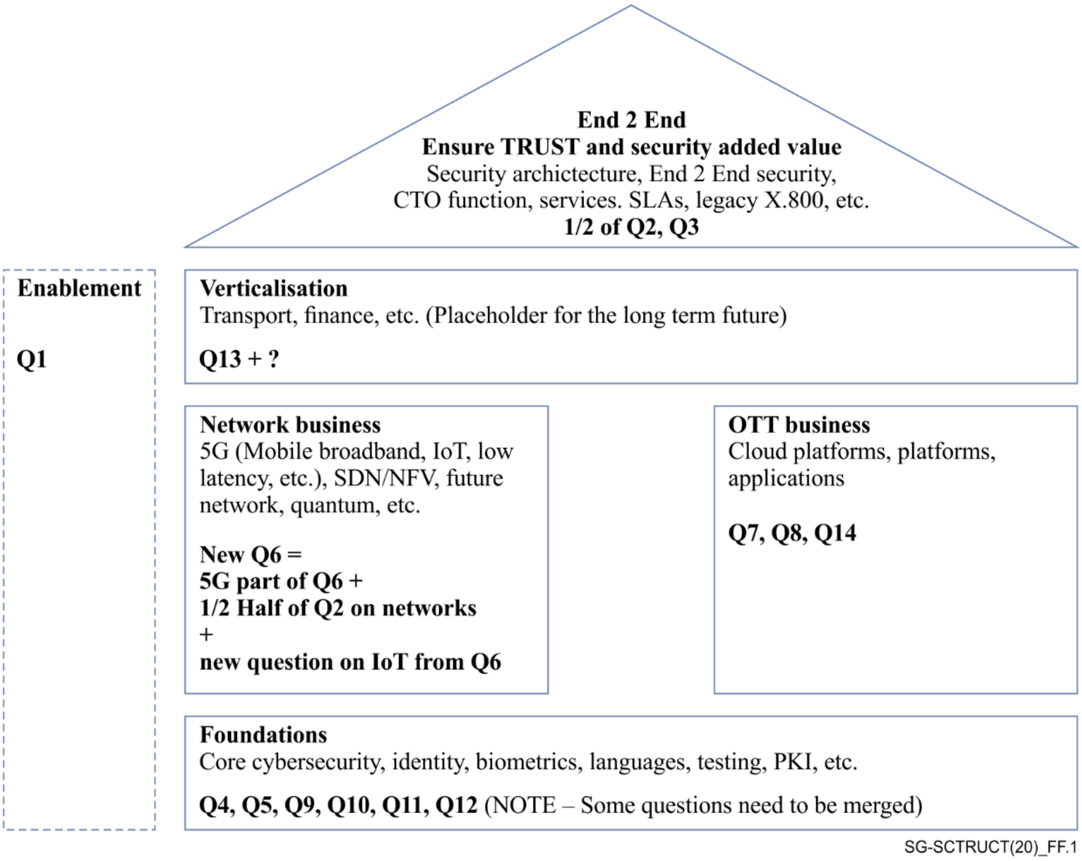
      i. Network businesses

      ii. OTT businesses

      iii. Verticalization (we are not obliged to start with this pillar but can consider for "in 5 years" see j and 2.4 f)

   c. Foundation of the house on the core elements of security.

   d. Enablement of the house keeps coordination as its core.



End 2 End
Ensure TRUST and security added value
Security archictecture, End 2 End security,
CTO function, services. SLAs, legacy X.800, etc.
1/2 of Q2, Q3
Enablement
Q1
Verticalisation
Transport, finance, etc. (Placeholder for the long term future)
Q13 + ?
Network business
5G (Mobile broadband, IoT, low latency, etc.), SDN/NFV, future network, quantum, etc.
New Q6 =
5G part of Q6 +
1/2 Half of Q2 on networks
+
new question on IoT from Q6
OTT business
Cloud platforms, platforms, applications
Q7, Q8, Q14
Foundations
Core cybersecurity, identity, biometrics, languages, testing, PKI, etc.
Q4, Q5, Q9, Q10, Q11, Q12 (NOTE – Some questions need to be merged)
SG-SCTRUCT(20)_FF.1

Figure F.1 – The "House" model for SG17

q) Provide specific roles and tasks to each SG17 vice chairs, such as:

   a. Working Party chairs

   b. CTO functions

   c. Liaison functions

   d. Regional group representation

Invites Member States

a) To contribute in the following ways to the above resolution:

   a. Continuously assess their alignment/misalignment and feedback.

   b. To leverage their relationships in their countries to reach out to the heads of security businesses in the main constituencies of the digital service provider space to offer a chance for an interview session with feedback on the above story or an alternative story.

   c. To qualify what are the impacts from current and potential future resolutions at WTSA level and how the structure can be protected from any attempts at micro-management.

   d. To qualify with their national regulators about how they consider the market dynamics regarding the security space between the digital service providers and if possible with business data.

Invites sector members, associates and academia

a) To contribute in the following ways to the above resolution:

   a. Continuously assess their alignment/misalignment and feedback.

   b. To establish relationships with their own security business leaders to offer a chance for an interview session with feedback on the above story or an alternative story.

   c. To qualify on their own market views and data regarding the security space in relation to the digital service providers new ecosystem and share their discoveries with discussions with their customers and partners.

Bibliography

[b-DOCRA] Hubbard/Sieresen, *Factor analysis of information risk (FAIR), The Duty of Care Risk Analysis Standard* (DoCRA). https://www.docra.org/standard/

[b-Incubation] ITU-T TP.inno. *Description of the incubation mechanism and ways to improve it*.

[b-ASEM] Letens, Geert & Verweire, Kurt & Slagmulder, Regine & Van Aken, Eileen & Cross, Jennifer. (2011). *Integrating Top-Down and Bottom-up Change: Lessons Learned from a Longitudinal Case Study*. Annual International Conference of the American Society for Engineering Management 2011, ASEM 2011.