

Critical information infrastructure: vulnerabilities, threats and responses

Myriam DUNN CAVELTY

The recent Estonian–Russian "cyberbattle" has once again focused the world's attention on the topic of cyberspace security and critical information infrastructure protection (CIIP). When the Estonian authorities began removing a Second World War memorial—a bronze statue of a Soviet soldier—from a park at the end of April 2007, a three-week cyberbattle ensued, in which a wave of so-called Distributed Denial of Service attacks (DDoS) swamped various web sites—among them the web sites of the Estonian parliament, banks, ministries, newspapers and broadcasters—disabling the sites by overcrowding the bandwidths for the servers running the sites.

The Estonian–Russian online squabble made headlines¹ and various officials pounced on the cyberwar theme, following an unfortunate but frequently observable pattern of hyperventilation in cybersecurity matters.² It was claimed both explicitly and implicitly that the Russian Federation was behind the attack and that this was the first known case of one state targeting another by cyber-warfare.³ One North Atlantic Treaty Organisation official reportedly said: "I won't point fingers. But these were not things done by a few individuals. This clearly bore the hallmarks of something concerted. The Estonians are not alone with this problem. It really is a serious issue for the alliance as a whole."⁴

A sober look at plain facts after the uproar reveals the usual pattern of such incidents: it is now clear that the "attacks" were not initiated by the Russian government or its security service. Fake Internet Protocol (IP) addresses—in this case, a Russian government computer was involved in the DDoS attack—are a routine part of any "hactivist" attack.⁵ Furthermore, the attacks were so low-tech and old-school that they were almost certainly carried out by large numbers of so-called script kiddies. These are teenagers with relatively little real computer expertise, who use readily available techniques and programs to search for and exploit weaknesses in other computers on the Internet. And finally, despite the fuss, the attacks had a relatively negligible effect (a usual feature of DDoS attacks).

There is an urgent need for such incidents to be considered in the right light, but fears connected to the risk of cyber-attacks cannot be entirely discounted as bogus. These fears, connected to the perception of the large-scale vulnerability of modern societies, have engaged the attention of security experts for a long time. This article will show how and why cybersecurity has come to dominate the *political* security debate at times over the last decade. It will look at the range of threats that seem to confront modern networked societies, set them into perspective and focus on obstacles and prerequisites of national and international protection measures.

Myriam Dunn Cavelyt is head of the New Risks Research Unit at the Center for Security Studies at ETH Zurich, Switzerland and coordinator of the Crisis and Risk Network, see <www.crn.ethz.ch>.

The rise of CIIP to the political security agenda

Protection concepts for strategically important infrastructures and objects have been part of national defence planning for decades.⁶ Today's concept of critical infrastructure protection (CIP), however, goes far beyond traditional national defence and military considerations. Its establishment as a focal point of the current national security debate is the result of two interlinked and at times reinforcing factors: the expansion of the threat spectrum after the Cold War, especially in terms of malicious actors and their capabilities; and a new kind of vulnerability due to modern society's dependence on inherently insecure information systems.

During the Cold War era, threats to national security mainly arose from the aggressive intentions of states to achieve domination over other states. The end of the Cold War brought the end of such clear, distinct threats: following the disintegration of the Soviet Union, a variety of "new" threats were moved onto the political security agendas of most countries.⁷ These challenges have a quality of uncertainty about them: uncertainty concerning the entire range of "who, how, where, what, why, when".⁸ Clearly, the understanding of "threat" as something imminent, direct and certain does not describe these challenges. Rather, they can be characterized as "risks", which are by definition indirect, uncertain and situated in the future.⁹

As a result of these diffuse risks and the difficulties of locating and identifying enemies, security policies have shifted away from focusing solely on actors, capabilities and motivations and toward looking at the general vulnerabilities of society as a whole as well. The United States military was a driving force behind the shaping of this threat perception in the early 1990s. As the only remaining superpower, the United States was considered predestined to become the target of asymmetric warfare, and those foes likely to fail against the US military might instead plan to bring the country to its knees by striking "soft targets" fundamental to the essential functioning of its entire society. These points are generally defined as critical infrastructure (CI). They are deemed critical because their incapacitation or destruction would have a debilitating impact on the national security and the economic and social welfare of a state. Examples are telecommunications, power grids, transport and storage of gas and oil, banking and finance, traffic, water supply systems, emergency rescue services and public administration.

Fear of asymmetric measures against such targets has been aggravated by the so-called information revolution. Today, almost all CI relies on a spectrum of software-based control systems for smooth, reliable and continuous operation. In many cases, information and communication technologies (ICTs) have become omnipresent, connecting infrastructure systems and making them interrelated and interdependent. The part of the information infrastructure that is essential for the continuity of CI services is known as critical information infrastructure (CII). CII is thus part of a state's CI and includes components such as computers, software, the Internet, satellites and fibre optics.

CII are in general regarded as inherently insecure. Most of the components are developed in the private sector, where competition means that pressure to reduce time-to-market is intense, and where security does not drive system design. Computer and network vulnerabilities are therefore to be expected, and these lead to information infrastructures with in-built instabilities and critical points of failure.¹⁰ Moreover, many researchers agree that the infrastructure is its own worst enemy because of its complexity.¹¹ Systems begin to blend into one another due to increasing use of ICTs and increasing functional demands and it is useless to try to maintain a separation of systems, each with an internally demarcated mode of responsibility. The distinction between inside and outside the system, and even the concept of systems boundaries as such, becomes blurred. Attacking infrastructure therefore has a "force-multiplier" effect that allows even a relatively small attack to achieve a great impact.¹² The spread of ICT appears to make the post-Cold War asymmetric threat easier; facilitating access to the

tools for attack, and making the success of an attack more likely. Borders, which are already porous in the real world, are non-existent in cyberspace.

The threat to CII

As most critical infrastructure is either based on or monitored and controlled by vulnerable ICT systems, the information infrastructure became *the* focal point of CI protection policies in the 1990s.¹³ Today, the information infrastructure is still regarded as an easy and vulnerable entry point. But discovering the threat to CII—the perpetrators, the likely nature of an attack—remains difficult.

The spectrum of potential perpetrators ranges from teenagers (the script kiddies described above), to sophisticated, expert hackers and crackers, to criminals, terrorists and even nation states. Since it would seem peculiar to cast all of these actors into the same pot, they are sometimes separated into two groups, based on organizational complexity, motivation and resources, albeit with fluent boundaries: the first group is considered to be an "unstructured" threat, the second a "structured" threat.¹⁴

The unstructured threat is random and relatively limited. It consists of adversaries with restricted funds and organization and short-term goals, such as individual hackers and crackers as well as small groups of organized criminals. The resources, tools, skills and funding available to the actors are too limited to accomplish a sophisticated attack against CI and, more important, the actors lack the motivation to do so. They do it for thrill, prestige or monetary gain. In contrast, structured threats are considerably more methodical and better supported. Adversaries from this group have extensive funding, organized professional support and access to intelligence products, and long-term strategic goals. Foreign intelligence services, well organized terrorists, professional hackers involved in information warfare, larger criminal groups and industrial spies fall into this threat category.

Unfortunately, there are no clear boundaries between the two categories. Even though an unstructured threat is not usually considered of direct concern to national security, there is a possibility that a structured threat actor could masquerade as an unstructured threat actor, or that structured actors could seek the help of technologically skilled individuals from the other group. While ordinary hackers lack the motivation to cause violence or severe economic or social harm,¹⁵ it is feared that an individual with the capability to cause serious damage but lacking motivation could be swayed by sufficiently large sums of money to provide knowledge to more malicious actors.

The global nature of information networks means that attacks can be launched from anywhere in the world, so discovering the origins of an attack remains a major difficulty, if indeed the attack is detected at all. The problem of identifying actors is made particularly complicated by time lapses between an intruder taking action, the intrusion itself and the effects of the intrusion. Methods of attack have also become more sophisticated, even automated in parts, resulting in greater damage from a single attack. Furthermore, technology develops extremely quickly: the time between the discovery of a new vulnerability and the emergence of a new tool or technique that exploits that vulnerability is getting shorter. Indeed, the technology employed in many attacks is simple to use, inexpensive and widely available on computer bulletin boards and various web sites, as are encryption and anonymity tools. Without doubt, cyberthreats fall into the category of "new" challenges: indirect, and all too uncertain.

CYBERTERROR? UNLIKELY

Not surprisingly, the attacks of 11 September 2001 strengthened the general CIP debate's focus on terrorism, including cyberterrorism. The media is fascinated by the "cyber-" prefix in connection with disaster, and routinely features sensationalist headlines.¹⁶ For their part, experts and government

officials also frequently warn about cyberterrorism as a looming threat to national security. This creates a strange circle of news generation: the evidence that is presented in hearings is often based on (true or false) stories in the media; the media then quote these government officials' statements.

"Cyberterrorism" plays on two fears of the unknown: of the power of computer technology and of random and violent victimization.¹⁷ A highly emotive word then, and frequently misused, although the fears that it invokes make a concise definition and accurate usage all the more important. Only attacks that are carried out by terrorists, which instil fear by effects that are destructive or disruptive, and which have a political, religious or ideological motivation, should fall under the term cyberterrorism.¹⁸

According to this definition, none of the disruptive incidents that we have seen so far qualify as examples of cyberterrorism. In fact, even though most terrorist groups have seized on the opportunity accorded by the information revolution to establish a multiple web presence for recruitment and fundraising purposes, as well as the dissemination of uncensored propaganda,¹⁹ cyberspace has so far mainly served terrorists as a force multiplier in intelligence gathering and target acquisition, and not as an offensive weapon. And, in the eyes of some experts, it is unlikely to emerge as a weapon of choice.²⁰ So although we cannot afford to shrug off the threat altogether, because of the rapid progress of technological development and changes in the capabilities of terrorist groups,²¹ decision makers as well as experts must be very careful not to foment "cyber-angst" and add to the hype that is clouding the issue.

The infrastructure of modern societies is vulnerable to all kinds of threats and risks, and terrorism is neither the most likely nor the most dangerous in terms of damage. Risks from natural disasters,

The entire CIIP debate can only benefit if it moves away from focusing too much on malicious attacks and toward the far broader range of potentially dangerous events.

mechanical failure and the inadvertent actions of an authorized user are just as serious as the risk of deliberate attack. The complexity of CII means that even planned maintenance operations, despite careful assessment and approval procedures, can cause disruptions. Clearly, the entire CIIP debate can only benefit if it moves away from focusing too much on malicious attacks and toward the far broader range of potentially dangerous events, including failure due to human error or technical problems. This not only does justice to the many facets of the security problem, but also prevents us from carelessly invoking the term terrorism.

CIIP: toward an all-hazard approach and a resilience strategy

Comprehensive protection of the entire critical infrastructure against all threats and risks is impossible, not only for technical and practical reasons, but also because of costs. So the greatest vulnerabilities need to be identified; those structures that are more critical, or vital points within the infrastructure. Criteria could also focus on the relative likelihood of the threat or the relative cost of protection. But when considering actual protection measures, all of these require knowledge of the nature of the threat: it makes a difference whether one needs to protect a facility against a group of well trained attackers or whether one wants to shield information systems from unauthorized access. There is no one-fits-all solution: protection measures have to be tailored to specific assets and specific threats.

For as long as there are no reliable data on the likely nature of threats, another approach promises better results. This focuses on the likely *effects* of a failure of a specific infrastructure or asset and seeks to mitigate them. The reasoning for this is quite simple, especially for CII: from the perspective of maintaining reliable services, it is not so important whether the events that triggered the surprise originated from within or outside the infrastructure. In practice, it is in fact often difficult to determine whether a particular detrimental event is the result of a malicious attack, a component failure or an

accident.²² The first and most important question is not what caused the loss of information integrity, but rather what the possible result and complications may be. A power grid might fail because of a simple operating error without any kind of external influences, or because of a sophisticated hacker attack. In both cases, the result is the same: a possible power outage that may set off a domino effect of successive failures in interlinked systems. Analysing whether a failure was caused by a terrorist, a criminal, simple human error or spontaneous collapse will not help to stop or reduce the effect.

It is therefore beneficial to follow an "all hazards" approach, designed for protection efforts irrespective of the nature of the threat, with a focus on the capability to respond to a whole spectrum of unanticipated events. The key is to create greater resilience, commonly defined as the ability of a system to recover from adversity and either revert to its original state or assume an adjusted state based on new requirements.²³ Most precautionary and response measures can be employed as protection against both deliberate and natural surprises, except for the activities of the intelligence services and certain police and military responsibilities (such as physical protection), which are all geared toward actor-induced threats.²⁴

NEED FOR COOPERATION WITH THE PRIVATE SECTOR

An all hazards approach, indeed any CIIP policy,²⁵ requires cooperation: when it comes to providing security for their citizens, governments can no longer go it alone. In many countries, the provision of energy, communications, transport, financial services, etc. have been, or are being, privatized.²⁶ Thus ownership, operation and supply of CII are largely in the hands of the private sector. Collectively, the private sector has far more technical resources and operational access to CII than the government.²⁷ But it has not used these resources to maximize security: satisfying shareholders by maximizing company profits has often led to minimal security measures. The government, however, wants industry to take responsibility for implementing protection measures in line with the parameters or frameworks set by public authorities.²⁸ In order to gain the support of the private sector without having to introduce heavy regulation, governments must strive to create a mutual win-win situation.

Luckily, states can provide a number of services that are of interest to the private sector. Clearly, CII operators know their business better than any governmental unit and usually have many other sources from which to obtain warnings or advice. However, a state-run CIIP unit would be able to provide non-technical analyses of the general risk situation prepared by national and international intelligence services, such as information about the nature of criminal organizations. Also, the private sector could gain knowledge about incidents and lessons learned by an exchange with other private actors mediated by a "neutral" government entity.²⁹ Further, states can provide financial assistance, through funding research on protection technologies and contributing to implementation costs.³⁰

GLOBAL ISSUE, GLOBAL RESPONSE

National efforts can only go so far: the vulnerability of modern societies—caused by their dependence on a spectrum of highly interdependent information systems—has global origins and implications. The information infrastructure transcends territorial boundaries, so that information assets that are vital to the national security and the essential functioning of the economy of one state may reside on the territory of other states. Additionally, cyberspace—a huge, tangled, diverse and almost ubiquitous web of electronic interchange—is present wherever there are telephone wires, cables, computers or electromagnetic waves, a fact that severely curtails the ability of individual states to regulate or control it alone. Any adequate protection policy that extends to strategically important parts of the information infrastructure will thus require transnational solutions.

However, an underlying tension concerning the use of cyberspace has been partly responsible for preventing the coherent establishment and implementation of rules and norms at the international level.³¹ Some states are developing doctrines and even capabilities to exploit cyberspace for military advantage: they are investing in military technologies and doctrines designed to disrupt the (information) infrastructure of rival states. The offensive and aggressive use of cyberspace, and initiatives to protect cyberspace from aggressors, are being pursued simultaneously.³² Due to this, there have been calls for efforts to control computer exploitation by state militaries through arms control or multilateral behavioural norms, agreements that might pertain to the development, distribution and deployment of cyberweapons, or to their use.³³ However, traditional capability-based arms control will clearly not be of much use, mainly because it is impossible to verify any such controls. Structural approaches, attempts to prohibit the means of information warfare altogether or to restrict their availability, are largely unfeasible because of the ubiquity and dual-use nature of information technology.³⁴ The avenues available for arms control in this arena seem primarily information exchange and norm-building, and even these are only being pursued to a limited degree.

Although there may be tensions regarding the use of cyberspace, and traditional arms control cannot meet the challenges posed by information technology, other international approaches are more promising. One key issue for all states is the harmonization of law to facilitate the prosecution of perpetrators of cybercrime. Cybercrime is considered a menace to the economic prosperity and social stability of all states that are plugged into the global information infrastructure. All states therefore have an interest in working together to devise an international regime³⁵ that will ensure the reliability and survivability of information networks. Again, this is more of a resilience strategy than a threat-focused approach. Multilateral conventions on computer crime, such as the Council of Europe's Convention on Cybercrime (2001), could be expanded and built on. International organizations could help develop and promulgate information security standards and disseminate recommendations and guidelines on best practices. International law enforcement institutions and mechanisms, like Interpol, could be used for information exchange—in order to provide early warning of any attack—and cybercrime investigations. Enhanced cooperative policing mechanisms could also be created.

It is key, however, not to duplicate efforts already undertaken at national level or below: the principles of subsidiarity and proportionality must be taken into account at all times. Activity at the international level should concentrate on challenges that cannot be mastered by a state or region on its own, such as global infrastructures, like the Internet, or truly large-scale interdependencies. By taking such steps, international organizations can help to strengthen the complex and at times overlapping web of national and regional initiatives in the realm of CIIP, and can improve the security and dependability of systems, management practices and international policing efforts.

Cooperation: the key to CIIP

The protection of critical information infrastructure has reached the international political security agenda. Cyberterror is often mentioned in relation to these threats, but the menace in fact ranges far wider, from more straightforward crime to natural disaster and even basic human error. But comprehensive protection against the entire range of threats and risks at all times is near impossible, not only for technical and practical reasons, but also because of the associated costs. What is possible is to focus protective measures on preventive strategies and on trying to minimize the impact of an attack when it occurs.

Because it is mainly infrastructure providers that are in the position to install technical safeguards for information technology security at the level of individual infrastructures, national governments depend on cooperation with the private sector to provide the public good of security to their citizens. But national protection measures only go so far: the securing of the global information infrastructure is a global task. Currently, divergences between national CIIP policies are a major obstruction to the development of an international regime, for international regimes are based on at least a minimal convergence of expectations and interests of (national) key actors. However, in consideration of their economic and security interests, industrialized states are working to overcome these temporary obstacles in order to move resolutely toward robust international conventions and mechanisms that protect the global information environment.

Notes

1. See, for example, "Cyberattack on Estonia Stirs Fear of 'Virtual War'", *International Herald Tribune*, 18 May 2007, at <www.iht.com/articles/2007/05/18/news/estonia.php>; "The Cyber Raiders Hitting Estonia", *BBC News*, 17 May 2007, at <news.bbc.co.uk/1/hi/world/europe/6665195.stm>; "Estonia Urges Firm EU, NATO Response to New Form of Warfare: Cyber-attacks", *The Sydney Morning Herald*, 16 May 2007, at <www.smh.com.au/news/Technology/Estonia-urges-firm-EU-NATO-response-to-new-form-of-warfare-cyberattacks/2007/05/16/1178995207414.html>.
2. Myriam Dunn Cavelty, forthcoming 2007, *Cyber-security and Threat Politics: US Efforts to Secure the Information Age*, London, Routledge.
3. "Russia Accused of Unleashing Cyberwar to Disable Estonia", *The Guardian*, 17 May 2007, at <www.guardian.co.uk/frontpage/story/0,,2081512,00.html>.
4. *Ibid.*
5. Hacktivism stands for the marriage of hacking and activism, and describes operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage. Examples are web "sit-ins" and virtual blockades, automated e-mail bombs, web hacks, computer break-ins, and computer viruses and worms. See Dorothy E. Denning, 2001, "Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy", in J. Arquilla and D. Ronfeldt (eds), *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica, CA, RAND, pp. 239–288.
6. Eric A.M. Luijff, Helen H. Burger and Marieke H.A. Klaver, 2003, "Critical Infrastructure Protection in the Netherlands: A Quick-scan", in Urs E. Gattiker, Pia Pedersen and Karsten Petersen (eds), *EICAR Conference Best Paper Proceedings 2003*, at <www.crypto.rub.de/imperia/md/content/lectures/kritis/bpp_13_cip_luijff_burger_klaver.pdf>.
7. B. Buzan, O. Wæver and J. de Wilde, 1998, *Security: A New Framework for Analysis*, Boulder, CO, Lynne Rienner.
8. E.O. Goldman, 2001, "New Threats, New Identities, and New Ways of War: The Sources of Change in National Security Doctrine", *Journal of Strategic Studies*, vol. 24, no. 2, p. 45.
9. J. van Loon, 2000, "Virtual Risks in an Age of Cybernetic Reproduction", in B. Adam, U. Beck and J. van Loon (eds), *The Risk Society and Beyond: Critical Issues for Social Theory*, London, Sage, pp. 165–182.
10. Michael Näf, 2001, "Ubiquitous Insecurity? How to 'Hack' IT Systems", *Information & Security: An International Journal*, no. 7, pp. 104–118.
11. M.J.G. van Eeten, E.M. Roe, P. Schulman and M.L.C. de Bruijne, 2006, "The Enemy Within: System Complexity and Organizational Surprises", in M. Dunn and V. Mayer (eds), *International CIIP Handbook 2006. Vol. II: Analyzing Issues, Challenges, and Prospects*, Zurich, Center for Security Studies at ETH Zurich, at <www.crn.ethz.ch/publications/crn_team/detail.cfm?id=16157>, pp. 89–109.
12. Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, Threat Analysis No. TA03-001, 12 March 2003, at <www.ocipep-bpiepc.gc.ca/opsprods/other/TA03-001_e.pdf>.
13. The attacks of 11 September 2001 highlighted the fact that terrorists could cause enormous damage by attacking critical infrastructures directly and physically and thus demonstrated the need to re-examine physical protections as well. See J.D. Moteff, 2003 (updated 13 March 2007), *Critical Infrastructures: Background, Policy, and Implementation*, Congressional Research Service report RL30153, Washington, DC, at <www.fas.org/spp/crs/homsec/RL30153.pdf>, p. 3.
14. National Research Council, 1991, *Computers at Risk: Safe Computing in the Information Age*, Washington, DC, National Academy Press; Kenneth A. Minihan, Director, National Security Agency, Statement to the Senate Governmental Affairs Committee on Vulnerabilities of the National Information Infrastructure, at <www.senate.gov/~gov_affairs/62498miniham.htm>, 24 June 1998.
15. Dorothy E. Denning, 2002, "Is Cyber Terror Next?", in Craig Calhoun, Paul Price and Ashley Timmer (eds), *Understanding September 11*, New York, W.W. Norton, at <www.ssrc.org/sept11/essays/denning.htm>.

16. See, for example, "Bracing for Guerrilla Warfare in Cyberspace", *CNN Interactive*, 6 April 1999; "Terror Groups Hide behind Web Encryption", *USA Today*, 5 February 2001; "Suspect Claims Al Qaeda Hacked Microsoft – Expert", *Newsbytes*, 17 December 2001; "FBI: Al Qaeda May Have Probed Government Sites", *CNN*, 17 January 2002; "Islamic Cyberterror. Not a Matter of If But of When", *Newsweek*, 20 May 2002.
17. M.M. Pollitt, "Cyberterrorism – Fact or Fancy?", *Proceedings of the 20th National Information Systems Security Conference*, October 1997, pp. 285–289.
18. Maura Conway, 2002, "Reality Bytes: Cyberterrorism and Terrorist 'Use' of the Internet", *First Monday*, vol. 7, no. 11, <firstmonday.org/issues/issue7_11/Conway>; Myriam Dunn Cavelty, forthcoming 2007, "Cyber-Terror—Looming Threat or Phantom Menace? The Framing of the US Cyber-Threat Debate", *Journal of Information Technology and Politics*, vol. 4, no. 1.
19. Timothy L. Thomas, 2003, "Al Qaeda and the Internet: The Danger of 'Cyberplanning'", *Parameters*, spring, pp. 112–123; Gabriel Weimann, 2004, *www.terror.net. How Modern Terrorism Uses the Internet*, United States Institute of Peace, Special Report 116; Gabriel Weimann, 2004, *Cyberterrorism—How Real Is the Threat?* United States Institute of Peace, Special Report 119.
20. S. Barak, 2004, "Between Violence and 'E-jihad': Middle Eastern Terror Organizations in the Information Age", in L. Nicander and M. Ranstorp (eds), *Terrorism in the Information Age – New Frontiers?* Stockholm, Swedish National Defence College, pp. 83–96.
21. Institute for Security Technology Studies, Technical Analysis Group, 2004, *Examining the Cyber Capabilities of Islamic Terrorist Groups*, Dartmouth College, NH, at <www.ists.dartmouth.edu/TAG/ITB/ITB_032004.pdf>.
22. R.J. Ellison, D.A. Fisher, R.C. Linger, H.F. Lipson, T. Longstaff, and N.R. Mead, 1997 (updated 1999), *Survivable Network Systems: An Emerging Discipline*, technical report CMU/SEI-97-TR-013, ESC-TR-97-013, at <www.cert.org/research/97tr013.pdf>, p. 3.
23. John A. McCarthy, 2007, "Introduction: From Protection to Resilience: Injecting 'Moxie' into the Infrastructure Security Continuum", in *Critical Thinking: Moving from Infrastructure Protection to Infrastructure Resilience*, CIP Program Discussion Paper Series, Washington, DC, George Mason University, at <cipp.gmu.edu/archive/CIPP_Resilience_Series_Monograph.pdf>, pp. 2–3.
24. Sergio Bonin, 2007, *International Biodefense Handbook 2007: An Inventory of National and International Biodefense Practices and Policies*, Zurich, Center for Security Studies at ETH Zurich, p. 378.
25. I. Abele-Wigert and M. Dunn, 2006, *International CIP Handbook 2006. Vol. 1: An Inventory of 20 National and 6 International Critical Information Infrastructure Protection Policies*, Zurich, Center for Security Studies at ETH Zurich.
26. Jan Joel Andersson and Andreas Malm, 2006, "Public-Private Partnerships and the Challenge of Critical Infrastructure Protection", in M. Dunn and V. Mauer (eds), op. cit., pp. 139–167.
27. Z. Baird, 2002, "Governing the Internet: Engaging Government, Business, and Nonprofits", *Foreign Affairs*, vol. 81, no. 6, pp. 15–20.
28. Seymour E. Goodman, Pamala B. Hassebroek, Daving Kind and Andy Azment, 2002, *International Coordination to Increase the Security of Critical Network Infrastructures*, document CNI/04; Olivia Bosch, 2002, *Cyber Terrorism and Private Sector Efforts for Information Infrastructure Protection*, both papers presented at the ITU Workshop on Creating Trust in Critical Network Infrastructures, Seoul, 20–22 May 2002.
29. Center for Security Studies at ETH Zurich, 2006, *Information Security in Swiss Companies: A Survey on Threats, Risk Management and Forms of Joint Action*, Zurich; Manuel Suter, 2007, *A Generic National Framework For Critical Information Infrastructure Protection*, paper presented at the ITU 2nd Facilitation Meeting for WSIS Action Line C5: Building Confidence and Security in the Use of ICTs, at <www.itu.int/osg/spu/cybersecurity/pgc/2007/events/docs/background-paper-suter-C5-meeting-14-may-2007.pdf>.
30. I. Abele-Wigert and M. Dunn, op. cit., pp. 385–402.
31. A. Rathmell, 2001 "Controlling Computer Network Operations", *Information & Security: An International Journal*, no. 7, pp. 121–144.
32. Ibid.
33. Heinrich Böll Stiftung, 2001, *Perspectives for Peace Policy in the Age of Computer Network Attacks*, Conference Proceedings, at <www.boell.de/downloads/medien/DokuNr20.pdf>; Dorothy E. Denning, 2001, *Obstacles and Options for Cyber Arms Controls*, paper presented at Arms Control in Cyberspace Conference, Heinrich Böll Foundation, Berlin, 29–30 June 2001, at <www.cs.georgetown.edu/~denning/infosec/berlin.doc>.
34. Ibid.
35. A regime can be 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". See Stephen D. Krasner (ed.), 1983, *International Regimes*, Ithaca, NY, Cornell University Press, p. 2.