Selected Bibliography for Cyber Security

Last updated September 9, 2011.

This list is a work in progress that we update regularly as new reports are found and/or published. If you have suggestions for additions, send them to techpolicy@csis.org.

Nongovernmental Organizations

Addressing Cyber Security Through Public-Private Partnership: An Analysis of Existing Models
Intelligence and National Security Alliance, 2009

Applicability of the Additional Protocols to Computer Network Attacks
Knut Dormann
International Committee of the Red Cross (ICRC), 2004

Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats
James A. Lewis
CSIS, 2003

Beyond Attribution: A Vocabulary for National Responsibility for Cyber Attacks
Jason Healey
Cyber Conflict Studies Association, 2010

In the Crossfire: Critical Infrastructure in the Age of Cyber War
McAfee and CSIS, 2010

Cyberdeterrence and Cyberwar
Martin C. Libicki
RAND, October 2009

Thresholds for Cyberwar
James A. Lewis
CSIS, October 2010

Cyberpower and National Security
Franklin D. Kramer, Stuart H. Starr, Larry Wentz (eds.)
National Defense University, 2009

Cyber Security and Politically, Socially and Religiously Motivated Cyber Attacks
Paul Cornish
Chatham House, 2009

Cybersecurity and National Policy
Dan Geer

Harvard National Security Journal, 2010

Cyber Security and the Intelligence Community
Eric Rosenbach and Aki J. Peritz
Belfer Center for Science and International Affairs, 2009

Cyber War: The Next Threat to National Security and What to Do About It
Richard A. Clarke and Robert Knake
New York: HarperCollins, 2010

Defending a New Domain
William J. Lynn III
Foreign Affairs, Sept / Oct 2010

Defending Against Cyber Terrorism: Preserving the Legitimate Economy
Olivia Bosch, 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, 2004. 187-196.

Freedom on the Net: A Global Assessment of Internet and Digital Media
Freedom House, 2009

The Future of the Constitution: The Cyberthreat, Government Network Operations, and the Fourth Amendment
Jack Goldsmith
The Brookings Institution, 2010

Google Confronts China's "Three Warfares"
Timothy Thomas
Parameters, Summer 2010. 101-113.

A Human Capital Crisis in Cybersecurity
Karen Evans and Franklin Reeder
CSIS Commission on Cybersecurity for the 44th Presidency, November 2010

International Cyber Incidents: Legal Considerations
Eneken Tikk, Kadri Kaska, Liis Vihul
NATO Cooperative Cyber Defence Centre of Excellence, 2010

Internet Governance in an Age of Cyber Insecurity
Robert K. Knake
Council on Foreign Relations, 2010

An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies
Isabelle Abele-Wigert and Myriam Dunn

International CIIP Handbook 2006, Vol. 1, Center for Security Studies, ETH Zurich

The "Korean" Cyber Attacks and Their Implications for Cyber Conflict
James A. Lewis
CSIS, October 2009

Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008
U.S. Cyber Consequences Unit, 2009

Plan for Enhancing Internet Security, Stability, and Resiliency
Internet Corporation for Assigned Names and Numbers (ICANN), 2009

Project Grey Goose
Phase 1: Russia/Georgia Cyber War – Findings and Analysis
Phase II: The Evolving State of Cyber Warfare
Greylogic, 2008-2009

Russia and the Cyber Threat
Kara Flook
Critical Threats, 13 May 2009

Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cybersecurity for the 44th Presidency
CSIS, 2008

Shadows in the Cloud: Investigating Cyber Espionage 2.0
Joint Report: Information Warfare Monitor and Shadowserver Foundation, 2010

Strategic Advantage: Why America Should Care About Cybersecurity
Melissa E. Hathaway
Belfer Center for Science and International Affairs, October 2009

Surviving Cyberwar
Richard Stiennon
Government Institutes, 2010

Targeting Information Infrastructures
Ian Dudgeon and Gary Waters (eds.)
Australia and cyber-warfare. Australian National University, 2008. 59-84.

Tracking Ghostnet: Investigating a *Cyber Espionage* Network
Ron Diebert and Rafal Rohozinski
Information Warfare Monitor, 2009

Unrestricted Warfare
Qiao Liang and Wang Xiangsui

PLA Literature and Arts Publishing House, 1999

Virtual Criminology Report 2009 – Virtually Here: The Age of Cyber Warfare
McAfee and Good Harbor Consulting, LLC, 2009

Government Publications and Policy Documents

An Assessment of International Legal Issues in Information Operations
Office of General Counsel, May 1999

Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress
Congressional Research Service, 2008

Capability of the People's Republic of China to Conduct Cyber Warfare and Computer Network Exploitation
U.S.-China Economic and Security Review Commission, 2009

Cornerstones of Information Warfare
US Air Force, 1997

Critical Foundations: Protecting America's Infrastructures
Report of the President's Commission on Critical Infrastructure Protection, 1997

Critical Infrastructure Protection: DHS Needs to Better Address Its Cybersecurity Responsibilities
Government Accountability Office, 2008

Critical Infrastructure Protection: Key Private and Public Cyber Expectations Need to Be Consistently Addressed
Government Accountability Office, July 2010

Critical Infrastructure Protection: Update to National Infrastructure Protection Plan Includes Increased Emphasis on Risk Management and Resilience
Government Accountability Office, July 2010

Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats
Government Accountability Office, 2007

Cybersecurity: Continued Attention is Needed to Protect Federal Information Systems from Evolving Threats
Government Accountability Office, 2010

Cybersecurity: Progress Made but Challenges Remain in Defining and Coordinating the Comprehensive National Initiative
Government Accountability Office, 2010

Cyber Security Strategy
Cyber Security Strategy Committee
Estonian Ministry of Defense, 2008

Cyber Security Strategy for Germany
German Federal Ministry of the Interior, 2011

Cyber Security Strategy of the United Kingdom: Safety, Security and Resilience in Cyber Space
UK Office of Cyber Security, 2009

Cyberspace: United States Faces Challenges in Addressing Global Cybersecurity and Governance
Government Accountability Office, 2010

Cyberspace Policy: Executive Branch is Making Progress Implementing 2009 Policy Review Recommendations, but Sustained Leadership is Needed
Government Accountability Office, 2010

Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure
The White House, 2009

Economics of Malware: Security Decisions, Incentives and Externalities
Directorate for Science, Technology, and Industry
Organisation for Economic Co-operation and Development (OECD), 2008

French Strategy for the Defense and Security of IT Systems (French)
French Republic, February 2011

Governing the Internet: Freedom and Regulation in the OSCE Region
Organization for Security and Co-operation in Europe (OSCE), 2007

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

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

The IT Security Situation in Germany in 2011
Federal Office for Information Security, 2011

ITU Global Cybersecurity Agenda: High-Level Experts Group Chairman's Report
International Telecommunication Union, 2008

ITU Study on the Financial Aspects of Network Security: Malware and Spam
ICT Applications and Cybersecurity Division, International Telecommunication Union, 2008

Japanese Information Security Status: Environment and Policies
IT Security Center
Information-technology Promotion Agency

National Cybersecurity Strategy
The Netherlands, 2011

National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture
Government Accountability Office, 2009

The National Military Strategy for Cyberspace Operations
The US Joint Chiefs of Staff, 2006

National Strategy for Trusted Identities in Cyberspace: Creating Options for Enhanced Online Security and Privacy (Draft)
The White House, 2010

NATO and Cyber Defence
NATO Parliamentary Assembly, North Atlantic Treaty Organization, 2009

Proceedings of a Workshop on Deterring Cyberattacks: Informing Strategies and Developing Options for U.S. Policy
Committee on Deterring Cyberattacks
National Research Council, 2010

Protecting Europe from Large-Scale Cyber-Attacks and Disruptions: Enhancing Preparedness, Security, and Resilience
European Commission, 2009

Reducing Systemic Cybersecurity Risk
OECD/IFP Project on "Future Global Price Shocks"
Organisation for Economic Co-operation and Development (OECD), 2011

The Second National Strategy on Information Security: Aiming for Strong "Individual" and "Society" in IT Age
National Information Security Policy Council, 2009

Security Issues and Recommendations for Online Social Networks
European Network and Information Security Agency (ENISA), 2007

Technology Policy Law and Ethics Regarding U.S. Acquisition and Use of Cyberattack Capabilities

Committee on Offensive Information Warfare
National Research Council, 2009