Incident Response Working Group Telephone Conference
10 February 2010

Attendees:

Fahd Batayneh, .jo
Bart Boswinkel, ccNSO
Wim Degezelle, CENTR (Observer)
Luis Diego Espinoza, .cr
Yurie Ito, ICANN
Otmar Lendl, CERT, .at
Kristina Nordström, ccNSO
Katrina Sataki, .lv
Jörg Schweiger, .de (Chair)

Apologies:

Paul McKitrick, .nz
Zoran Vlah, .hr

- The Chair noted that there was some preparatory material sent to the list and suggested that this is used as a baseline for the agenda of the call.

- The Chair noted that the Work Plan does not match the Charter since it has come to include much more than what was the initial intent of the Incident Response Working Group. He suggested that the Working Group should stick to the Charter adopted by the ccNSO Council, saying that the Incident Response Working Group should build a contact repository. *Katrina Sataki* agreed that either the charter or the Work Plan should be amended and suggested that the Working Group, in addition should look into the concept of DNS CERT.

- *Yurie Ito* informed the group that the DNS Search concept will be publicly available in a month. She explained that it will give operators better access to resources that can help when dealing with a security threat. The DNS CERT will in itself have no authority to respond to the threat; the response will be completely up to the operator.

- *Otmar Lendl* pointed out that the contact repository should not be confused with operational protection, which would need constant attention from staff, and therefore agreed that the Work Plan should be restricted to only include contacts.

- The Chair suggested that the definition of what an incident is according to the Working Group should be amended to also include registration systems. He further pointed out that the focus of the Working Group according to the Charter should be stability, resiliency and security of DNS, which does not include SPAM fighting or content. Otmar noted that the Confickr threat would fall outside of these arias since it is related to

content. The Chair welcomed the comment and encouraged Otmar to propose an alternative definition that would include threats like Confickr. *Luis Espinosa* noted that he thinks the definition should be moderately open. *Wim Degezelle* and *Katrina Sataki* noted that there should be a clear understanding of what is meant with 'systematic' and 'large scale' if these terms are used to define an incident.

- *Bart Boswinkel* suggested that once the Working Group members agree on a definition it should be presented to the community for feedback.

- *Yurie* sent a suggestion to the email list on how to define an incident and the Chair asked the members to look at the suggestion and provide feedback before the next meeting.

- It was decided that Yuri assisted by the chair will draft a summary of use cases for the contact repository that could be used as a stepping-stone for the Working Group in coming discussions.

The meeting closed