

	<p>For each paper you wish to comment on (Please repeat as many times as required) Name of the paper:</p> <p>Australia's Comment on Cybersecurity and Cybercrime</p>
	<p>Has the issue as it applies to the question of Internet Governance been adequately identified?</p>
	<p>Comments:</p> <p>In identifying the issue the paper cites various references, some of which are somewhat dated. The use of more relevant, current materials would be preferable.</p> <p>We would also note that a number of online security threats are now emerging that have the potential to seriously undermine public and business trust and confidence in the online environment. This paper would benefit from an added reflection on established and emerging trends such as spam as a vehicle for viruses, worms, Trojans and phishing attacks and the rise of spyware and zombie "botnets". Related issues include fraud, identity theft and the increasing use of cybercrime, by organised, well-funded crime syndicates.</p> <p>Australia believes it would be appropriate for a paper on cybersecurity and cybercrime to refer to recent trends in criminal activity as part of its background context.</p>
	<p>Does the paper cover the topic with sufficient depth and accuracy?</p>
	<p>Comments:</p> <p>Depth and accuracy of the discussion in this paper is affected by the range of measures offered as potential solutions. To this extent the paper would be improved through the acknowledgement of "free" security products. A wide range of freeware and shareware products are now available to combat spam, spyware and viruses – empowering users (consumers, business and administration) to protect themselves at little or no cost.</p> <p>We feel that the paper might be improved by a broader approach to the discussion of tools in the fight against cybercrime.</p>
	<p>Does the paper achieve a reasonable balance in weighing relevant matters?</p>
	<p>Comments:</p> <p>We agree with the paper that education and awareness of users is a key tool in the fight against cybercrime. However, we would note (as the paper also notes) that cybercrime is a rapidly evolving issue – with education campaigns tending to lag behind these rapid developments. In this context the paper could make a clearer statement about the need for a balanced approach to combating cybercrime – incorporating developments in technology and standards, regulation and legislation, alongside those of awareness-raising.</p>

We also feel that a more appropriate balance might be achieved between discussion on the relevance of multilateral compared with domestic initiatives and developments in developing countries. Australia agrees with the paper's recognition that the engagement of developing countries in multilateral policy development, regulatory and enforcement fora is critical in combating cybercrime. However, we feel that of equal importance to meaningful cooperation at an international level, is the need for developing countries to establish national protective measures. This would include national policy frameworks and infrastructure as well as technical cybersecurity capabilities.

Any other comments:

Australia supports the paper's emphasis on the wide range and variety of fora currently addressing different cybersecurity issues. However we feel that this actually represents an appropriate devolvement and distribution of responsibility, rather than a "fragmentation". Given the rapidly evolving nature of cybercrime, a single entity responsible for technical standards, decision making, law enforcement and policy development for all aspects of the fight against cybercrime would not be able to move rapidly enough to provide meaningful protection for internet users. Australia believes that a more appropriate goal would be the encouragement of ongoing collaboration and communication between various fora.

Examples of international collaborative efforts in operational arrangements already exist. Worldwide, there are more than 250 "CERTs" – Computer Emergency Response Teams. Although based at both national and sectoral and private and public levels, these CERTs form an existing worldwide operational network of computer security experts, targeting computer incident prevention, response and mitigation strategies. In addition to informal arrangements, a Forum for Incident Response and Security Teams (FIRST) was established in 1990 – and now has over 170 members interoperating on a global scale. APEC is also undertaking work to provide training and encouragement for the establishment of CERTs in developing economies.

Similarly, law enforcement agencies have established a number of international initiatives targeting aspects of cybercrime. An example is the Virtual Global Taskforce on Child pornography and online child abuse, established in 2003. The taskforce comprises law enforcement representatives from Australia, England and Wales, Canada, the United States and Interpol.

The paper would benefit from the inclusion of these initiatives as examples of effective collaboration and co-operation.