Broadcom feedback to the draft guidelines for utilization of the GCA

Date 27th of April 2020

Author Arnaud Taddei

# Introduction

Despite being engaged at the last minute, in this document, Symantec Enterprise Division (SED), now a Division of Broadcom, gives feedback to the draft guidelines for utilization of the GCA.

Before reviewing this draft, Symantec needs to clarify a few things regarding how it approached the GCA.

Firstly, this is only in the heat of ITU-T PP18, that Symantec discovered the GCA and that its legendary CEO, M. John Thompson, engaged on supporting the GCA. Yet, as Symantec went through a dynamic life until its enterprise division was acquired by Broadcom last November, currently, no-one in the current leadership team knows about the GCA. Investigating further with peers in the industry lead to exactly the same result.

As it was very clear from ITU-T PP18 that the GCA would become an important topic and in theory not just for the D sector, Symantec studied the GCA in relation to Resolution 130 and security related resolutions in the T sector.

The GCA must have been a huge effort that was certainly relevant at that time gathering the best brains of the planets on the topic but unfortunately lead to conclusions on which Symantec could not align.

Yet, on the way, it allowed Symantec to discover and appreciate the ITU and whilst Symantec used to be an active and supportive D member, Broadcom asked its division to now fully engaged as SED and more generally Broadcom in the T and R Sectors.

Back to the GCA and In contrast to it, Symantec and now SED took a very active role in the transformation of SG17 at short, mid and long term which generated

* A critically successful incubation mechanism that allowed emerging technologies to arrive to ITU
* A mid and longer term strategic thinking which some countries use directly for their national security
* A remarked support to improve the quality and architecture/design of recommendations

With no knowledge of the GCA, a correspondence group of now more than 100 persons with a core group of 20 persons has developed rationale, joint story and made a significant discovery that took all of us by surprise that operational security was vastly under-represented across any SDOs (not just the ITU).

This helped us understand one part of why we are in the situation where we are regarding, e.g. 5G Security, the limits of the Security by Design[[1]](#footnote-1) doctrine, the myiopy on encryption[[2]](#footnote-2), but as well why many programs to develop country security capabilities had issues and/or failures[[3]](#footnote-3), why CIRT, etc. have issues to develop and prompted us on capacity building, why we have such a difficulty to peacefully approach privacy (and not through PII!)

Pursuing the root cause analysis we realized the magnitude and to some degree the violence of the babel tower between the main actors (administrations, businesses, academia and civil society) which participates to the division of the defenders (and therefore why they lose) vs the attackers including now a number of cyber armies.

In this gloomy picture, and at the condition that this cold critique could be fully developed, we could recognize too some key opportunities for ITU and other SDOs. Yet how to organize both the adequate structure, collaboration and coordination?

In other words, it is possible to propose a new story but it will have to find its roots in a correct technological approach and then (and perhaps only then) one can consider organization, coordination/collaboration, capacity building and probably legal aspects too. In short

* The guideline for an agreed technical shared vision in Pillar 2
* Then the development of this story for the other Pillars

With the above considerations Broadcom reviewed the guidelines and observes that perhaps less than 1% of the 150 participants to the GCA were coming from the private sector, wondering how whoever arrived to the guidelines and how it is expected that the private sector could ever participate to implement such guidelines. Is there anyone who thought about the cost that the dilution of resources, of body sharing, inherent to the proposed distribution of work will be? On which “story”[[4]](#footnote-4) is it supposed to convince the industry for a good return on investment?

# Detailed review

## Section 1

1.3 Broadcom has issues in several aspects of C19/58 in section 2 and wondering how a facilitator role can be achieved when the story needs to be significantly reviewed. In addition it is still very confusing on how the GCA framework was used and will be used. As this is coming very early in the document we are wondering how it will affect the rest of the document

1.10 We would disagree with this rosy picture. This seems to only take into consideration the direct positive impact of the ICTs on the SDGs. The SDGs are a very rich set of goals and the design of any ICT artefact may have direct and indirect, positive and negative impacts to the SDGs. There are examples too with cybersecurity actually has negative impacts on certain SDGs (e.g. will lead to too much energy consumption). The text could finish with something in the line of “and Security solutions should seek to optimize their design towards the SGDs”.

1.12 Broadcom is wondering why this is mostly a positive tone and where will be discussed the fact that ALL of these new technologies not only emerged, but are accelerating each other or are required between each other (e.g. you cannot make a large network work without AI, or in 5G it will be just impossible to do it without AI), yet they all introduce a massively bigger attack surface by scale and complexity.

The point on quantum could be improved with

 Quantum technologies offered both a) quantum computing that delivers new computing architectures that allow to resolve problems that traditional computers could not resolve but also putting at risk, inter alia, current cryptography, and b) solutions to quantum resistance by mathematical means with quantum safe cryptography and by physical means by quantum key distribution and quantum information technology.

1.13 why the terms fake news, disinformation and misinformation are not used here?

1.14 Broadcom is wondering what was the intention of this clause as if it is to explain that the threat landscape has changed, then the clause is grossly under-representing the situation. Since 2008 the threat landscape has changed significantly in the arms race between attackers and defenders and any new emerging technology (in 1.12 or 1.19) is used and abused leading now to targeted attacks, ransomware, etc. and the significant increase of a few cyber armies capabilities now at play.

1.19 Broadcom has a massive set of issues with this section as per our preamble. Broadcom understands the intention of Security by Design but unfortunately this leads to limits such as local optimisation of the artefacts security vs end to end security (which will be one of the key problem on 5G), no global model for operational security, security interoperability, Babel Tower effect due to significant tensions between private sector actors, fundamental disagreement on the overall security model. As well no mention of labelling and market education vs certification/accreditation. We precisely disagree on the fact that security standardisation remains a moving target. It is a moving target because no one decided it won’t be otherwise. An out of the box approach could be proposed and would lead to a different conclusions. It is impossible here for Broadcom to propose a fix of this text at this late stage. Broadcom has in mind a more radical approach.

1.24 Broadcom would recommend to go further here and “while recognizing the mutual inter-dependence of the five Pillars, The Technical and Procedural Measures will need a clear prioritization

## Section 2 Pillar 1

Broadcom is engaged on the ITU on technology only. Yet Broadcom is wondering how the legal pillar will be able to cope with the evolution of both the legal landscape, the threat landscape, the industry landscape and the technology landscape changes. Eg. on point 2.5 b) how to technically implement disinformation measures when the first problem is that those attacks are not an attack on any device, they are like phishing attacks, an attack on the brain. What will happen when brain devices will be more widely used as companies develop in this area.

## Section 3 Pillar 2

3.1 Broadcom agrees with this statement but we think it is largely understated and it is not revealing why we are in this situation (see the Broadcom text on the problem of operational security overall strategic and tactical)

3.2 Broadcom agrees with the intention but considers this is understated. “However, tehcnial issues can often be at the root of all the other Pillars”. This clause should be more direct and make the Second pillar should be prioritised over the others as it can offer terminology and concepts that can make the other Pillars more focused and more coherent between each other.

3.3 This clause is not crisp enough. What does it mean ‘somewhat independent’. We are just pointing in 3.2 that it is not. So who is right. 3.2 or 3.3?

3.4 Yes, Broadcom fully agrees with this point and this is why Broadcom is at ITU-T. But why such a generic statement, how does it apply to security?

3.5 Broadcom regrets that no mention was made to the fact that SG17 is proactively engaged in a transformation program which resulted into an incubation mechanism that allowed a number of emerging technologies to start developing along others. That the long term strategy considerations in its transformation have revealed that some countries are actually using these results to develop their own national security, that it leads to a major qualification on the gap on operational security and the architecture of security itself which is now the topic of a separate correspondence group and a significant opportunity for ITU-T and it’s partner SDOs therefore setting the potential story for both pillar 3, 4 and 5

The point on privacy technologies could be avoided and replaced by Technologies ensuring confidentiality, integrity and availability.

3.6 Whilst Broadcom can agree with the intention of SG17 in a coordinating/leading role, it recognized too at the last TSAG the immense difficulty it is going to be be to not only do coordination (there are a few models for that) but to do collaboration in an effective manner will be a major challenge due to the bottom-up nature of the organization and with the strong impression that it will require a significant effort from the private sector to participate cross groups. This clause doesn’t seem to pass the test of the Return on Investment for the industry nor simply the resources that it will require as much as technologies will converge.

3.7 this clause seems to not take into account the competitive nature of the SDOs and their differences, the lack of resources to sustain such a fractalisation, the lack of a joined up story.

3.8 this clause doesn’t seem to recognize that this can only work IF there is a common shared vision and story that can be pre-agreed.

3.9 ITU is a global center of excellence, not the global center of excellence. No SDO is. The point on the private sector should be incentivized … by which magic is this happening? The private sectors who could participate, most of the time have no idea on what is standardisation, let alone what is the ITU or IETF, etc. and when they are aware the cost of the resources, travel etc. is a no-go in itself.

3.10 Again Broadcom is reading this one as a vision with no execution is an hallucination. How can it be achieved when there is no model for operational security which is agreed at any level of what is required to reduce the risk? People who can deliver security services, their knowledge as playbooks, a potential security architecture stack and the possibility for intrinsic security through security by design to be part of the orchestration lead by the above security architecture stack? Today end to end security is undefined, security by design is showing dangerous limits, interoperability between security solutions is very limited.

3.11 It is interesting to note that this clause is made only with ‘protection of the ICT assets’ only in mind. There is no view on the users of the ICT services whether residential or business customers. SG17 transformation of security studies has proposed an alternative here because ICTs are delivering security products to the customers! When taking this approach this is not just certifications of the network elements that is at play but as well the market education through say labelling for cybersecurity which would have a major impact on society as a whole and echoes 1.21 or could support some aspects of pillar 1

In addition in the bullets, 3.11 speaks about security by design but 3.10 speaks about end to end security. Of course, an end to end security strategy is way more costly like good architecture is.

With all of the above, Broadcom would have significantly revisited the guidelines to utilize Pillar 2

## Section 4 Pillar 3

Broadcom cannot ignore the COVID19 situation and is wondering if in addition a new type of MIRAI attack would happen now, would the cyberworld be able to deploy the equivalent of hospitals in 30 hours like in Italy?

Broadcom has developed a different story called the ‘clinic metaphor’ and shows that there is a significant gap that could be fulfilled if the orientation would be given towards professionalisation with a real learning of what the health sector managed to achieve in codifying jobs, services, buildings, etc. depending on which situations.

This story includes the operational security aspects discussed earlier and could help revisit powerfully the whole security stack from people, knowledge, security stack and assets to protect. This could have interesting out of the box approaches for organisations as well as for capacity building (pillar 4)

Secondly Broadcom is recognizing that this Pillar is probably more directed to the D sector, yet Broadcom observes numerous contributions from African or Arab countries to SG17 in regards to their CIRT or other aspects and recently in Q3/17 where now an Incident Response only can be exposed in the context of a Cyber Defence Center (CDC) which encompasses a broader set of services than Incident Response.

Thirdly Broadcom notes that the focus is on national and international levels but there is no mention of the Cyber Defence Centers of the private sectors and in particular the ICTs. Isn’t the remit of the ITU on the ICTs?

## Section 5 Pillar 4

As a continuation of the previous comments, Broadcom notes that there are alternative approaches that could be considered from Pillar 2 to Pillar 3, 4 and now to Capacity Building.

5.2 should insist more on the professionalisation aspect

5.3 again, if the role of the ICTs include the end customers, the ICTs themselves could play a role in awareness and market adoption, good practices, etc. See remark to 3.11.

## Section 6 Pillar 5

Broadcom is overall significantly concerned with the dilution of the effort across SDOs which is making the participation to the standardisation work more and more expensive and close to unscalable. Broadcom would prefer to see an approach by which a sound story developed first in Pillar 2 could help create a shared vision

Broadcom would like to see an efficient international cooperation and whilst staying opened would concentrate on the key security SDOs to deliver on the above shared vision. An honest SWOT analysis would have allowed an easier mapping of the work across SDOs.

A creative model should be thought through to decrease the costs for the private sector and allow a limit “body sharing”.

# Conclusion

In this late review Broadcom sees a number of significant issues that should be addressed in the right format and with proper timing. Broadcom could propose some alternatives in the current thinking. Broadcom considers that the pillar 2 should be prioritized first as this will have a significant impact on all the other Pillars and allow them to be more focused and aligned to a story. As well Broadcom is significantly concerned by the cost implications for the private sector should the current direction be pursued.

1. No this is not because you are secure by design that you are secure [↑](#footnote-ref-1)
2. No, encryption is not equal to security [↑](#footnote-ref-2)
3. As shared by several countries examples at the excellent ITU Regional Cybersecurity Forum for Europe and CIS 27-28 February 2020 Sofia, Bulgaria [↑](#footnote-ref-3)
4. By story we mean a narrative AND the back to back pre-agreements with all the participants that are supposed to deliver on the narrative. [↑](#footnote-ref-4)