NLIGF
NEDERLANDS INTERNET GOVERNANCE FORUM

IGF 2016 - Report Workshop #153

Let’s break down silos in cyber security and cyber crime

Submitted by: NLIGF and SIDN
Moderator: Wout de Natris with assistance of Thijl Klerkx
Rapporteur: Wout de Natris with assistance of Thijl Klerkx

Introduction

This workshop was organised around the theme: The identification of best practices in cooperation with different actors working on enhancing cyber security or fighting cyber crime. The novelty to the IGF was to do this in a, well-prepared, 90 minutes session. There was no panel, there were no presentations, statements nor fixed speaking slots. This resulted in an highly interactive debate. The workshop was presented as a fact finding session and organised around several, previously shared, questions:

- Is your organisation able to cooperate and/or share information with those you want to?
- What is the basis of the cooperation?
- What were the main challenges that you had to overcome when establishing your organisation?
- Have you overcome them?
- Were there one or more key factors that were instrumental towards success?
- Can you identify key players that were instrumental in your success?

It is worthwhile to note that the workshop gathered interest from around a dozen organisations in developing nations after we announced the workshop in several online fora. Responses commented on how these organisations struggle with achieving successful cooperation. Despite active invitations to participate (online), this, unfortunately, did not lead to participation in the workshop from these nations/organisations in situ. (Many stated that it was not possible for them to come to the IGF.) The received responses as such are seen as valuable as they provide a clear insight and that a lot of work still lies ahead for these organisations and countries. The best practices presented below can be seen as steps forward towards reaching their goals.

The following organisations participated actively in the discussion: IETF, M3AAWG, First, AbuseHUB, INhope, US State Department (including insight into the G7 network) and Homeland Security, Internet & Jurisdiction, RIPE NCC, NCSA, OAS, CERT-BR and the GFCE. Each shared valuable insight into the way they have organised themselves to enable cooperation, what they had to overcome and what challenges they see in the near future.

The following remarks can be seen as basic prerequisites that, once in place, allow for cooperation, the sharing of data and/or working together towards a common goal that overrides commercial interests and individual gain. Each key word is mentioned separately and is underscored.

Best Practices

Challenge. No matter how different the participating organisations are from each other, most started out from a similar position: there was a challenge that needed to be addressed. E.g. managing and/or mitigating abuse, raising awareness, managing the Internet, establishing cooperation across boundaries c.q. borders, etc. Ownership. Someone or a group of persons addressed that challenge, in a way made themselves owner of that challenge and organised a meeting around the topic which grew into organisations. The room largely agreed that to grow into a success several conditions must be met in one way or another.

Perspective. There has to be a perspective as to the way forward. This was often met by addressing the following. Equality. All the participants all must have the ability to participate and share in equal ways. Trust. Without it no one will ever share information with competitors or outside organisations. Trust models. Several organisations mentioned the way they had organised themselves to enable trust to grow between participants. Often a variation to the traffic light model was brought forward. When all is said and done trust grows between individuals. Time. It takes time and patience to build trust between participants, often over several meetings.

Neutrality. It was also pointed out that creating these circumstances needs hard work. A neutral place to meet in the initial phase, e.g. with the aid of a neutral secretariat or building to meet in, is seen as a good first step and the examples show that it takes multiple meetings before success is met with. Comfort zone. Stepping out of a (personal) comfort zone was a condition mentioned in this context.

Expectations and goals. In these initial meetings an inventory of expectations is made, which allows for goals to be set. Alignment. In this process an alignment to each other's expectations is made. Common cause. This is the only way forward that allows defining a common cause. Commitment. It is important that this is felt and shared by all participants as this leads to commitment to that common cause and the workload ahead.

Once the initial participation has been achieved, other aspects come forward. Transparency and integrity. Processes within organisations of this kind have to be transparent for the participants and those participating actively in projects have to show integrity, which aligns directly with trust. Anonymization of data. Data shared is often anonymised.

Once these circumstances are in place, a framework is created that makes it possible to work with many people from different backgrounds and organisations on large projects that make a difference for all concerned. Critical mass. From there the critical mass is built that allows for real successes. A significant number of participants has to come on board to make a difference in the topic on hand.

Costs and effort. Nothing comes for free. All participating have to put in effort and make costs and/or pay a membership fee to have a chance of success. There were very different examples of funding, including examples of meeting required financial conditions with the aid of initial government support or support from outside organisations that step in to assist in financing or providing a technical solution that aid cooperation to go forward.

Result. It is also important that participants receive something in return. Whether solutions, recognition or value, a result must be the ultimate outcome to make it worthwhile. On the other hand most recognised that there is a sensitivity in this form of cooperation. Participants do not only cooperate but show vulnerability in sharing incidents, even to the extent of reputational damage if others misuse information shared. Here we return to trust, the word, the value that is perhaps the fundament of this all and extremely important to meet. This can only be overcome if the environment is trustworthy and used to learn from each other and not taking direct competitive advantages from sharing.

Regulation. There was a rough consensus that regulation ought to be absent if at all possible. Voluntary. The voluntary nature of cooperation was stressed by nearly all. Regulation ought to be considered as a last resort in the case of failure to solve the challenge at hand. In this context there was a call to review older laws that sometimes make cooperation and sharing data hard. Stimulation. Governments are invited to stimulate cooperation. That is the best way forward. Several examples showed how governments had contributed successfully through stimulation and assistance in creating neutrality. “Stimulate where you can and regulate where you must”, as someone said.

In conclusion.

Although the organisations participating in this workshop are very different, the pattern they presented is clear. The participants were in agreement on the summary presented at the end of the workshop, which is presented, somewhat more elaborately, above.

As an observation we would like to add the following. The IGF is the only conference where all the different organisations meet. This workshop shows the potential of the IGF to grow in meaningful ways and use the knowledge and experience from these organisation.

The approach of a fact finding session proved to work. The participants stated that they found the approach refreshing and were “at work” together on a specific topic. They were actively sharing experiences, gaining insight from others and provided input for third parties to learn from.