UK Contribution in response to ITU Circular CL-19/47

Background. The then ITU Secretary-General launched the Global Cybersecurity Agenda in 2007 as a follow-up the WSIS. The ITU is the sole facilitator/moderator for Action Line C5.

There are 5 strategic pillars :-

1 Legal Framework

2 Technical Measures

3 Organizational Structures

4 Capacity Building

5 International Cooperation

The ITU Sec-Gen formed a High Level Experts Group (HLEG) which met during 2007 and 2008, delivering a report.

Since then, the GCA framework has underpinned many activities both within the ITU, and where the ITU has worked jointly with other organisations. The ITU Plenipotentiary Conference 2018 in Dubai included the following text in Resolution 130 under Resolves "to utilize the GCA framework in order to further guide the work of the Union on efforts to build confidence and security in the use of ICTs". In accordance with that, ITU Circular CL-19/47 was issued, inviting contributions as part of a process to develop guidelines for the utilization of GCA by the ITU. We note that the Secretary-General will publish a report on how the ITU is currently utilizing the GCA. We think that such a report will be key to any discussions related to the GCA and we encourage the early publication of that important document.

Although this is not a review of the GCA framework, we note that **the 5 pillars are the right pillars**. The UK has produced many national initiatives, policies, strategies and documents on cybersecurity, and they are entirely compatible with the 5 pillars developed in 2007. We also note that the 5 pillars are comparable with the architecture developed and used by other organisations, including the 5 Dimensions used in the Oxford Martin School CMM, a scheme which has been used in a variety of international cybersecurity projects, some of which have been run jointly with the ITU. This suggests to us that the 5 pillars are well designed, are technologically neutral and are future-proof. These are excellent characteristics.

Previous and existing initiatives utilizing the GCA framework .

The two most high profile activities are the COP initiative and the GCI, but there have been many others.

GCI, the Global Cybersecurity Index, is the most tangible and practicable usage of the GCI. It is a method by which nations can benchmark their level of cybersecurity preparedness against that of other nations. There have now been 4 iterations of the GCI. The method is based on the 5 GCA pillars. The details of the GCI questionnaire are discussed in ITU-D SG2 Q3, allowing all ITU members to influence the design of the questionnaire. The questionnaire itself is conducted on a member state basis, but the detailed questions cover the contribution of all stakeholders in the preparedness of the nations. The results are published via the ITU web site. GCI is a robust and complete use of the scheme and has become a flagship for the GCA and the ITU. Whereas there are other cybersecurity preparedness evaluation schemes, none combine the number of nations and breadth of information in the GCI. The questionnaire has improved markedly in every iteration, partly because of the BDT wish to innovate and partly because of the level of cooperation withing ITU-D SG2 Q3. The UK has been pleased to participate in the GCI from the first iteration and looks forward to the GCI going from strength to strength in the future and further enhancing the ITU's reputation.

The COP initiative, which has been enacted in conjunction with formal structures such as JCA-COP and CWG-COP, reaches out into a multistakeholder environment. It 'works to establish an international collaborative network for promoting child online protection through information sharing, providing guidance and best practices on safe online behavior, and helping partners develop and implement effective plans. COP brings together partners from all sectors of the global community to ensure a safe and secure online experience for children everywhere'. ITU COP works in both directions, by developing guidelines and advice aimed at the target audience, and by providing a comprehensive mechanism by which entities from all sectors can engage and contribute to this vital work. The ITU COP web pages contain a very useful directory of bodies that have chosen to engage via this GCA-related activity, and it is clear that other bodies that wish to use ITU COP as a vehicle for their work will be welcomed as partners.

<u>Perspectives on the 5 pillars</u>

Regarding the individual pillars, Whereas we do not give specific guidelines at this level, our observations are as follows

Legal Framework. There are a number of sensitivities regarding this pillar, and there are questions regarding the remit of the ITU in some aspects, especially given that there are relevant discussions in the UNGA and elsewhere. The UK supports the principle that all nations should have effective cybercrime legislation, and we further believe that the Budapest Convention provides the best model for cybercrime legislation. There are opportunities for the ITU to work with regional and other organisations to support nations in their development of cybercrime legislation. However, legislation is a sovereign issue for nations.

Technical Measures. The ITU-T study groups, notably SG17, develop relevant Recommendations. ITU-D SG2 Q3 offers an excellent forum for the exchange of best practices. CSIRTs are party an organisational topic but also partly a technical issue, in that they are a repository of technical expertise and data, and provide gateways to the vast amount of assistance available from industry, academia and others. The ITU has a track record of engaging with the many types of stakeholder on technical measures under the GCA framework and we hope that this will continue and improve.

Organisational Structures. Having the right structures in place is key, and the GCA framework has been used to assist nations in developing their national cybersecurity strategies. The nature and remit of the national and other CSIRTs will be key, and we note that GCA framework supports this as well. There was a new element to PP-18 Res 130 'that Member States make efforts to improve institutional environments' which may provide the basis for some future GCA-related work.

Capacity Building. There are many organisations active in cybersecurity capacity building, the UK commits significant resources to the topic, as do others. The nature of the work lends itself to cooperation between different bodies and we note the very important work that BDT undertake in partnership with a wide variety of organisations under the GCA umbrella. There are significant overlaps with other pillars but nevertheless the subject is widely recognised as a topic in its own right. ITU-D SG2Q3 provides an excellent forum for raising issues and reporting progress and we hope that all ITU members will support its work.

International cooperation. This can take many forms, and we should recognize that governments, industry and individuals may have their own rules and preferences for protecting their information. However, the right forms of cooperation are extremely valuable, and the UK has committed very heavily to international cooperation for many years. For example the UK national CSIRT is a leading member of a number of international CSIRT bodies, has very strong bilateral relationships, and regards cooperation with international partners as being key to its operational effectiveness. We encourage other CSIRTS behave in a similar manner We note the ITU initiative under GCA on Regional Cybersecurity Centres and regional workshops and cyberdrills. We hope that GCA will continue to encourage international cooperation as a key element of the framework while taking due account of the need to respect the remit and sensitivities of all stakeholders.

Recommendations

We note that the success of the projects is related to applicability of the 5 pillars. Some projects will relate to several pillars, others to just one pillar. Our first recommendation for the guidelines is that **utilization will be much easier if there is a clear linkage to one or more pillars**. We also suggest that a clear linkage to a small number of pillars is better than a loose linkage to more pillars.

We also note that as cybersecurity has become more of a priority for all stakeholders, there are many more active participants in cybersecurity. This affords a very significant opportunity for the ITU to engage with a wide variety of organisations in order to deliver success. Outside organisations should be able to benefit from ITU expertise, and the ITU should be able to benefit from outside perspectives. Our second recommendation for the guidelines is that **GCA-related activity should involve, wherever possible, a variety of partners.** Linked to this, we note that some of the existing and potential partners will be regional in nature, and that some of the most successfully cybersecurity projects are regionally-based. There are good reasons for this, regional groupings are often the basis for trust and capacity building. Cooperation can only be built on the basis of trust between partners, and trust is more easily built initially between regional neighbours. In cybersecurity it is very often the case that one size does not fit all, and we remain cautious about the relevance, value and applicability of global projects. We believe that in order to produce successful, well-focussed deliverables, **GCA-related initiatives should look to be regional or smaller in nature**, global schemes should be very much the exception. We accept that the first word in GCA is 'Global' but experience suggests that in cybersecurity, global improvements are often achieved by using regional or national granularities. To illustrate that, it is very clear to us that all nations should have effective national cybersecurity strategies, and that regional bodies may well provide excellent assistance to nations in the development of those strategies, and that a global body such as the ITU acting withing the GCA framework may publish a reference document on establishing such strategies, that document gaining extra credibility by being developed in partnership with a number of prestigious partners. We are happy to be clear that even in a regional project that global standards are vital, and we support the work of ITU-T and other SDOs, and we encourage ITU-D, where appropriate, to use recognised international standards in its work. The crucial nature of regional approaches in delivering cybersecurity has been widely recognised and should be made clear in any future documentation related to any or all of the pillars.

Our fourth recommendation is from the UK's considerable experience of cybersecurity projects and is linked to the 2nd recommendation, in that it may be key to attracting the participation of reputable and experienced partners, in fact some may insist that this guideline is in place. We recommend that **GCA-related activities should all be focussed on clear deliverables**, supported by **good metrics** throughout the life of the activity. The report on how the ITU currently utilizes the GCA will be an important background document to this aspect.

<u>Summary of UK recommendations</u>

1. Clear linkage to one or more pillars
2. Joint working with a number of partners
3. Regional or smaller in nature
4. Focussed on clear deliverables, with good metrics.