Panel discussion Quality Peering against Large volume DDoS attacks

The continuous development of DDoS attacks and especially large volume DDoS is a growing concern for the use of Internet. In 2013 the Dutch government started experiencing the impact of large DDoS attacks for their public services (DigID and www.belastingdienst.nl). In order to mitigate these attacks the contracts for Internet connectivity were extended with Anti-DDoS measures like scrubbing centers. At the same time it was foreseen that this would be a finite solution e.g. looking at the cost of the measures and the cost of initiating volume attacks so other ideas were looked into.

In 2014, a project called *Trusted Network Initiative* (TNI), facilitated by The Hague Security Delta, was launched in the Netherlands. By the end of 2015, the *Dutch Continuity Board* (DCB) [2] was created for taking over the TNI project. The central idea of TNI/DCB is to provide an emergency solution for cases of very large and/or prolonged Distributed Denial of Service (DDoS) attacks. Therefore, if an emergency situation requires, the target organization would become temporarily accessed only via the 'trusted Internet' and *disconnect* from the global Internet. Note that this project was intended as a **temporary** last-resource solution.

In 2018, *Logius*, the digital government service of the Netherlands Ministry of the Interior and Kingdom Relations, deployed a prove-of-concept (PoC) infrastructure very similar to the TNI/DCB. The main difference is that the 'trusted infrastructure' (preferred called as 'quality Internet Service Providers (ISPs)'—*Kwaliteitsspeering*) is intended to be **permanent** for accessing critical services, such as Dutch governmental online services. Instead of disconnecting a target organization from the global Internet, Logius proposed a primary way for accessing governmental online services from 'quality ISPs' in contrast to transit from 'general ISPs'. Logius' resilient infrastructure concept is depicted in Figure 1.

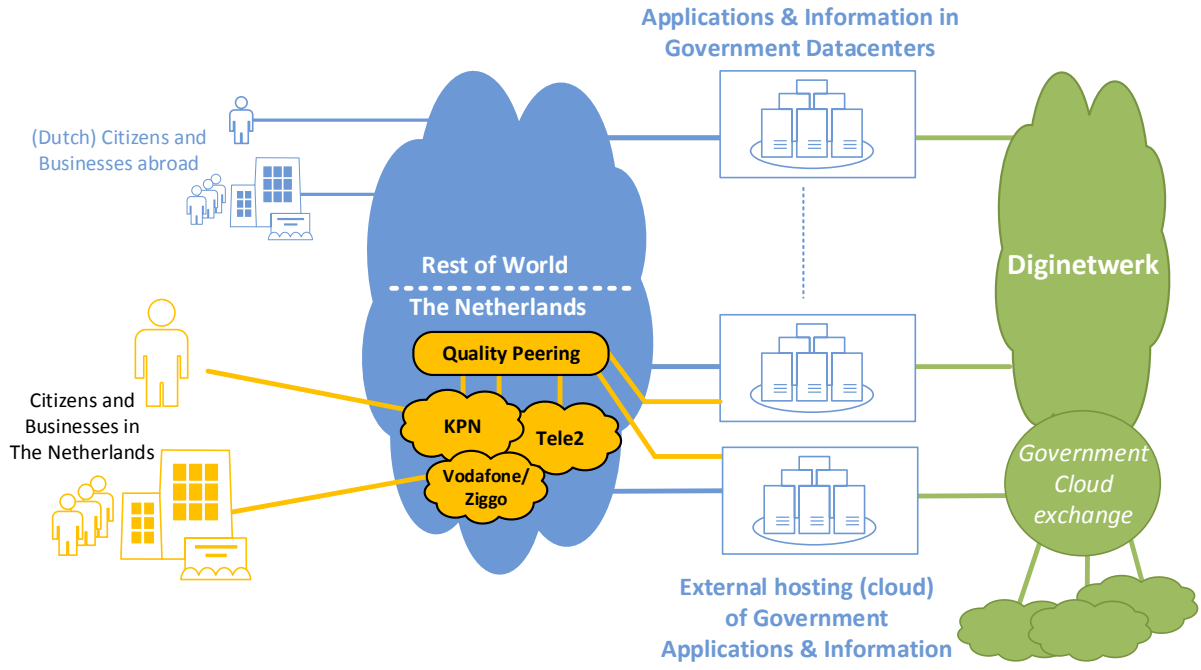

Figure 1

The concept is built on the idea that Quality ISP's are in control of their customer's traffic and as such are able to deliver that traffic "free of large DDoS" via a separate connection. In contrast, ISPs are generally not in control of other ISPs traffic. In addition to that, "legitimate" traffic to the

government is mainly from the Dutch ISPs, roughly >90%. (E.g. top 10 traffic sources of Digid are Dutch ISP's in total 90% of the traffic volume.)

With these in mind Logius and the Dutch Taxation Office tested the idea in a proof of concept together with the three largest Dutch Quality ISPs. The first results are positive and show that working with two traffic streams is feasible from a technical point of view.

Logius and the Dutch Taxation Office are looking into bringing the Quality Peering concept in production for her part of governmental services. At the same time advice and confirmation with the academic world is sought-after as is verification within the government and at ISPs level for feedback for a broad approach. The goal of the panel is to discuss the merits of this quality ISP concept.