FAQ Trusted Network Initiative

1. Q: Is the Trusted Networks Initiative only open for national users/partners or as well for international stakeholders?
   A: The Trusted Network Initiative is an internationally oriented cooperation initiative among stakeholders. The idea was born in the Netherlands, but the network is not bounded by territory. Trusted Routing, routing internet traffic to other 'Trusted Networks' is already accessible to partners from ten different countries.

2. Q: Is the Trusted Routing, routing internet traffic to other 'Trusted Networks', done centrally and collectively or independently and decentralised?
   A: The Trusted Routing is done independently by the partners themselves. There is no 'central authority'.

3. Q: What is the role of the government in Trusted Routing?
   A: The government does not play a role

4. Q: Does Trusted Routing result in a denial of service for the 'untrusted part of the world'?
   A: Yes, heavy DDOS attacks from the untrusted part of the Internet, cause a denial of service. Trusted Networks that participate in the Trusted Networks Initiative, can reactively choose to use the Trusted Routing service as a last resort measure. This ensures that the participants can maintain and uphold the critical connectivity between important applications and the 'local' access networks during such attacks independently from traffic with the untrusted part of the Internet.

5. Q: Is Trusted Routing to other Trusted Networks only designed for emergencies or can it be accessed permanently?
   A: Trusted Routing to Trusted Networks can be done as well during emergencies as last-resort measure, or permanently for risk mitigation.

6. Q: What is the use of certification?
   A: It identifies Trusted Networks on the Public Internet. It is a quality label that ensures the self regulated quality standard of the network.

7. Q: What if a DDOS attack comes from within the trusted part of the Internet?
   A: Statistically a DDoS attack by its nature is a spread attack (a bell curve normal distribution) from a non discriminatory set of sources. By closing off a large part of the internet the attack will be decimated and better mitigated. Furthermore Trusted Networks are better secured as attribution analyses could be done easier (anti-spoofing) and faster (24/7, CERT of IRT or equivalent team by the Trusted Networks.)

8. Q: Does the Trusted Networks Initiative only provide a solution for DDOS attacks or as well for other risks?
   A: The Trusted Networks Initiative provides as well a solution for other vulnerabilities, such as hacking assaults. Partners of the Trusted Networks Initiative can offer risk mitigation controls, which help partners to avoid service disruptions and down time.

9. Q: Who can participate?
   A: Organisation can apply for qualification as Trusted Network when they are compliant to the protocol (e.g. own AS number, own IP address block of a minimum of 256 IP addresses, BGP, possibility to connect to a neutral datacentre for its services).

10. Q: What is the role of the Hague Security Delta?
    A: The Hague Security Delta (www.thehaguesecuritydelta.com) has a neutral position (Triple Helix Cluster on security, biggest in Europe) and acts as a facilitator (neutral broker) and expertise centre.

11. Q: Will this Trusted routing be a separate Internet for emergencies?
    A: No, the solution is developed to be able to use the normal internet and existing exchanges and peering technology, but Trusted Networks are trusted by their peers because they are compliant to the protocol.

12. Q: Could Trusted Network solutions be combined with other technologies?
    A: The Trusted Networks Initiative is open to good solutions and ideas. Thoughts on combining activities are discussed.

13. Q: How are the criteria of the protocol determined?
    A: Members of the Trusted Networks Initiative collaboratively decide on the necessary and useful requirements that should be applied to the protocol.