Comment to BPFCybersecurity

Koichiro Komiyama, Deputy Director, JPCERT/CC

1. Is your organization a signatory to any of the agreements covered, or any other ones which intend to improve cybersecurity and which our group should look at? If not, we are still interested in your opinion on the rest of this questionnaire!
   JPCERT/CC is a partner of NoMoreRansomware Project(nomoreransom.org). One of the JPCERT/CC members participate in the process of GCSC Six Critical Norms discussion.

2. What projects and programs have you implemented or have seen implemented to support the goals of any agreements you signed up to? Do you have any plans to implement specific projects?
   For example, China CERT, Japan CERT, Korea CERT have a trilateral agreement on cooperation on cyber security incidents affecting the three countries. This cooperation includes their annual face-to-face meeting.

3. During our review, we identified a few key elements that were part of multiple agreements and seem to have more widespread support and/or implementation. Do you have views around the relative importance of these (e.g. by providing a ranked list), or are there any others that you consider to be significant commitments in these types of agreements?
   These are all important. I personally wonder whether we are at the stage where we all need to work on VEP. VEP is necessary when offensive activities exist within an economy.

4. What has the outcome been of these agreements? Do you see value in these agreements either as a participant, or as an outsider who has observed them?
   N/A

5. Have you seen any specific challenges when it comes to implementing the agreement?
   Every agreement made in the past contains some ambiguity. Leaving a room for interpretation is not merely inevitable but rather necessary because otherwise various actors cannot come to an agreement overcoming their different situations, interests, opinions, and beliefs. However, it is true that ambiguous agreements are hardly enforced. Although the UNGGE Consensus Report in 2015 includes very important items such as prohibition of attacks against CERTs, some parts in the agreement are still left ambiguous and thus requires clarification through international discussions.

6. Have you observed adverse effects, or tensions from any of the elements of these agreements, where specifics may be at odds with intended end results? For instance a commitment that may seem like it improves cybersecurity at first sight or tries to fix one issue, but has effects that lead to a reduction in cybersecurity?

From an incident responder’s perspective, the US-China bilateral agreement had the largest impact . Like many others, we also observed decrease in the number of sophisticated attacks to our constituents. (https://www.reuters.com/article/us-cyber-spying-china/chinese-economic-cyber-espionage-plummets-in-u-s-experts-idUSKCN0Z700D)
International or global agreement can be more effective if global powers are involved.