SWITZERLAND

Towards an International Regime for the Protection of Cyberspace?

Myriam Dunn, CIIP Research Group, Center for Security Studies
ETH Zurich (Swiss Federal Institute of Technology), Switzerland

Like other security issues, the vulnerability of modern societies caused by dependency on a spectrum of highly interdependent information systems has global origins and implications. To begin with, a variety of malicious actors in the cyber environment are willing to contravene national legal frameworks and hide in the relative anonymity of cyberspace. Further, the information infrastructure transcends territorial boundaries so that information assets vital to the national security and the essential functioning of the economy of one state may reside outside its sphere of influence on the territory of other nation-states. Additionally, cyberspace - a huge, tangled, diverse, and literally universal blanket of electronic interchange - exists everywhere where there are telephone wires, cables, computers, or electromagnetic waves, a fact that severely curtails the ability of states to regulate or control it alone. Any adequate protection policy extending to strategically important information infrastructures will thus ultimately require transnational solutions, such as an international regulatory regime for the protection of cyberspace.

Regulatory regimes[1] emerge from the mediation of disparate interests of various stakeholders within arenas of political interaction. The outcome of these interactions usually takes the form of new rules, which are created by constraining actors' choices and pre-scribing who can act when, and affect behavior both directly and indirectly. But even though the need for such an international regime in the area of information security or critical information infrastructure protection (CIIP) is evident, there are at least two problems delaying its emergence.

First, CIIP is an issue of high relevance to many different, very diverse, and often over-lapping communities. These different groups - be they private, public, or a mixture of both - do not often agree on what needs to be protected with what means. In addition, turf battles within governments are frequent; only in a few countries have central governmental organizations been created to deal specifically with CIIP issues. Often, responsibility is given to well-established governmental organizations or agencies that appear suitable for the task.[2] Depending on their key assignment, these agencies bring their own perspective to bear on the problem and shape policy outcomes accordingly.

As a result of both points, the difference in the scope and quality of national CIIP policies is considerable. CIIP policies in various countries are at various stages of imple-mentation - some are enforced, while others are just a set of suggestions - and come in various shapes, ranging from a regulatory policy focus concerned with the smooth and routine operation of infrastructures and questions such as privacy or standards, to the inclusion of CIIP into more general counterterrorism efforts. This divergence of national CIIP policies is 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.

Second, there exists a paradoxical desire of many NATO states to both exploit and restrict attacks against the information infrastructure simultaneously. Under the broad heading of "Information Operations" they seek to integrate attacks against the information infrastructure of a foreign state into routine

(*Continued, Page 11*)

Dunn (*Cont. from Page 10*) military planning as a tool of strategic coercion, while at the same time, they take a range of actions, both unilaterally and multilaterally, to mitigate the risks resulting from the dependency of their own militaries, governments, economies, and societies on networked information systems.

The problem with these military ideas for the strategic use of cyberspace is that they fail to recognize the nature of the (emerging) interdependent network environment, which will likely be characterized by ubiquitous computing and networking - and thus even greater interdependencies. This fact makes it unlikely that computer attacks can ever be a tool for precise targeting of enemy infrastructures or a means to deliver effectively to a particular geographic conflict zone. In fact, not only could military use of computer attacks directly "blowback" on Western societies through the network interdependencies; routine use of computer attacks would also likely result in a more intangible side effect: the undermining of trust in cyberspace with long-term effects on the global economy. This basically means that the investments in military technologies and doctrines designed to disrupt the infrastructures of rival nations seem like a comparative strategic advantage only at a first glance: A closer look will reveal that these benefits are considerably flawed by misperceptions of the emerging technical environment and the nature of the international system in the information age in general.[3]

The problems outlined above are two main factors slowing down the emergence of norms for the protection of cyberspace. However, in the light of economic and security interests, industrialized states would be well-informed to work towards overcoming these temporary obstacles and move resolutely towards robust international conventions and mechanisms that protect the global information environment.

[1] 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 interna-tional relations". See: Krasner, Stephen D. (ed.). International Regimes. (Ithaca: Cornell University Press, 1984): p. 2.

[2] Dunn, Myriam and Isabelle Wigert. The International CIIP Handbook 2004: An Inventory of Protection Policies. (Zurich: Center for Security Studies, 2004).

[3] 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, Volume 7 (2001): pp. 121-144 ❖

Sweden (*Cont. from Page 8*) a robust peacetime society is still valuable. Especially with regard to the cooperation that took place within the Total Defence framework. Most Swedish adults were involved in Total Defence in some way. Redundancy and reserve systems were incorporated into important infrastructure systems such as the electricity supply, telecommunications, water supplies, data systems, etc.

A Total Defence system though had to be a planned system, as most defence forces. The challenge now is to build a Risk Management based system with short OODA (observe, orient, decide, act) decision loops. New threats, risks and vulnerabilities must be addressed in time. This demands new methods and changing the mind sets of those used to the old Total Defence concept, while not losing the lessons learned in cooperation and CIP.

SWEDISH EMERGENCY MANAGEMENT AGENCY

Sweden's security policy situation has now undergone a fundamental change. The country, itself an EU member, is surrounded by democratic states that are members of the EU, NATO or both. Russia does not constitute a military threat to Sweden.
Our world has become more secure but less predictable. History has not ended; international terrorism and organized crime constitute the new threats. Open borders, interconnected infrastructure systems and the rapid expansion of electronic information services create new vulnerabilities. The challenges can only be solved by co-operation: nationally, within the EU and in other international fora. The transatlantic cooperation is an import part of successful CIP.

For more information:
www.krisberedskapsmyndigheten.se and www.isn.ethz.ch/crn ❖