

Cyberattack conclusions

The availability of cyber attack technologies for national purposes greatly expands the range of options available to U.S. policy makers as well as to policy makers of other nations.

Although the actual cyberattacks capabilities of the U.S. are highly classified, they are at least as powerful as those demonstrated by the most sophisticated cyberattacks perpetrated by cybercriminals.

The U.S. Government should conduct a broad, unclassified national debate and discussion about cyberattack policy.

Secrecy has impeded widespread understanding and debate about the nature and implications of U.S. cyberattack.

The failure to engage non-governmental analysis increases the likelihood that the full array of national and international intellectual capital will not be brought to bear on the issue, thereby depriving policy makers of its potential contribution to understanding the issue.

From the report - Technology, Policy, Law and Ethics regarding U.S. acquisition and use of cyberattack capabilities (2009), National Research Council, National Academies, Washington.

Chair: Admiral (ret.) William A. Owens, former Vice Chairman of the Joint Chiefs of Staff, and former CEO of Nortel.

Call for presentations

Cyber Warfare and Nation States: Recent developments in offensive and defensive capabilities to advance national interests

A conference at Safeguarding Australia 2010, Canberra
23 September 2010

Cyber capabilities to support national objectives are no different from other land, air, sea and space capabilities. They are a tool which can expand the range of options available to governments. However unlike other capabilities, the policy and legal framework controlling their development and use is in its infancy. The debate on these capabilities is currently conducted behind closed doors which impedes the understanding of their implications, and does not provide the rigour required to develop robust policy, guidance and doctrine.

Historically, academics, researchers and others in the non-government sector have led the development of strategy and doctrine for nuclear, chemical and biological weapons. This discussion was carried out in the open. Unclassified discussion built consensus on the strategic use of these technologies, as well as leading to international approaches to counter their proliferation.

Given the recent opening of Cyber Security Operations Centre (CSOC) within the Defence Signals Directorate which “provides Defence with a cyber warfare capability”¹ and that the Defence White Paper states that “the ADF of 2030 will need to be a more potent force in ... cyber warfare”,² it is timely to consider the policy framework in which cyber warfare capabilities function.

This conference will start this discussion and focus on questions including:

- What are the foreign perspectives on the use of cyber offensive capabilities?
- How can cyber capabilities (defensive and offensive) be used as an instrument of national policy?
- What would cyberconflicts look like?
- What are the lessons to be learned in developing cyber security strategy from the nuclear, chemical and biological weapon experience?
- How does the Law of Armed Conflict and International Law apply to cyberattacks?
- What could be the rules of engagement for cyber attacks?
- How do cyber capabilities be used in a graduated fashion?

¹ Department of Defence, 2009, *Cyber Security Operations Centre*, p. 4.

² Department of Defence, 2009, *Defence White paper 2009*, p. 13.

- How could cyber capabilities be used to support national missions, including intelligence?
- What are the escalation dynamics of cyberconflicts?

The conference will not examine cyber security issues such as online security, fraud and typical law enforcement activities associated with computer use.

The conference will consist of plenary sessions and discussions. A restricted workshop will be held on the afternoon of 22 September 2010.

The location is Rydges Lakeside, Canberra. More information on Safeguarding Australia is available at <http://www.safeguardingaustraliasummit.org.au/?getp=344>

Speakers are required to register for the conference but are entitled to the recovery rate for the conference (ie. AUD\$300).

People interested in presenting at the conference are requested to send a 50 word summary of their topic to Trudy Southgate at admin@securityresearch.org.au or call 02 6161 5143 or Int+612 6161 5143.

Conference Secretariat

Australian Security Research Centre
Int tel+612 6161 5143, Fax +612 6161 5144
PO Box 295, Curtin ACT 2605, Australia
International Affairs House, 32 Thesiger Cct, Deakin ACT 2600, Australia
admin@securityresearch.org.au