"Governance in the Information Age"
International Studies Association
Hong Kong, July 28, 2001

"Encryption Policy and the Role of the Internet Community: Regulation of a New Weapon in the United States and Japan"

Motohiro TSUCHIYA[1]
CIDCM, University of Maryland
GLOCOM, International University of Japan
taiyo@glocom.ac.jp

Summary

The purpose of this paper is to consider the role of the Internet Community in encryption policy. Digital encryption technology is regarded as a military weapon, which enables secret and secure transmission over networks including the Internet. Some governments are trying to regulate its use on the Internet, because there are concerns that the technology might empower terrorists or criminals. However, some people in the Internet Community, people who are interested in online issue, claims that the Internet should be free from any government regulation. This paper compares attempts of encryption regulation and reactions in the United States and Japan. This analysis implicates that the Internet governance may not be easily harmonized.

[1] Visiting Senior Research Fellow, Center for International Development and Conflict Management (CIDCM), University of Maryland, and Assistant Professor and Senior Research Fellow, Center for Global Communications (GLOCOM), International University of Japan. The author acknowledges detailed comments of Dr. Lance Hoffman, George Washington University.

1. Encryption Technology as a Weapon

In human history, military communities used encryption or cipher technologies. Ancient codes like the Caesar Cipher were used for secret communications between allies.

Now encryption technology is becoming a commodity in our Internet life. It is used for secure online communications and authentication between two parties. Secure electronic commerce is impossible without them. So encryption is not only for government or military communities, but also for other communities including the Internet Community.

In addition to secure communication, encryption technology is used for protecting privacy. Encrypted message enables people to communicate without interception of third parties.

However, some government and military communities cannot accept this change. They are afraid that terrorists or criminals might use this powerful technology for their activities without letting know anyone outside confederates.

Therefore, governments are trying to regulate public use of encryption technologies. The United States government tried to introduce a key escrow (or key recovery) system domestically, and still regulates exports of encryption software, though the system is much less restricted than it used to be.

These government regulations met strong opposition from many in the Internet Community. People in the community think that laws in many countries protect the privacy or confidentiality of correspondence and that it must be protected in the cyberspace too. They insist that all online communications should not be intercepted by anybody including governments.

2. Internet Community and Internet Governance

The word "the Internet Community" is frequently used, but no fixed definition. Edward J. Valauskas adopts a simple one saying that “a collection of individuals who use computers, software, and other means to discuss common interests transcendentally, outside of time and space[2].”

Until mid-1990s it meant an academic or computer engineer group who were developing the Internet (or earlier versions of it). At that time, "academic techies (people who are familiar with technologies)" owned the Internet. It was a small community and people knew each other. However, after the privatization of the Internet around 1995, many other groups joined the Internet Community, and it became bigger.

First, corporate techies joined it. They are also familiar with technologies, but are hired by commercial companies like Microsoft, Cisco, Netscape, AOL, Nortel and others. They are interested in developing the Internet and introducing new technologies, but their interests are often based on commercial benefits of their own companies. Their join to the Internet Community has changed a pure academic community into a more mixed community of academic and commercial interests.

Second, non-techie, ordinary Internet users joined it. The

[2] Edward J. Valauskas, "Lex Networkia: Understanding the Internet Community," first Monday <http://www.firstmonday.dk/issues/issue4/valauskas/>, published online in 1996 (Access: July 22, 2001).

number of Internet user is growing very rapidly, and it is said that it reached 500 million in the world in 2001. Not all, but a small portion of the whole Internet user is interested in governance of the Internet, but the small portion includes at least 30 thousand people, because 30 thousand people voted in the online election to select new directors of ICANN (Internet Corporation for Assigned Names and Numbers) in 2000.

Third, lawyers joined it, especially in the United States. As the Internet becomes more important in people's daily life, legal issues arise, and these issues are discussed and solved domestically and internationally by lawyers.

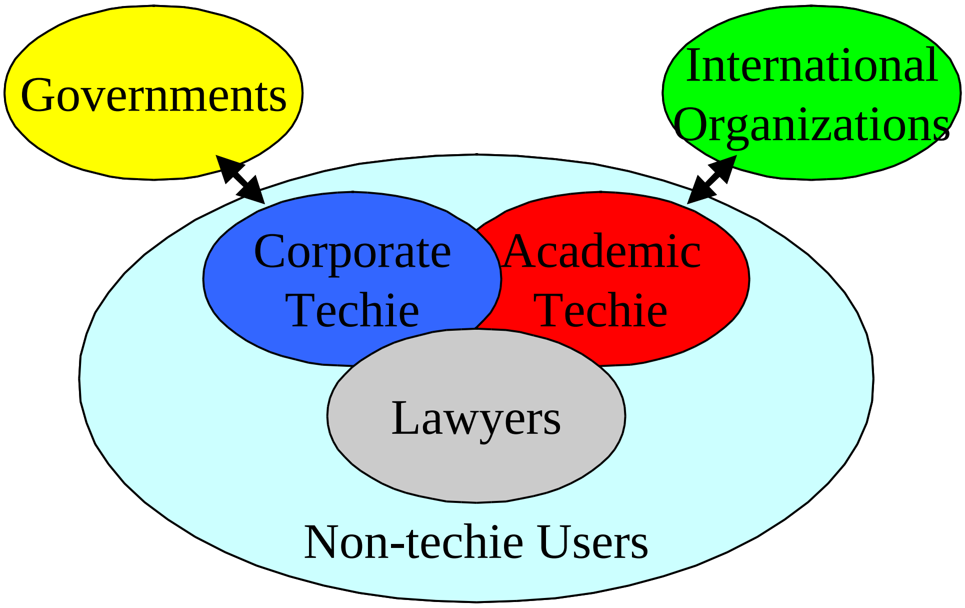
Therefore, the Internet Community is changing itself and contains various people. It is no longer a small group who knows each other, but a vast group of mixed interests.

Outside the community, governments are interested in the Internet too. Most governments did not realize the importance of the Internet at first. However, as some social problems like pornography or gambling rise, they started considering regulation of it. In addition, fruits of electronic commerce or so-called "new economy" attracted policy makers.

International organizations participated in the discussion later. The World Trade Organization (WTO), the Organization for Economic Cooperation and Development (OECD), the World Intellectual Property Organization (WIPO), the International Telecommunication Union (ITU) and others are interested in the Internet. In 2000 G8 (Group of Eight) adopted the Okinawa IT Charter to establish a taskforce called DOT Force (Digital Opportunity Task Force), and DOT Force made a report to G8 Genoa Summit in 2001.

As many actors are involved (see Chart 1), the "governance" of the Internet is being perceived as an important issue.

Chart 1: Internet Community, Governments, and International Organizations



"Governance" is frequently used and a common word in many disciplines. As a word of business administration, "corporate governance" means the structure of governing a company by stakeholders. In development theories, "good governance" means the wellness or healthiness of one country's political and economic status.

In international relations theories, James N. Rosenau defines it as "a system of rule that works only if it is accepted by the majority (or, at least, by the most powerful of those it affects), whereas governments can function even in the face of widespread opposition to their policies[3]."

Governance system is different from government system in some points (See Table 1). First, governance system usually allows anybody interested in an issue to join decision-making process, though government system sometimes requests qualification by any means like election. Second, because governance system allows many people's participation, it tends to take more time to reach an agreement than government system. Third, government system usually adopts voting at the final stage of decision, though governance adopts "rough consensus." It means "a large majority of those who care must agree[4]." And finally, in decision-making process of government system information sharing is sometimes limited, but in governance system information sharing is strongly recommended.

Table 1: Government and Governance

	Government System	Governance System
Participants	Representatives, Limited	Anybody, Open
Time for Decision	Less	More
Decision Means	Voting	Rough Consensus
Information Sharing	Sometimes Negative	Very Positive

Governance system is working in the decision-making process of the Internet. At the core of the Internet governance, there are technical standard-setting processes by some organizations or groups. These organizations include the Internet Society (ISOC), the Internet Engineering Task Force (IETF), the Internet

[3] James N. Rosenau, “Governance, Order, and Change in World Politics,” in James N. Rosenau, and Ernst-Otto Czempiel, eds., *Governance Without Government: Order and Change in World Politics* (New York: Cambridge University Press, 1992), p 4.
[4] Paul Hoffman, "A Novice's Guide to the IETF," <http://www.imc.org/novice-ietf.html> (Access: May 6, 2001).

Architecture Board (IAB), the World Wide Web Consortium (W3C), and the Internet Corporation for Assigned Names and Numbers (ICANN). Basically these groups are adopting governance system.

As Craig Simon argues, "the standards-making process for global telecommunications is moving out of the hands of traditional state authorities into the hands of people whose goals and loyalties are less national than commercial[5]." Political processes in Internet governance are becoming quite complicated, since the number and the type of actors are increasing.

In the following two sections, encryption regulations and reactions in the United States and Japan are analyzed.

3. Reaction to Government Regulation in the United States

3.1. U.S. Government Control

Governments were concerned with this new technology. The French government made a rule to regulate domestic use of the new encryption technology. The Wassenaar Arrangement agreed to make a common regulation not to handover the encryption technology to rogue countries.

The U.S. government was most concerned with wider spread of strong encryption technologies in the world. The Clinton administration considered two measures to regulate encryption use. One is domestic "key escrow" or "key recovery" system and the other is export control of stronger encryption products.

[5] Craig Simon, “Internet Governance Goes Global,” Vendulka Kubálková, Nicholas Onuf, and Paul Kowert, eds., International Relations in a Constructed World (New York: M. E. Sharpe, 1998), p. 147.

The key escrow or key recovery system was to make mandatory for communication equipment manufacturers to install into their devices a system enabling the government to decode encrypted communication with an appropriate judicial authorization. In essence, keys to decode communications would be kept in government’s hands.

The other export control was aimed to stop exporting equipment or software with "strong" encryption function of a certain level or higher. American intelligence agencies are eavesdropping communications all over the world for security reasons. If stronger encryption technology were available, the agencies might lose their capabilities. As Frances Cairncross says, "the U.S. government has fought a long battle to prevent the American public -- or, worse, foreign citizens -- from being able to use encryption technologies that U.S. government agencies could not easily decode[6]."

Therefore, according to Wayne Rash, "the Federal Bureau of Investigation and the National Security Agency [were] pressing the administration and Congress hard for laws that would require a form of encryption to which the government would hold the key, meaning that a law enforcement agency could read encrypted information[7]." Encryption was no more technology issue, but it became a political issue.

American government's approach can be said to be "forecasting" than "observing." The government thinks that they must be ready

[6] Frances Cairncross, *The Death of Distance: How the Communications Revolution Will Change Our Lives* (Boston, Massachusetts: Harvard Business School Press, 1997), p. 114.
[7] Wayne Rash, Jr., *Politics on the Nets: Wiring the Political Process* (New York: W.H. Freeman, 1997), p. 157.

for future problems, which encryption may bring, before they actually show up. No fact, but fear is important to make a new policy and a new regulation.

3.2. Organized Reaction

The government regulations drew much attention and roused public opinion against the policy. Especially the Internet Community reacted furiously. They argued that the key escrow is violating the right of privacy.

Private companies producing encryption equipments and software joined the side of the Internet Community. They insisted that export control would be meaningless unless other countries impose those limits. The U.S. computer industry argued, "it is losing millions of dollars in sales on the world market because of the export controls[8]."

Some online groups in the Internet Community activated online campaigns against government control. The American Civil Liberties Union (ACLU) has a web page called "Privacy and Encryption Page" <http://www.aclu.org/issues/cyber/priv/priv.html>. It advocates protection of online privacy.

The Center for Democracy and Technology (CDT) has a page for encryption <http://www.cdt.org/crypto/>, and it says, "Encryption systems, which scramble electronic communications and information, allow users to communicate on the Internet with confidence, knowing their security and privacy are protected. But

[8] See Graeme Browning, *Electronic Democracy: Using the Internet to Influence American Politics* (Wilton, CT: Pemberton Press, 1996), p. 75.

the US government blocks export of strong encryption, limiting its widespread use."

The Electronic Privacy Information Center (EPIC) published a book titled "Cryptography and Liberty 2000" and its online version is available <http://www2.epic.org/reports/crypto2000/>. It analyzes encryption policies of many countries, and EPIC is also opposing regulations.

These groups are lobbying in the Congress vigorously. They are following introduced bills, send e-mail to their supporters, provide information on the web, attend Congressional hearings and make statements, and so on. Their political power has much influence in real political arenas.

At last, Clinton administration relaxed its export control in 1998, and could not implement the key escrow system before inauguration of new Bush administration in 2001. The Internet Community in the U.S. played a critical role.

4. Reaction to Government Regulation in Japan

4.1. Negative Image of Encryption

People in Japan have had a negative image towards encryption since the end of the World War II. In the final stage of the WWII, American intelligence agencies broke almost all Japanese codes[9]. After the occupation by GHQ (General Headquarters of the Supreme Commander for the Allied Powers) following the end of the war, Japan joined the American alliance through the Japan – U.S. Security Treaty in 1951. Under the alliance, military and

[9] Michael Smith, *The Emperor's Codes: The Breaking of Japan's Secret Ciphers* (New York: Arcade Publishing, 2001).

security information was brought to Japan through the American government. Japan does not need to be keen on development of secure communications mechanisms.

Necessities for secure communications were reminded in the "economic war" between Japan and the U.S. on auto industry broke out in 1995. Internal conversations of the Japanese negotiators were eavesdropped by CIA (Central Information Agency) and NSA (National Security Agency)[10].

Meanwhile the penetration of the Internet started in 1995 in Japan. Expectations for the growth of the electronic commerce (EC) became wider, as the number of the Internet user increased. However, most people didn’t want to buy things online other than books, CDs, or other ones, which had been already popular in the United States.

People didn't believe that EC was secure enough, but only few realized existence of encryption technology functioning behind web browsers. Because of U.S. export control of stronger encryption software, Japanese people were not allowed to download Netscape Navigator with 128 K bit encryption. However, few users cared it and chose one with 64 K bit encryption, even though they could download the 128 K bit software technically. They did not care if it was safe, because they did not shop online.

4.2. Japanese Government Control

In the Japanese government, ICT (Information and Communication Technology) discussions started in 1995 when the Advanced Information and Telecommunications Society Promotion

[10] Sanger, David E., and Tim Weiner. "Emerging Role for the C.I.A.: Economic Spy." *New York Times*, 15 Oct. 1995.

Headquarters was established under Murayama administration. The Headquarters took leadership to coordinate ICT policies among ministries.

The Ministry of International Trade and Industry (MITI) administered control of Japanese encryption policy, and the Ministry of Economy, Trade and Industry (METI) succeeded MITI after the major government organizational reform on January 6, 2001.

The Policy of MITI and METI regarding encryption is to follow the Wassenaar Arrangement (Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies)[11]".

The arrangement was formed in September 1996 after the dissolution of COCOM (Coordinating Committee for Export to Communist Areas for Multilateral Export Controls) in 1994. COCOM's goal was to prevent exporting goods to communist countries under the Cold War. Wassenaar Arrangement's goal is to prevent exporting goods to "rogue countries." The definition of rogue countries is not fixed, but countries like Iran, Iraq, Libya, and North Korea might be included[12].

The arrangement has a list of items to be controlled. The items are divided into 9 categories: (1) Advanced Materials, (2) Materials Processing, (3) Electronics, (4) Computers, (5) Telecommunications (Part 1) and Information Security (Part 2), (6) Sensors & Lasers, (7) Navigation & Avionics, (8) Marine, and

[11] The Wassenaar Arrangement Homepage is <http://www.wassenaar.org/>.

[12] THE BUREAU OF PUBLIC AFFAIRS, "U.S. DEPARTMENT OF STATE DISPATCH," VOLUME 5, NUMBER 15, APRIL 11, 1994 <http://dosfan.lib.uic.edu/ERC/briefing/dispatch/1994/html/Dispatchv5no15.html> (Access: July 15, 2001).

(9) Propulsion. Encryption software is in Category 5 - Part 2: Information Security.

The regulation has conditions and exceptions in detail[13]. The Japanese government changes their laws and ordinances when the Wassenaar changes its list. For example, METI changed the Export Trade Control Order and the Ministerial Ordinance on Freights in June 2000 and in December 2000 according to Wassenaar's deregulation of computer, computer chip and computer programs related to encryption.

Japanese government's approach is more "observing[14]" than "forecasting." It is not trying to capture issues before a problem comes up. It is watching what other countries do, especially the U.S. This approach reduces time and labor to consider what has never happened. However, it is vulnerable to a sudden attack or accident.

4.3. Individual Reaction

Reaction from the nation is also different from American one. It is more "individual" than "organized."

Some academic researchers in universities are interested in the encryption issue. Shinji Yamane at Iwate Prefectural University defines himself as a "Crypto Anarchist." Crypto Anarchism is an assertion that everyone has a right to use strong encryption[15].

[13] See <http://www.wassenaar.org/list/> for the list.

[14] "Observing" is not always equal to "reactive." "Reactive" includes a sudden reaction without expectation.

[15] Shinji Yamane, "Who knows what a Crypto Anarchist is?" <http://www.vacia.is.tohoku.ac.jp/~s-yamane/articles/crypto/> (Japanese) (Access: July 15, 2001).

Toshimaru Ogura at Toyoma University says, "Encryption is the last resort for network users to protect their own privacy." He stresses that Cyberspace can never be a new and intimate community without encryption[16].

Hironobu Suzuki, independent software consultant and writer, criticizes that Japanese government's policy is just echoing American government's words[17].

These individual activities are not organized much. They are writing online and offline many articles about the issue, but they seem not to be attracting wider audiences.

There is only one organized group discussing the issue online. One example is JCA-NET. This group was organized at the time of Rio de Janeiro Environmental Summit in 1992. JCA-NET is influenced much by the Association for Progressive Communications (APC)[18].

JCA-NET opposes the government control of encryption technology because of privacy concerns. However, their major activity seems to be translating English materials on American cryptography issues into Japanese.

The organized level of activity by the Internet Community is lower in Japan. In other words, Japanese Internet Community has weaker

[16] Toshimaru Ogura, "What an idea!!! I can't accept any government and legal control of encryption," <http://www.jca.ax.apc.org/~toshi/Crypt/CryptIndex.html> (Japanese) (Access: July 15, 2001).
[17] Hironobu Suzuki, "Obsolete Key Escrow," <http://www.pp.iij4u.or.jp/~h2np/docs/KeyEscrow.html> (Japanese) (Access: July 15, 2001).
[18] APC homepage is <http://www.apc.org/>.

influence than American counterpart.

5. Is Internet Governance Robust?

Regulation of encryption is controversial in the United States already, and will be in Japan in the near future. However, some differences are found between two countries. The American government is forecasting what might happen, for example, terrorists or criminals use secure communication for dangerous plots. However, Japanese government's approach is observing what are happening in Japan and other countries.

Reactions to government actions are also different. In the United States some well-organized interest groups are influencing people's ways of thinking and policy processes on Capitol Hill. However, there are few organizations in Japan pursuing this issue, and individuals' voices are weaker.

Why are Japanese reactions not organized? Does it mean that Japanese information society is not mature? It rather means that the balance between privacy and social order is different. Most Japanese people do not think they need secret communication. They think that someone who needs secret communication has something evil in his or her mind. The incorrect view that only military people are using encryption is affecting their attitudes.

What does this difference in approach mean for the governance in the information age? First, Internet governance is not homogeneous geographically. It is said that globalization homogenizes world cultures. However, these cultures are affected by their histories and political systems.

Second, forecasting countries like the U.S. can be a showcase for other observing countries. The U.S. is leading the world in terms of technology and policy. Its political discussions, policies, and their results might help other countries make their own policies and get informed of recent tasks.

Third, even though observing countries are watching forecasting countries' policies, their policies cannot be always same. Observing countries might adopt a different type of policy. Therefore, the Internet governance will keep on seeing cultural and political diversities. When developing countries are increasingly involved in the Internet governance, it will not be easily harmonized.

Finally, the Internet Community does exist in theory, but it is a weak entity. The Internet Community is playing a significant role now, but it might have to consider changing itself. The future of the Internet governance will be dependent on that change.

6. Reference

Adams, James, *The Next World War: Computers Are the Weapons & the Front Line is Everywhere* (New York: Simon & Shuster, 1998).

Bamford, James, *Body of Secrets: Anatomy of the Ultra-Secret National Security Agency From the Cold War through the Dawn of a New Century* (New York: Doubleday, 2001).

Browning, Graeme, *Electronic Democracy: Using the Internet to Influence American Politics* (Wilton, CT: Pemberton Press, 1996).

Bull, Hedley, *The Anarchical Society: A Study of Order in World Politics, Second Edition* (New York: Columbia University Press, 1977).

Cairncross, Frances, *The Death of Distance: How the Communications Revolution Will Change Our Lives* (Boston, Massachusetts:

Harvard Business School Press, 1997).

Clark, Ronald W., *The Man Who Broke Purple: The Life of the World's Greatest Cryptologist Colonel William F. Friedman* (1977), translated into Japanese as *Ango no Tensai* (Tokyo: Sinchosha, 1981).

Commission on Global Governance, *Our Global Neighborhood: The Report of the Commission on Global Governance* (Oxford: Oxford University Press, 1995).

Comor, Edward A., ed., *The Global Political Economy of Communication: Hegemony, Telecommunication and the Information Economy* (New York: St. Martin's Press, 1994).

Denning, Dorothy E., *Information Warfare and Security* (Boston: Addison-Wesley, 1999).

Diffie, Whitfield, and Susan Landau, *Privacy on the Line: The Politics of Wiretapping and Encryption* (Cambridge, Massachusetts: The MIT Press, 1999).

Drake, William J., *The New Information Infrastructure: Strategies for U.S. Policy* (New York: The Twentieth Century Fund Press, 1995).

Dyson, Esther, *Release 2.1: A Design for Living in the Digital Age* (New York: Broadway Books, 1998).

Ebata, Kensuke, *Information Terrorism (Joho Tero)* (Tokyo: Nikkei BP, 1998, Japanese).

Everard, Jerry, *Virtual States: The Internet and the Boundaries of the Nation-State* (London and New York: Routledge, 2000).

Ford, Warwick, and Michael S. Baum, *Secure Electronic Commerce: Building the Infrastructure for Digital Signatures and Encryption* (Prentice Hall, 2000).

Garfinkel, Simson, *PGP: Pretty Good Privacy* (Cambridge, MA: O'Reilly & Associates, 1994).

Godwin, Mike, *Cyber Rights: Defending Free Speech in the Digital Age* (New York: Times Books, 1998).

Headrick, Daniel D., *The Invisible Weapon: Telecommunications and*

International Politics 1851-1945 (New York: Oxford University Press, 1991).

Hill, Kevin A., and John E. Hughes, Cyberpolitics: Citizen Activism in the Age of the Internet (Lanham: Rowman & Littlefield, 1998).

Hoffman, Lance J., ed. *Building In Big Brother: The Cryptographic Policy Debate* (New York: Springer-Verlag, 1995).

Kahin, Brian, and Charles Nesson, eds., *Borders in Cyberspace: Information Policy and the Global Information Infrastructure* (Cambridge, Massachusetts: The MIT Press, 1997).

Krasner, Stephen D., *International Regimes* (New York: Cornell University Press, 1983).

Kubálková, Vendulka, Nicholas Onuf, and Paul Kowert, eds., *International Relations in a Constructed World* (New York: M. E. Sharpe, 1998).

Lebow, Irwin, *Information Highways and Byways: From the Telegraph to the 21st Century* (New York: IEEE Press, 1995).

Lessig, Lawrence, *Code and Other Laws of Cyberspace* (New York: Basic Books, 1999).

Levy, Steven, *Crypto: How the Code Rebels Beat the Government-Saving Privacy in the Digital Age* (New York: Viking, 2001).

Liberty (The National Council for Civil Liberties), *Liberating Cyberspace: Civil Liberties, Human Rights and the Internet* (London: Pluto Press, 1999).

Loader, Brian D., ed., *The Governance of Cyberspace: Politics, Technology and Global Restructuring* (London: Routledge, 1997).

Marks, Leo, *Between Silk and Cyanide: A Codemaker's War 1941-1945* (New York: The Free Press, 1998).

Neuman, W. Russell, Lee McKnight, and Richard Jay Solomon, *The Gordian Knot: Political Gridlock on the Information Highway*

(Cambridge, Massachusetts: The MIT Press, 1998).

Rash, Wayne, Jr., *Politics on the Nets: Wiring the Political Process* (New York: W.H. Freeman, 1997).

Rikitake, Kenji, *Internet Community* (Tokyo: Ohmsha, 1994, Japanese).

Rosenau, James N., and Ernst-Otto Czempiel, eds., *Governance Without Government: Order and Change in World Politics* (New York: Cambridge University Press, 1992).

Rosenoer, Jonathan, *Cyber Law: The Law of the Internet* (New York: Springer, 1997).

Salus, Peter H., *Casting the Net: From ARPANET to INTERNET and beyond…* (Reading, Massachusetts: Addison-Wesley, 1995).

Schneier Bruce, and David Banisar, *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance* (New York: John Wiley & Sons, 1997).

Schneier, Bruce, Secrets & Lies: Digital Security in a Networled World (New York: John Wiley & Sons, 2000).

Shapiro, Andrew L., *The Control Revolution: How the Internet is Putting Individuals in Charge and Changing the World We Know* (New York: Public Affairs, 1999).

Singh, Simon, *The Code Book: The Evolution of Secrecy from Mary, Queen of Scots to Quantum Cryptography* (New York: Doubleday, 1999).

Smith, Michael, *The Emperor's Codes: The Breaking of Japan's Secret Ciphers* (New York: Arcade Publishing, 2001).

Standage, Tom, *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's On-line Pioneers* (New York: Walker and Company, 1998).

Tsuchiya, Motohiro, *Information and Global Governance: Nation States in Turbulent Internet World (Joho to Global Governance: Internet kara mita Kokka)* (Tokyo: Keio University Press, 2001, Japanese).

Tsujii, Shigeo, *Ango (Cryptography)* (Tokyo: Kodansha, 1996, Japanese).

Valauskas, Edward J., "Lex Networkia: Understanding the Internet Community," *first Monday* <http://www.firstmonday.dk/issues/issue4/valauskas/>, published online in 1996 (Access: July 22, 2001).

Yoshida, Kazuhiko, *Invisible Cryptographic War (Ango Senso)* (Tokyo: Shogakkan, 1998, Japanese).

Young, Oran R., *Governance in World Affairs* (Ithaca: Cornell University Press, 1999).

Zacher, Mark W., with Brent A. Sutton, *Governing Global Networks: International Regimes for Transportation and Communications* (New York: Cambridge University Press, 1996).