Australian Government

Australian Security
Intelligence Organisation

Director-General of Security

26 June 2009

eA: 1132889

The Hon Ms Belinda Neal, MP
Standing Committee on Communications
Suite R1-109
Parliament House
CANBERRA ACT

Dear Ms Neal,

INQUIRY INTO CYBER CRIME

I refer to the letter of Mr Jerome Brown of 28 May 2009 inviting ASIO to provide a submission to the Standing Committee on Communications inquiry into Cyber Crime. Noting the public nature of this inquiry, and its focus on the criminal environment, my comments below are necessarily of a general nature, though I trust they will help your Committee's deliberations.

ASIO's functions and responsibilities are detailed in the *Australian Security Intelligence Organisation Act 1979*. Broadly, ASIO obtains, correlates and evaluates intelligence relevant to security and provides advice as appropriate. 'Security' in this context is defined as:

> *The protection of, and of the people of, the Commonwealth and the several States and Territories from:*
>
> - *Espionage;*
> - *Sabotage;*
> - *Politically motivated violence;*
> - *Promotion of communal violence;*
> - *Attacks on Australia's defence system; or*
> - *Acts of foreign interference;*
>
> *whether directed from, or committed within, Australia or not;*
>
> *and*
>
> - *the carrying out of Australia's responsibilities to any foreign country in relation to a matter mentioned in any of the above.*

Australian Government

Australian Security
Intelligence Organisation

Director-General of Security

ASIO discharges its responsibilities in relation to the cyber environment in a number of ways, including through:

- Investigation and analysis of cyber attacks where they are conducted by nation-State actors for the purpose of espionage or foreign interference, or directed at Australian interests or at other countries using Australian infrastructure by terrorist or other groups; and

- Production of threat assessments and protective security advice — in particular for governments and critical infrastructure sectors which may be subject to cyber attack.

I should add however that, even if not relevant to 'security', the ASIO Act permits ASIO to pass information to law enforcement authorities where that information relates to indictable offences. Some cyber crime activities which come to ASIO's attention may fall within this category.

I have attached ASIO's responses to the Committee's specific questions on cyber crime. Thank you for the opportunity to comment on this increasingly complex and challenging issue.

yours,

David Irvine

STANDING COMMITTEE ON COMMUNICATIONS
INQUIRY INTO CYBER CRIME

ASIO RESPONSES TO INQUIRY QUESTIONS

a) Nature and prevalence of e-security risks including financial fraud and theft of personal information, including the impact of malicious software such as viruses and Trojans;

The threat of electronic attack on any computer/IT system connected to the Internet is high — that is to say, it is to be expected. Cyber threats are becoming more wide ranging, increasingly sophisticated (not only involving Trojans and malicious code, but also using social engineering techniques) and increasing in intensity. The perpetrators of such attacks can range from the ubiquitous hacker through to criminals, issue-motivated groups, terrorist organisations and nation states. Due to the nature of the Internet and obfuscation techniques employed by these perpetrators, the actual identification of the source of malicious cyber activity can often be difficult to determine.

The motivation underlying such activity includes personal satisfaction, information theft for personal, criminal, strategic, political or economic advantage or intent to damage IT systems or infrastructure.

Terrorists use the Internet for a variety of purposes — including communications, propaganda, recruitment and reconnaissance of targets. It is also feasible that terrorists or extremists may engage in malicious cyber activity that would exploit Australia's reliance on Information Communications Technology to significantly disrupt services, cause casualties and/or inflict economic harm.

Issue motivated groups may use denial of service and website defacement tactics to draw attention to their particular causes or, potentially more concerning, to disrupt or sabotage the operations of entities at the focus of their concerns.

And at the most sophisticated end of the spectrum, nation states may use cyber attack capabilities for espionage, foreign interference or sabotage in times of war.

A most concerning feature of the interconnected cyber environment is that today's technology enables the rapid and anonymous exfiltration of vast amounts of data from systems – either remotely or via direct human intervention. Such capability was not possible a few years ago. And even if potential aggressors do not possess sophisticated cyber capabilities themselves, groups or individuals are constantly developing techniques or expertise which can be readily transferred (purchased) by those who wish to use them.

b) The implications of these risks on the wider economy, including the growing economic and security impacts of botnets;

Your attention is drawn to the 2009 U.S. Cyberspace Policy Review, stating that *"the growing sophistication and breadth of criminal activity along with harm already caused by cyber incidents, highlight the potential for malicious activity in cyberspace to affect U.S. competitiveness, degrade privacy and civil liberties protections, undermine national security, or cause a general erosion of trust, or even cripple society."* Examples of cyber attack include a CIA report of the disruption of electric power capabilities overseas resulting in a multi-city power outage; fraudulent transactions of over 130 ATM teller machines in 49 cities over a 30 minute period and the loss of intellectual property to data theft (in 2008) estimated to be valued as high as $1 trillion.

We have no doubt that the same sort of potential to cause harm exists in Australia, though others are better placed to judge the implications to our economy.

As mentioned above, the interconnectedness of systems (and thereby the utility of botnets) and their exfiltration capacities magnifies the harm impacts.

c) Level of understanding and awareness of e-security risks within the Australian community;

The promotion of a suitable culture of cyber awareness amongst all levels of society — government(s), the private sector and individuals — coupled with appropriate physical, personnel and procedural arrangements in conjunction with technical security measures, is necessary to guard against nefarious activities perpetrated via cyber means. This type of activity will be increasingly important as Australia develops a comprehensive, common 'cyber backbone' through the National Broadband Network.

Technical measures in isolation will not provide an adequate degree of security. Despite general understanding of risks among many sectors of the population, the constant administrative and time overheads incurred in guarding against threats often militate against the conduct of technical security best practice. A better informed and strengthened security culture is also needed.

d) Measures currently deployed to mitigate e-security risk faced by Australian consumers:

a. Education initiatives
b. Legislative and regulatory initiatives
c. Cross-portfolio and inter-jurisdictional coordination
d. International cooperation.

ASIO is a partner in the Joint Operating Arrangements (JOA) that were established during 2000 by the Secretaries Committee on National Security. Comprising the Defence Signals Directorate, the Australian Federal Police High Tech Crime Operations and ASIO, the JOA assesses, coordinates and responds to incidents of a critical nature affecting Australia's National Information Infrastructure.

ASIO is also a close partner with the Attorney-General's Department, providing input into policy matters through the inter-departmental E-Security Policy and Coordination Committee, and through its engagement with GOVCERT. GOVCERT acts as an initial point of government interface with the private sector on cyber-security and threat mitigation matters. ASIO also often incorporates advice in relation to cyber security in own engagement with the private sector, including through the Business Liaison Unit.

Cyber-security is also a subject of ongoing dialogue between ASIO and its international counterparts.

e) Future initiatives that will further mitigate the risks to Australian Internet users:

Noting the comments above, ASIO is strongly supportive of measures designed to ensure Australia has the capability and capacity to detect, and analyse cyber-threats — to determine their true source(s), intent and harm, and to swiftly respond with appropriate mitigation action.

The Cyber Security Operations Centre – an outcome of the Defence White Paper — is seen as an important capability in this respect. ASIO will have close ties to this Centre.

f) Emerging technologies to combat these risks.
ASIO has no public comment to make on this issue.