Multilateral Solutions for Protecting Cyberspace

Learning Object Description

This learning object discusses international endeavors to protect cyberspace. It looks at the way international regimes come about and how they are formed. This learning object also highlights fundamental assumptions made by security specialists with regard to the use of cyberspace and the implications of these assumptions with regard to security policy. Various international endeavors are investigated. The last section of the learning object looks at the possibility of establishing an arms control regime and the challenges that would have to be overcome to establish such a regime.

Learning Object Objectives

The student will understand why international efforts are necessary to protect cyberspace. Students will understand what an international regime is, what the fundamental assumptions of such regimes are regarding cyberspace, and the ways in which these assumptions ultimately influence future cyberspace protection regimes. Students can describe international initiatives that have been introduced in response to the need to protect cyberspace against malicious abuse. They can argue why an arms control regime that governs information operations is urgently needed, and they understand which obstacles have to be overcome to establish such a regime.

Introduction

The current information revolution has brought about the information age and along with it myriad changes, opportunities, and risks in the economic, military, political, and societal realms. The benefits of e-government and e-commerce are clearly evident, as is the need to provide trustworthy systems and lasting infrastructures. If these are not provided, the information revolution will not progress. Hence, an increasing number of international organizations, governments, businesses, and NGOs are beginning to look at building secure electronic environments and ensuring protection of their critical information infrastructures.

At the same time, however, the United States and its NATO allies are developing doctrines and capabilities for exploiting cyberspace for their military advantage. In other words, the US military and the militaries of other NATO member states have invested heavily in military technologies and doctrines designed to disrupt the (information) infrastructures of rival nations. The US and NATO believe that these will give them a comparative strategic advantage, and they will be reluctant to give them up. Consequently, we can observe two parallel developments: On the one hand, various militaries are developing their ideas and doctrines on information operations and are pushing for an offensive and aggressive use of cyberspace. On the other hand, many official bodies are calling for initiatives to protect cyberspace from enemy nations and terrorist groups.

The question arises: Will there ever be an international regime for the protection of cyberspace, and if so, what shape will it take? The need for multilateral action to control criminal and terrorist activity on the Internet has been recognized and is being pursued by official bodies such as the Council of Europe. However, any efforts to control the military use of computer exploitation through mechanisms such as arms control or multilateral behavioral norms are simultaneously being undermined by the fundamental question that leading powers have yet to resolve: Should the strategic advantage of ICT be exploited, or should cyberspace be protected?

This learning object addresses these issues by looking at multilateral solutions to protect cyberspace. We will start with a general introduction of various international regimes.

The Importance of International Regimes in Protecting Cyberspace

Why should the protection of cyberspace occur at an international level? Security is a global issue. In particular, the vulnerability of modern societies, which arises from societies' dependence on a range of highly interdependent information systems, has global origins and global implications. In particular:

- Information infrastructures transcend territorial boundaries. Therefore, information assets vital to the national security and the functioning of the economy of one state may reside outside its own sphere of influence, on the territory of other nation states.

- Malicious actors in cyberspace do not hesitate to contravene national legal frameworks, and they are hidden in the relative anonymity of cyberspace – a huge, tangled, diverse, and literally universal electronic interchange that exists wherever there are telephone wires, cables, computers, or electromagnetic waves.

Any adequate protection policy to protect strategically important information infrastructures will ultimately have to be transnational. Such a policy may take the form of an international regulatory regime for the protection of cyberspace.

Regimes are usually defined as "sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors' expectations converge in a given area of international relations" (Krasner, 1983:2). Such regimes are formed when various stakeholders negotiate solutions to their disparate political interests. The outcome of such negotiations are new rules that constrain actors' choices and prescribe who can act when. These rules thus affect the stakeholders' behavior both directly and indirectly.

Reference

For more in-depth reading on international regimes, consult the seminal work by Stephen D. Krasner.

Krasner, Stephen D. (ed) (1983). *International Regimes.* Ithaca: Cornell University Press.

In the past two decades, there have been many international initiatives to improve the security and dependability of systems, of management practices, and of international policing efforts. These initiatives now form a complex and overlapping web of national, regional, and multilateral rules. However, the establishment of coherent international rules and norms on the use of cyberspace has been hampered by two fundamentally different ways of looking at the use of cyberspace. In the next section, we will look more closely at these questions.

Two Paradigms for the Protection of Cyberspace

There are two distinct ways of dealing with and looking at cyberspace protection. These two paradigms are outlined below:

Cyber-Threats as a Threat to the Economic Prosperity of All Nations

One model is based on the notion that threats originate mainly from organized crime, electronic vandalism, and corporate espionage, thus putting in danger the economic prosperity and social stability of all nations that are part of the global information infrastructure. According to this paradigm, all nations have an interest in devising international regimes that will ensure the trustworthiness and survival of information networks. A range of mechanisms could be used to counter the risks, and the paradigm foresees a non-zero-sum game. A zero-sum game is a situation in which a participant's gain (or loss) is exactly balanced by the losses (or gains) of the other participant(s) – so-called because the total gains of the participants minus the total losses equals zero. In a non-zero-sum game, one actor's gain is not necessarily a loss to other actors. In fact, in non-zero-sum games the players' interests can be the same. International organizations can promulgate information security standards, and industry can be encouraged to make its information systems more secure and dependable. International law enforcement institutions and mechanisms – for instance, Interpol – can exchange information and engage in joint investigations, while multilateral conventions on computer crime, such as the Council of Europe convention, can be negotiated in ways similar to those for hijacking and other forms of crime. It will always be difficult to undertake transnational investigations and tracebacks, but if all parties work together, the resulting measures can facilitate such actions against cyber-crime.

Cyber-Threats as a Threat to National Security

The second model is based on the notion that nation states are the key threat to national security. In this model, information operations and attacks against the information infrastructure are considered tools of strategic coercion. Attacks that breach the confidentiality, integrity, and/or availability of information systems could theoretically be treated as weapons of war and should thus be subject to arms control or the laws of armed conflict. According to this paradigm, existing mechanisms and methods, such as the laws of armed conflict and arms control/verification regimes, might apply to this new weapon system. Those who perceive cyber-threats as a threat to national security see any attempt to counter malicious use of cyberspace as a zero-sum game.

Militaries face a particular dilemma: On the one hand, they wish to exploit cyberspace to their advantage and develop doctrines and capabilities as part of their information operations, yet on the other hand, they are worried about the dependency of militaries, governments, economies, and societies on the networked information systems that have become the backbone of post-industrialized societies. This dilemma needs to be addressed before international regimes and a clear direction in policy can be developed.

In the next section, we will look at the two paradigms in more detail. We will start with the many international initiatives that are based on the notion that cyber-threats are a threat to the economic well-being of all nations.

Exercises

Before continuing, please complete the two exercises below.

Question 1

Give a definition of the term “international regime”:

✍____

Question 2

Which of the following statements are correct?

- ☐ Attacks of one nation state against the information infrastructure of another could, in theory, be seen as violations of human rights or crimes against humanity.
- ☐ Attacks of one nation state against the information infrastructure of another could, in theory, be seen as violations against laws or regulations governing arms control or armed conflicts.
- ☐ A zero-sum game is a situation in which a participant’s gain (or loss) is exactly balanced by the losses (or gains) of the other participant(s).
- ☐ A zero-sum game is a situation in which a participant’s gain (or loss) amounts to exactly twice the losses (or gains) of the other participant(s).
- ☐ Cyber-threats cannot be considered a threat to the economic prosperity of all nations.
- ☐ Cyber-threats can be considered a threat to the economic prosperity of all nations.

Protecting Cyber-Space: International Approaches

For several years, high-ranking European and US policy-makers have expressed concern that insecure information systems are threatening economic growth and national security. As a result, they have established a complex web of national, regional, and multilateral initiatives. The force driving these initiatives stems from the inadequacy of existing state-centric policing and legislative structures for policing international networks, and from the recognition that private networks must be protected from disruption.

We can divide these initiatives into four types, according to the main focus taken by the multilateral actors who launched them:

Deterrence

Measures that discourage the abuse and destruction of an asset

Prevention

Measures that prevent assets from being damaged or destroyed

Detection

Measures that help to discover when, how, and who has damaged or destroyed an asset

Reaction

Measures that stop ongoing damage or destruction and help repair the damage to an asset

In the following, we will look at the four different categories in more detail.

Deterrence – the use of multilateral cyber-crime legislation

Multilateral initiatives to protect systems from the malicious use of cyberspace include initiatives to a) unify various cyber-crime legislations in order to facilitate international prosecution of criminals and to promote tougher criminal penalties (e.g. the Council of Europe Convention on Cybercrime); and b) improve e-commerce legislation (e.g. work on electronic commerce undertaken by the United Nations Commission on International Trade Law [UNCITRAL]).

Have a look at one of the following links for an impression of ongoing deterrence efforts.

Council of Europe Convention on Cybercrime

Since the late 1980s, the Council of Europe (CoE) has been trying to address the growing international concerns regarding threats posed by hacking and other computer-related crimes. In 1997 the CoE established its Committee of Experts on Crime in Cyberspace (PC-CY), whose task is to draft a binding convention to facilitate international cooperation in the investigation and prosecution of computer crimes.

Hyperlink to http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm

United Nations Commission on International Trade Law (UNCITRAL)

This website contains the reports of the UNCITRAL working group on e-commerce.

Hyperlink to http://www.uncitral.org/english/workinggroups/wg_ec/index.htm

Prevention – designing and using more secure systems and better security management, and promoting security mechanisms

Multilateral initiatives to prevent the malicious use of cyberspace aim to a) promote the design and use of more secure information systems (e.g. the Common Criteria Project); b) improve information security management in both the public and private sectors (e.g. the ISO and OECD standards and guidelines initiatives); c) establish a legal and technological framework, such as the use of security mechanisms (e.g. electronic signature legislation in Europe).

Have a look at one of the following links, if you are particularly interested in preventive security initiatives.

Common Criteria Project

The Common Criteria Project is developing and applying common criteria for IT security evaluation.

Hyperlink to http://www.commoncriteriaportal.org/

ISO standard in information security management

The International Organization for Standardization ISO has developed a code of practice for information security management (ISO/IEC 17799:2000). Find more information about ISO on this website.

Hyperlink to http://www.iso.org/iso/en/prods-services/popstds/informationsecurity.html

OECD guidelines initiatives

The Organisation for Economic Co-operation and Development (OECD) promotes a "culture of security" for information systems and networks. Find the relevant guidelines here.

Hyperlink to

http://www.oecd.org/document/42/0,2340,en_2649_33703_15582250_1_1_1_1,00.html

Detection – cooperative policing mechanisms and early warning about attacks

Multilateral initiatives to detect the malicious use of cyberspace include a) the creation of enhanced cooperative policing mechanisms (e.g. the G-8 national points of contact for cyber-crime); and b) early warning through information exchange between the public and private sectors, aimed at providing early warning about cyber-attacks (e.g. US Information Sharing and Analysis Centers, the European Early Warning and Information System, and the European Network and Information Security Agency [ENISA]).

European Network and Information Security Agency (ENISA)

ENISA was created in 2004. Get more information about its work here.

Hyperlink to http://www.enisa.eu.int/

Reaction – the design of more resilient information infrastructures, crisis management programs, and policing and judicial endeavors

Multilateral initiatives that aim to react to the malicious use of cyberspace include a) the design of robust and resilient information infrastructures; b) the development of crisis management systems; and c) the improvement of the coordination of policing and criminal justice efforts.

These four types of initiatives and most of the information provided in this section is based on an article by Andrew Rathmell entitled "Controlling Computer Network Operations".

Reference

Rathmell, Andrew (2001). “Controlling Computer Network Operations.” In: Wenger, Andreas (ed.). The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal 7 (2001), 121-144.

You can download the article in a printer-friendly format from the ISN Publishing House.

Hyperlink to http://www.isn.ethz.ch/pubs/ph/details.cfm?r_oID=707

To sum up, the international initiatives mentioned above involve significant investments of time and labor of the government departments of many countries, of many international organizations, and of many companies, big and small.

However, these initiatives are so diverse that we cannot speak of a regime as defined above. Further, NATO countries are developing doctrines and capabilities that will allow them to exploit cyberspace to their military advantage as part of their information operations. Thus, there remains a policy dilemma between the notion that cyber-threats are a threat to the economic well-being of nations and the notion that cyber-threats are a threat that arises in one country and is directed at another. The debate between those pursuing the military (offensive) track and those pursuing the civil (defensive) track is likely to intensify and could undermine attempts to produce an effective cyber-protection regime.

Exercises

Before continuing, please complete the three exercises below.

Question 3

Which of the following statements is correct?

□ Regimes emerge when a particular issue has transnational implications.

□ Regimes emerge when various stakeholders negotiate solutions to their disparate interests.

□ Regimes emerge when all state and regional actors agree on a given outcome.

Question 4

What are the four types of national and international initiatives on cyber-threats?

□ Interference

□ Deterrence

□ Prevention

□ Dissection

□ Detection

□ Action

□ Reaction

Question 5

Describe, in your own words, the reason for the newly established web of national, regional, and multilateral initiatives that aim to ward off the malicious use of the cyberspace:

✍____

We now come back to the security paradigm that treats attacks – breaches of the confidentiality, integrity, or availability of information systems – as weapons of war and views such attacks as violations against arms control regulations or the laws of armed conflict. In the following, we will discuss attempts by various actors to deal with cyber-attacks as tools used in information operations and as an issue pertaining to arms control.

Arms Control in Cyberspace

What are the main characteristics of arms control? Arms control is

- Based on the assumption that a given security threat can be controlled through cooperative regulations rather than by unilateral measures
- Based on the premise that there is or could be a mutual, not one-sided threat to the political-military security and survival of a country or countries
- Dependent upon the willingness of the protagonists to engage in cooperative security policy and arms control endeavors in a specific area

Arms control approaches aimed at warding off information infrastructure attacks are already under discussion. Future treaties might focus on the development, distribution, and deployment of cyber-weapons, or they might apply only to the use of cyber-weapons; they might relate primarily to criminal law, or they might govern the conduct of nation states under international law.

However, it is difficult to believe that traditional capability-based arms control will be of much use, as it is impossible to verify that the regulations governing the technical capabilities are being adhered to by a state. At present, the best arms control methods available are information exchange and norm-building; by comparison, structural approaches that prohibit the means of information warfare altogether or restrict their availability are useless in the fight against cyber-attacks because information technology is so widely available and has a dual purpose.

Although the creation of organized military information operation units could be monitored by Western intelligence services, the proliferation of information infrastructure attack capabilities cannot be monitored, since the technology is globally available. Multilateral and national arms control regimes are only now beginning to deal with the possibility of controlling the proliferation of software and know-how (as opposed to hardware), indicating how difficult controls are when cyber-attack code is stored on Internet host computers around the world.

Thus, an effective cyber-arms control treaty will have to take several obstacles into account. We will look at these in more detail below.

Obstacles to a Cyber-Arms Control Regime

This section looks at the obstacles to future cyber-arms control regimes. It deals mainly with computer network attacks and the cyber-weapons deployed in those attacks. These weapons (hacking tools) include software and methods for sabotaging systems and data and for launching computer viruses, worms, and denial-of-service attacks.

Enforceability

It has been extremely difficult to enforce existing criminal laws that govern computer network attacks. Many attacks are never detected initially. When they are, finding the perpetrators is seldom easy, especially when they have looped through many computers in various countries. An attack against computers in one country, for example, might appear to originate from government computers in another, while in fact it was launched by teenage hackers in a third country who had gained control of the other computers. It would be very difficult to enforce general laws against cyber-weapons, as such weapons can be manufactured without any special physical materials or laboratory facilities. All that is required is a computer and standard software. And once produced, cyber-weapons are easily copied and distributed on the Internet via e-mail, websites, instant messaging, peer-to-peer sharing systems, and other tools. Further, if a controlled cyber-weapon were detected, it would be impossible to find and destroy all copies, as these might be stored on thousands of computers around the world. Monitoring treaty compliance would also be difficult, given the rapid changes to technology and to the methods and tools of attack.

Security

An argument against enacting cyber arms controls that prohibit the production and distribution of attack tools is that such controls would curtail research and publication in the area of computer security. It is not possible to build strong defenses without knowing what attacks are possible and what vulnerabilities might be exploited, so investigating methods and tools of attack is an important element of cyber security.

Privacy

To investigate crimes in cyberspace, law enforcement agencies need to be able to search and seize digital evidence and to intercept network communications. In the United States, for example, the FBI developed Carnivore (a computer-based monitoring system), now called

DCS1000, to support court-authorized Internet wiretaps. Yet such law enforcement tools raise concerns about privacy. If a cyber-arms control treaty were to prohibit certain cyber-weapons, the process of policing the Internet in order to find these weapons would raise additional privacy concerns. Scanning the personal computers of citizens would violate the privacy laws of many nations

Free Speech

Restrictions on cyber-weapons, particularly on source code and scripts, would raise serious legal issues in countries with laws protecting the freedom of speech. In the United States, for example, speech is protected under the First Amendment, and software is considered a form of speech under US law.

Corporate Responsibilities and Liabilities

A cyber-arms control treaty could have a substantial impact on industry. Industry could be required to implement costly mechanisms to control the use or spread of cyber-weapons or to investigate violations of arms control regulations. Companies might also be held responsible for actions on their network that are in violation of laws of the particular treaty.

Foreign Policy

It will be impossible to establish useful cyber-arms controls if nation states are opposed to such controls. As we have shown above, attempts to impose international restrictions on information warfare would likely meet with resistance. And there are other reasons why sovereign states might oppose a cyber-arms control treaty, at least a treaty that applies to state-level operations (as opposed to one that applies to individual and organized criminal conduct). One reason is that such a treaty could be considered unnecessary, given existing international law, most notably the law of war. Governments might recognize a need for interpreting these laws and principles in the cyber-domain but might not see a need for new laws, at least for now. Governments might also oppose a treaty that restricts their ability to develop offensive cyber-weapons on the grounds that such restrictions would hamper their ability to prepare an adequate cyber-defense in the event of an attack. The United States says it is too early to negotiate an international agreement on information warfare, and the energy of the international community would be better spent in cooperating to secure information systems against criminals and terrorists.

Most of the information provided in this section is based on an article by Dorothy Denning.

Reference

Denning, Dorothy E. (2001). “Obstacles and Options for Cyber Arms Controls.” Paper presented at Arms Control in Cyberspace, Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001.

You can download the article in a printer-friendly format from Dorothy Denning’s website at Georgetown University.

Hyperlink to http://www.cs.georgetown.edu/~denning/infosec/berlin.doc

The problems outlined above are the main factors slowing down the development of norms for protecting cyberspace, when such norms involve the general prohibition of cyber-weapons. However, one option remains open: a treaty that pertains exclusively to the domestic criminal laws and procedures of the signatories. It would have no bearing on the law of war and the military operations of sovereign states. Indeed, the Council of Europe’s Cyber Crime Convention is an example of such an approach, as it applies only to criminal acts and law enforcement practices and procedures.

Exercise

Before continuing, please complete the exercise below.

Question 6

Which of the following statements about arms control in cyberspace are correct?

- □ The arms control approach to cyberspace protection is limited because of the widely spread availability of information technology and its dual use.
- □ A future arms control treaty might apply only to the use of cyber-weapons, not to their distribution and deployment.
- □ Arms control is an instrument of coercive security.

□ Traditional capability-based arms control seems to be a useless approach.

□ At present, the best arms control method available is the verification of limitations to technical capabilities.

Summary

This learning object has discussed some of the issues related to the protection of cyberspace. It has shown the two related paradigms that form the basis of the debate about risks in the information age, and it has highlighted the various initiatives to protect cyberspace launched by multilateral institutions, transnational and national businesses, and NGOs.

The following points are worth remembering:

- The development of information operations capabilities has brought about new vulnerabilities of both the military and societies. Militaries are exploiting ICTs to enhance their military force, and societies are dependent on critical (information) infrastructures, which might be targeted by enemy states or terrorist groups.
- Thus, the question remains open about whether the various stakeholders will coordinate their disparate interests and whether they will be able to form a regime – a set of implicit or explicit principles, norms, rules, and decision-making procedures – with regard to cyberspace protection.
- So far, increased concern about the security of information systems through which the economic growth and national security of a state might be threatened and the inadequacy of existing state-centric policies have brought about a complex web of national, regional, and multilateral initiatives.
- The various initiatives are designed to coordinate cyber-crime legislation, to promote the design and use of more secure information systems, to enhance cooperative policing mechanisms, to provide early warning systems and to promote the exchange of information, to design robust and resistant information infrastructures, and to develop crisis management systems.
- However, the underlying dilemma between policy approaches that aim at making cyberspace more resistant to criminal abuse and policy approaches that aim at making use of information operation tools has inhibited the development of a coherent set of norms for cyberspace protection. (The two diametrically opposed policy approaches are indicative of differing threat perceptions.)

- Arms control approaches to securing information infrastructures are already under discussion. Nevertheless, this approach has severe limitations, due to the ubiquity and dual-use of many ICTs. The two main challenges to the development of an effective arms control regime are, first, to get the support of the private sector and, second, to ensure that states are not disadvantaged in comparison to sub-state groups.

- Further obstacles to establishing an effective arms control regime are the enforcement of criminal national laws; the fear of curtailing research and publication; the need for a balance between securing the privacy of citizens and the policing of the Internet; legal issues with regard to free speech; the impact of such a regime on industry; and the need to make the benefits of such an agreement clear to governments.

Answers to the Exercises

Question 1

Give a definition of the term “international regime”:

Possible answer: *According to Stephen Krasner, international regimes are “sets of implicit or explicit principles, norms, rules, and decision-making procedures around which actors’ expectations converge in a given area of international relations”. Such regimes are formed when various stakeholders negotiate solutions to their disparate political interests. The outcome of such negotiations are new rules that constrain actors’ choices and prescribe who can act when. These rules thus affect the stakeholders’ behavior both directly and indirectly.*

Question 2

The following statements are correct:

- ✓ Attacks of one nation state against the information infrastructure of another could, in theory, be seen as violations against laws or regulations governing arms control or armed conflicts.
- ✓ A zero-sum game is a situation in which a participant’s gain (or loss) is exactly balanced by the losses (or gains) of the other participant(s).
- ✓ Cyber-threats can be considered a threat to the economic prosperity of all nations.

Question 3

The following statement is correct:

- ✓ Regimes emerge when various stakeholders negotiate solutions to their disparate interests.

Question 4

What are the four types of national and international initiatives on cyber-threats?

- ✓ Deterrence
- ✓ Prevention
- ✓ Detection
- ✓ Reaction

Question 5

Describe, in your own words, the reason for the newly established web of national, regional, and multilateral initiatives that aim to ward off the malicious use of the cyberspace:

Possible answer: *Many state and non-state actors have recognized that existing state-centric policy development, legislation, and law enforcement are inadequate. States, businesses, and NGOs who aim to improve the security of the global information environment have reacted to the perceived risks to national security and economic growth by creating various initiatives. Because there are many different aspects to cyber-security, these initiatives are very diverse.*

Question 6

The following statements about arms control in cyberspace are correct:

- ✓ The arms control approach to cyberspace protection is limited because of the widely spread availability of information technology and its dual use.
- ✓ A future arms control treaty might apply only to the use of cyber-weapons, not to their distribution and deployment.
- ✓ Traditional capability-based arms control seems to be a useless approach.

Bibliography

- Aldrich, Richard W. (1996). *The International Legal Implications of Information Warfare.* Colorado Springs: US Air Force Academy.

- Denning, Dorothy E. (2001). “Obstacles and Options for Cyber Arms Controls.” Paper presented at Arms Control in Cyberspace, Heinrich Böll Foundation, Berlin, Germany, June 29-30, 2001.
  URL http://www.cs.georgetown.edu/~denning/infosec/berlin.doc.

- Giacomello, Giampiero and Fernando Mendez (2001). “Cuius Regio, Eius Religio, Omnium Spatium? State Sovereignty in the Age of the Internet.” In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal* 7 (2001), 15-27.

- Gladman, Brian (1998). “Wassenaar Controls, Cyber-Crime and Information Terrorism, Cyber Rights and Cyber Liberties.”
  URL http://www.cyber-rights.org/crypto/wassenaar.htm.

- Hasenclever, Andreas, Peter Mayer, and Volker Rittberger (1997). *Theories of International Regimes.* New York: Cambridge University Press.

- Krasner, Stephen (ed.) (1983). *International Regimes.* Ithaca: Cornell University Press.

- Loader, Brian D. (ed.) (1997). *The Governance of Cyberspace.* London and New York: Routledge, 1997.

- Nye, Jospeh S. Jr. and John D. Donahue (eds.) (2000). *Governance in a Globalizing World*. Cambridge: Visions of Governance for the 21st Century.

- Rathmell, Andrew. “Controlling Computer Network Operations.” In: Wenger, Andreas (ed.). *The Internet and the Changing Face of International Relations and Security. Information & Security: An International Journal* 7 (2001), 121-144.

- Sofaer, Abraham D., Seymour D. Goodman, et al. (2000). *A Proposal for an International Convention on Cyber-Crime and Terrorism.* Center for International Security and Cooperation: Stanford University.

ISN
Run by CSS

This PDF was produced by the International Relations and Security Network (ISN) and is part of the e-learning course “Security in the Information Age”. Last update 26 March 2005.