

Existing and Potential Threats in the Sphere of Information Security

November 2009

Cyber conflict is a new and complicated strategic problem that will engage the international community at many different levels. The cyber environment challenges traditional strategic thinking, and work on an adequate lexicon and policy framework to assess and manage cyber conflict is at an early stage. Many traditional security concepts will need to be adjusted for the cyber environment through review and discussion at the national, regional and international levels.

This bibliography provides an overview of publicly available documents on cybersecurity to assist that discussion. The first section contains reports from researchers in several different nations on the nature of cyber conflict, the risks to critical infrastructure, and possible ways to mitigate these risks. The second section provides source documents from multilateral organizations on cooperative regional or global approaches to cybersecurity. The final section provides, to the extent available, descriptions of national policies on cybersecurity. This first iteration of a cybersecurity bibliography provides a selection of thinking on this new and challenging problem and will be expanded as the international discussion develops.

Research reports

Abele-Wigert, Isabelle and Myriam Dunn, 2006, "An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies", in *International CIIP Handbook 2006*, vol. 1, Center for Security Studies, ETH Zurich.
www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16651

Bosch, Olivia, 2004, "Defending Against Cyber Terrorism: Preserving the Legitimate Economy", in Alyson J.K. Bailes and Isabel Frommelt (eds.), *Business and Security: Public-Private Sector Relationships in a New Security Environment*, SIPRI and Oxford University Press, pp. 187-96.
<http://books.sipri.org/files/books/SIPRI04BaiFro/SIPRI04BaiFro16.pdf>

Center for Strategic and International Studies, 2008, *Securing Cyberspace for the 44th Presidency*, A Report of the CSIS Commission on Cybersecurity for the 44th Presidency.
http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf

Cornish, Paul, 2009, *Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks*, European Parliament, Report to the Directorate-General for External Policies of the Union.
www.chathamhouse.org.uk/files/13346_0209_eu_cybersecurity.pdf

Dudgeon, Ian, 2008, "Targeting Information Infrastructures", in Gary Waters (ed.), *Australia and Cyber-warfare*, Australian National University, Chapter 4, pp. 59-84.
http://epress.anu.edu.au/sdsc/cyber_warfare/pdf/whole_book.pdf

International Institute for Strategic Studies and the Young Professionals in Foreign Policy, 2007, "NATO — Cyber-Crime and Cyber-Security", Panel Report.
www.iiss.org/EasysiteWeb/getresource.axd?AssetID=2695

Internet Corporation for Assigning Names and Numbers, 2009, *Plan for Enhancing Internet Security, Stability, and Resiliency*.
<http://icann.org/en/topics/ssr/ssr-draft-plan-16may09-en.pdf>

Lewis, James A., 2003, *Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats*, Center for Strategic and International Studies, Washington, DC.
http://csis.org/files/media/csis/pubs/021101_risks_of_cyberterror.pdf

Qiao Liang and Wang Xiangsui, 1999, *Unrestricted Warfare*, Beijing, PLA Literature and Arts Publishing House.
<http://cryptome.org/cuw.htm>

Multilateral Organizations

ASEAN Regional Forum, *Co-Chairs' Summary of the ARF Seminar on Cyber Terrorism (2004)*
[www.aseansec.org/arf/12arf/Co-Chairs' Report, Seminar on Cyber Terrorism, Jeju Island, 13-15Oct04.pdf](http://www.aseansec.org/arf/12arf/Co-Chairs%20Report,%20Seminar%20on%20Cyber%20Terrorism,%20Jeju%20Island,%2013-15Oct04.pdf)

Asia-Pacific Economic Cooperation, *APEC Strategy to Ensure Trusted, Secure and Sustainable Online Environment (2005)*
www.apec.org/etc/medialib/apec_media_library/downloads/workinggroups/telwg/pubs/2005.Par.0003.File.v1.1

European Commission, *Protecting Europe from Large Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security and Resilience (2009)*
<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2009:0149:FIN:EN:PDF>

Council of Europe, *Convention on Cybercrime (2001)*
<http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm>

European Network and Information Security Agency (ENISA), *Security Issues and Recommendations for Online Social Networks (2007)*
www.enisa.europa.eu/act/it/library/pp/soc-net/at_download/fullReport

International Telecommunication Union, *ITU Global Cybersecurity Agenda: High-Level Experts Group Global Strategic Report (2008)*
www.cybersecurity-gateway.org/pdf/global_strategic_report.pdf

International Telecommunication Union, *ITU Study on the Financial Aspects of Network Security: Malware and Spam (2008)*
www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf

North Atlantic Treaty Organization, *NATO Parliamentary Assembly, NATO and Cyber Defence (2009)*
www.nato-pa.int/default.Asp?SHORTCUT=1782

Organisation for Economic Co-operation and Development, Directorate for Science, Technology, and Industry, *Economics of Malware: Security Decisions, Incentives and Externalities (2008)*
www.oecd.org/dataoecd/53/17/40722462.pdf

Organization for Security and Co-operation in Europe, *Governing the Internet: Freedom and Regulation in the OSCE Region (2007)*
www.osce.org/publications/rfm/2007/07/25667_918_en.pdf

National Reports and Policies¹

The reports and policies of the seven nations below were selected because they are publicly available.

Estonia, Ministry of Defense, *Cyber Security Strategy* (2008)

www.mod.gov.ee/static/sisu/files/Estonian_Cyber_Security_Strategy.pdf

France, *White Paper on Defence and National Security* (2008)²

www.livreblancdefenseetsecurite.gouv.fr/IMG/pdf/white_paper_press_kit.pdf

Germany, Federal Office for Information Security, *The IT Security Situation in Germany in 2009* (2009)

www.bsi.bund.de/cae/servlet/contentblob/517474/publicationFile/28002/bsi_lagebericht09_pdf.pdf

Japan, National Information Security Policy Council, *The Second National Strategy on Information Security: Aiming for Strong “Individual” and “Society” in IT Age* (2009)

www.nisc.go.jp/eng/pdf/national_strategy_002_eng.pdf

Japan, Kei Harada, IT Security Center, Information-Technology Promotion Agency, *Japanese Information Security Status: Environment and Policies* (no date)

www.ipa.go.jp/security/fy14/evaluation/tog/paper-tog0302e.pdf

Russian Federation, *Information Security Doctrine of the Russian Federation: Approved by President Vladimir Putin on September 9, 2000* (2000)

www.mid.ru/ns-osndoc.nsf/1e5fode28fe77fdcc32575d900298676/2deaagee15ddd24bc32575d9002c442b?OpenDocument

United Kingdom, *Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space* (2009)

www.cabinetoffice.gov.uk/media/216620/css0906.pdf

United States, *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009)

http://cio.energy.gov/documents/Cyberspace_Policy_Review_final.pdf

Recent United Nations Resolutions

General Assembly, *Developments in the field of information and telecommunications in the context of international security*, A/RES/63/37 of 9 January 2009.

www.un.org/Docs/journal/asp/ws.asp?m=A/RES/63/37

General Assembly, Report of the Secretary-General, *Developments in the field of information and telecommunications in the Context of international security*, A/64/129 of 8 July 2009.

www.un.org/Docs/journal/asp/ws.asp?m=A/64/129

General Assembly, Report of the Secretary-General, *Developments in the field of information and telecommunications in the Context of international security* (Addendum), A/64/129/Add.1 of 9 September 2009.

www.un.org/Docs/journal/asp/ws.asp?m=A/64/129/Add.1

¹ UNIDIR welcomes further additions of national policies to be included in future updates. Contact kvignard@unog.ch

² This document is on national security and defence, but with a significant focus on cybersecurity that helped to guide national policy.