SUBMISSION NO. 40

The Internet Corporation for Assigned Names and Numbers

10 July 2009

Mr Jerome Brown
A/g Committee Secretary
Parliament of Australia
House of Representatives
Standing Committee on Communications
PO Box 6021
Parliament House
Canberra ACT 2601

Dear Mr Brown

Response to Inquiry on Cyber Crime

Thank you for your letter of 25 May 2009 inviting ICANN to provide comments on the terms of reference developed to conduct an inquiry into cyber crime and its impact on Australian consumers. ICANN's ability to add value in understanding issues related to cyber crime and e-risks stem from its role as the global coordinator of the Internet's unique identifier systems, particularly the Domain Name System (DNS).

The terms of reference suggested for the inquiry should provide a good basis for conducting the inquiry. Outlined below are some observations, and concerns, you may find useful in the work of the Standing Committee.

In ICANN's view, the e-crime problem continues to worsen both in the prevalence of activity and, more importantly, the sophistication of those conducting the activity. We have observed a continual rise in the number of significant incidents, including abuse of the DNS through misdirecting traffic for high-profile users and in misleading users in the conduct of cyber fraud. We are particularly concerned about the continued evolution of botnets and the demonstrated capability of those creating these nets to make them larger (they now commonly exceed over 1 million computers); the sophisticated code that enables control and makes these networks hard to remove; and the capability of botnet operators to adapt quickly to defensive responses. We've also increasingly observed the use of the DNS as an aspect of how botnets operate within the Internet ecosystem – as a means of pointing attacks at targets; as a mechanism for malware to receive commands and updates; and the DNS itself as a target of such attacks. Botnets are a core enabler of the widespread phishing and malware propagation that underpins cyber fraud as a major and growing threat to almost all financial activity conducted on the Internet. These botnets can also be used as instruments of disruptive attacks, as they were in the events in Estonia in the spring of 2007, to create a wide range of e-security risks including disruption of critical infrastructure, interference with governmental ability to communicate with the public, and making governmental e-services inaccessible to the public.

ICANN's observation is that Australian communities' awareness and understanding of these e-security risks is relatively high in comparison to others in the global Internet community that ICANN works with. We are best equipped to comment on the utility of initiatives to combat e-security risks as they relate to collaborative efforts that tend to be cross-portfolio and inter-jurisdictional within national governments and require the global collaboration of stakeholders. Addressing cyber threats that involve the use of large networks of compromised computers distributed across the globe necessarily involves collaboration across a wide stakeholder base - security

researchers, IT and anti-virus vendors, network operators and the DNS community, law enforcement and other government agencies. ICANN has recently participated in large-scale collaboration across these communities in efforts to stop the spread and use of the Conficker botnet. These efforts have been effective in leveraging a wide range of private sector security expertise and allowing operators in the DNS community to take action while also engaging governmental entities to improve their understanding of how Conficker was behaving and the private sector was responding. We would encourage the Australian government to look at this response as a model and proactively engage its international partners in fostering such effective public – private collaboration in sustained engagement against these threats.

As the Committee moves forward with its work, ICANN would welcome continued opportunity to engage with its views and as useful, participate in initiatives in combating botnets and other e-security threats to the degree that they fall within our remit.

Yours sincerely

Paul Twomey
Senior President
ICANN