IGF 2016 Workshop Report Template

Session Title	WS152 - Working Together: Collaborative Security in local contexts
Date	Wednesday 7th December 2016
Time	15h00 – 16h30
Session Organizer	Matthew Ford, Technical Community, Internet Society Hirofumi Hotta, Technical Community, JPRS Japan Registry Services
Chair/Moderator	Olaf Kolkman, Internet Society
Rapporteur/Notetaker	Matthew Ford, Internet Society
List of Speakers and their institutional affiliations	Hiroshi Esaki, University of Tokyo, WIDE Project Nick Shorey, Department for Culture, Media & Sport, UK Government Yurie Ito, CyberGreen Institute, JPCERT/CC Moctar Yedaly, African Union Commission
Key Issues raised (1 sentence per issue):	• How does working together to address cyber security issues actually apply in the local context? • What are the various aspects of the collaborative security approach that work, or that don't work in your situation? • What does collaborative security mean for real practitioners? • How do you get real consensus and collaboration at national and regional levels? • How does the model of collaborative security apply to the Internet-of-Things?
If there were presentations during the session, please provide a 1-paragraph summary for each Presentation	Olaf Kolkman presented the Collaborative Security principles as outlined in a recent paper from the Internet Society. These principles stem from an understanding of the open Internet as an enabler for all kinds of social and economic opportunities. Maintaining the Internet invariants is critical in order to preserve the ability to deliver higher level benefits. However, there are security aspects to each of these invariants, e.g. voluntary collaboration makes it hard to mandate security solutions. The open, interconnected and interdependent characteristics of the Internet require a collaborative approach to security. The principles identified are: 1) Fostering confidence and protecting opportunities 2) Collective responsibility 3) Evolution and consensus 4) Fundamental properties and values 5) Think globally, act locally Hiroshi Esaki presented the outputs of the recent G7 summit where a commitment to a multi-stakeholder approach to cyber security was identified. Hiroshi identified Internet-of-Things (IoT) silos as problematic for interconnectivity. More data sharing and consensual adoption of interoperable technology solutions across business sectors can be a benefit in the case of natural disasters such as

	earthquakes. Security by design and establishing a Security Operation Center are recent recommendations from the Japanese government. Finally Hiroshi mentioned the Internet Governance Conference Japan that have adopted a 10-point set of recommendations for their local environment aligned with the principles established by ISOC. Nick Shorey stressed the support of the UK Govt. for a free and open Internet facilitated by multi-stakeholder mechanisms. He presented the objectives of the UK's recently published national cyber security strategy and highlighted the correlations with the Collaborative Security principles. The creation of a National Cyber Security Centre (NCSC) on October 1st provides a unique opportunity to build effective partnerships between government, industry and the public. Increasing awareness and collaborative work between sectors is key to the approach. Initiatives include real-time information sharing partnerships between government and industry, public campaigns to raise awareness, and best practice guides for businesses. The UK government recognises that resilience is dependent on international capacity building, including support for the CyberGreen Initiative. Yurie Ito presented the objective of CyberGreen to consider an environmental approach to cybersecurity. The traditional approach of borders and threat models is increasingly outdated: actors also need to consider the threat they pose to other users of the network. Trying to identify systemic risk conditions and then proactively and collaboratively remediate those conditions. This is a lot like a public healthcare approach. Metrics and transparency provide the motivation to operators to take action and provide vital information for policy makers. There is a need to change the mindset that says you can protect yourself by yourself – working together is key to making the global network resilient to threats and attackers now and in the future. Proactive mitigation is good for you, but really great for everyone else. Moctar Yedaly explained that the African situation remains one of building capacity both to deliver Internet services and to learn how to secure them. Threats into and out of Africa are not as important as what is happening in other regions, however things are developing quickly. The increasing number of IXPs is helping to build the ground for collaborative security approaches in African countries. The African Union has taken the lead to ensure that we are putting in place an ecosystem that will allow collaboration in the matter of cybersecurity in general. Now establishing the national and regional bodies necessary to allow for good cybersecurity collaboration in future. Collaborations with ISOC, the US State Department, and China (Huawei) are all helping greatly.
Please describe the Discussions that took	There are various approaches to national capacity building including

place during the workshop session: (3 paragraphs)	private sector led, government led, private initiatives, and regional bodies. The diversity of national circumstances mean multiple solutions all based on an understanding of best current practice are the right approach. Trying to incorporate and evaluate feedback is critical. Given the level of private sector development in Africa, regional bodies have an important role. There is a need to ensure that governments understand their responsibility to secure critical infrastructure without resorting to drastic measures like Internet shutdowns. Conversely, while the cyber domain is naturally global, we need to consider the specific needs of discrete geographies when considering cybersecurity practice. Practical measures are inspired by transparent measurements and virtue signalling is important. Funding challenges for measurement activities like CyberGreen are ever-present – messaging about the inter-dependence of cyber-security is fundamental to change minds here. It is challenging to make this argument and make it scale across many operators. We need to demonstrate the positive results of collaborative security to change minds. Incentives to being a good Internet citizen are something that need to be acknowledged and encouraged. Bringing branding power to this will help. Government can be a source of problems too, for example a lack of investment in infrastructure means lots of unpatched devices in school networks etc. become a source of cyber security problems. Internet-of-Things devices are made fast and cheap, but not securely – so how are we going to deal with this global vulnerability?
Please describe any Participant suggestions regarding the way forward/ potential next steps /key takeaways: (3 paragraphs)	Cybersecurity demands a global perspective – setting rules in terms of cooperation. The network is as strong as its weakest link, so protecting yourself isn't sufficient – you need to work with others to build mutual capacity and learn from experience. A culture of sharing increases cyber security but also improves physical security (cf. Esaki's remarks). Building cybersecurity into school curricula from the earliest level and designing programs for policy makers to build a cadre of cybersecurity educated professionals will help. http://stats.cybergreen.net presents measurements to inform the debate. The public sector procurement process can be a useful tool in the public sphere. Regulating to require meeting technical specifications for best current practice may be required. IoT obsolescence and software update issues are very real – getting a cross-industry collaborative approach will be key in future. Product lifecycle management is very important. There are lots of groups working on this issue now, and there are some new technical

	proposals. We also hear calls for regulation, and we expect the debate to get more pressing in the near term. Retailers may have an important role vis-à-vis the global network. Bridging the gap and addressing IoT problems probably have a common answer. Who has the power to address the risks? Responsibility should be shifted from users to device vendors – they have greater power. Once devices have shipped it is very hard to get end users or even operators to address flaws. New devices shipped in safe configurations can help a lot. CyberGreen is considering developing vendor health metrics and the community seems to be moving in that direction too. Convincing those with negative opinions regarding the multi-stakeholder model about the importance of collaboration vis-à-vis cybersecurity will be a severe near-term challenge.