Canadian Centre
For Foreign Policy
Development

Centre canadien
pour le développement
de la politique étrangère

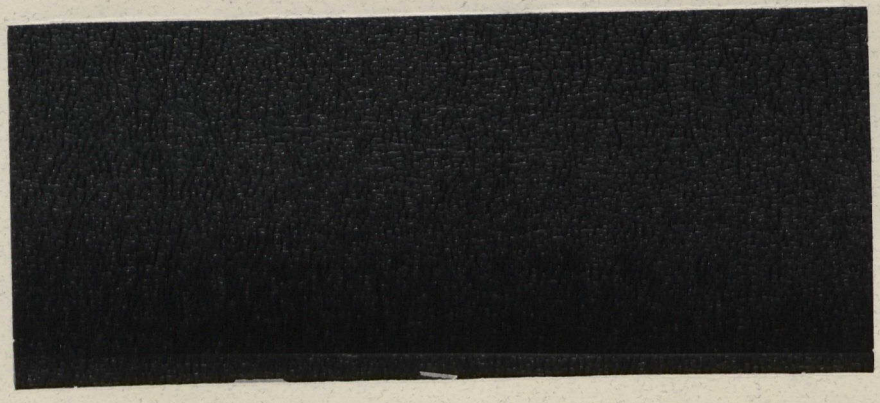
SECURITY IN THE INTERNET ENVIRONMENT: ISSUES FOR CANADIAN FOREIGN POLICY

-A report-

July 1998

Ronald J. Deibert
University of Toronto

125 promenade Sussex Drive, Ottawa, Ontario K1A 0G2
Telephone/Téléphone : **613 944 8278** Fax/Télécopieur : **613 944 0687**
www.cfp-pec.gc.ca

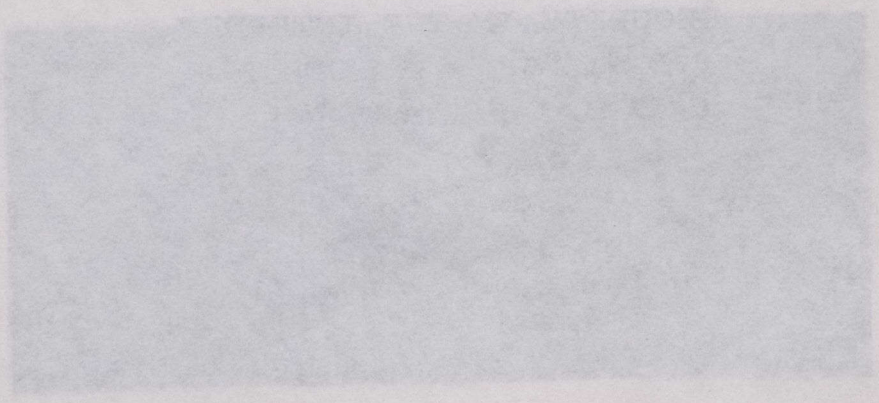


SECURITY IN THE INTERNET ENVIRONMENT: ISSUES FOR CANADIAN FOREIGN POLICY

-A report-

July 1998

Ronald J. Deibert
University of Toronto



Security in the Internet Environment: Issues for Canadian Foreign Policy
July 1998
Ronald Deibert
University of Toronto

The paper examines the linkages between security, the internet, and Canadian foreign policy. It argues that the linkages can be assessed against four frameworks: national, state, privacy, and network. Each framework emphasises its own referent or object to be secured and the policy responses to achieve security. Although the paper recognises the difficulty in determining which framework predominates and, therefore, how Canada's information and security policy should be consequently formulated, it concludes that network security will become increasingly relevant in the long-term and that policy responses which include firewalls, virus-protection software, prevention of illegal penetration of computer systems, development and distribution of highly sophisticated encryption technologies, systems of secure access, will be increasingly necessary. Thus, while internet security is a valid concept within the framework of network security, it is important to recognise that there is no single set of threats or policy prescriptions, and, therefore, no single or simple solution to threats to internet security.

Table of Contents

Security in the Internet Environment:

Issues for Canadian Foreign Policy[1]

Ronald J. Deibert

Assistant Professor

Department of Political Science

University of Toronto

July 1998

In 1995, the United States Central Intelligence Agency and Department of Defense issued a joint press release noting that "The security of information systems and networks is *the major security challenge* of this decade and possibly the next century." Given the pantheon of both old and new security threats – from nuclear weapons to environmental degradation – such a pronouncement was of no minor significance. Indeed, in a very short time the Internet has acquired a rather ominous association, one that invokes images of anonymous "hackers" and "crackers", nebulous transnational criminals and money-launderers, cyber-terrorists, pornographers and pedophiles. At the root of this more ominous association is the belief – articulated in an increasingly large volume of popular and academic literatures -- that as societies become more dependent on networked information infrastructures, they also become more vulnerable to potential electronic catastrophe, either through accident or malicious intent. These new problems

[1] Thanks to Philip Howard, Andrew Price-Smith, Trevor Fleck, and Eugene Shmeilen for research assistance on this report.

of "security" in the context of Internet communications -- and their relevance to Canadian security in particular -- are the focus of this paper.

As many have commented, "security" is a loaded term that activates a powerful set of interconnected symbols and ideas. To be thrust into the realm of security, an issue takes on the imprimatur of utmost importance; the division between the "high" politics of military-security affairs and the "low" politics of economics reflects this importance. More specifically, the notion evokes a specific set of responses characterized by what Paul Chilton calls "metaphors of containment" -- that is, state surveillance of, and territorial defense from, "external" or "outside" forces.[2] A residue of the Westphalian war-system -- where states have been the primary aggregations of political power with territorial encroachment from other states in the system constituting the primary "threat" -- "security" has been traditionally conjoined with policies of fortification, balancing, and a "hardening" of the "outer shell" of the state.[3] It is because of these associations, and recent policy initiatives by governments in China, Singapore, Germany, and elsewhere, that many foresee a coming government "clampdown" on the Internet.

Yet a quick glance at some of the ways "security" is being used in conjunction with the Internet, and the actual policy responses developed by states and non-state actors, reveals a more complex picture. Certainly the steps taken by the Chinese

[2] Paul Chilton, Security Metaphors: Cold War Discourse from Containment to Common House, (New York: Peter Lang, 1995); Hans J. Morgenthau, Politics Among Nations: The Struggle for Power and Peace, Fifth Edition. (New York: Alfred Knopf, 1973).
[3] John Herz, "Rise and Demise of the Territorial States," World Politics 9 (July 1957), pp: 473-493.

government to build a great "Firewall" fall in step with the expectations outlined above (whether or not they ultimately prove successful), as do attempts by sectors of the U.S. government to limit the spread of enhanced encryption technologies. But out of step with these expectations are ideas concerning networked communications and computer security in areas such as Internet commerce or corporate communications. Rather than building walls and clamping down on the Internet, here the emphasis is on devising policies and protocols to further *accelerate* transnational communication flows. In this sense, "security" is employed with reference to insuring the validity of purchase transactions, detecting network viruses, and preventing system "crashes" -- measures designed to *free up*, rather than clamp down on the further development of a global information infrastructure.

Is the Internet a "security threat?" If so, to whom is it a threat and in what ways? More specifically, should Canada perceive the Internet as a security threat, and if so, which of the security notions and policy options alluded to above should the Canadian government adopt? What are the consequences of adopting one as opposed to another?

A conventional approach to these questions would take the form of analyzing the unique properties of the Internet to assess whether it constitutes a threat to the Canadian state, in the same way that a physician might analyze an emerging virus to assess its threat to the health of a human being. Yet as the examples above suggest, the matter is more complicated than a conventional approach such as this can accommodate. First, the

referent of security -- unlike the physical structure of a human being -- is a variable bundle of competing values, rather than a fixed unit. While a body is a body is a body, a state is not simply a state like every other state. A state is a system of governance -- an institution that expresses and protects a set or bundle of principles and values. Moreover, these principles and values are contested. What from the perspective of value-bundle *A* appears as a "threat" would from the perspective of value-bundle *B* or *C* appear as benign. A virus in one case is nourishment in another. Complicating matters further is the related issue of what might be called "linguistic variability." Although terms and concepts certainly carry connotational baggage that activate specific responses, as the associations surrounding the notion of security listed above suggest, they nonetheless can be co-opted, altered, and transformed over time. Because language is an intersubjective expression, meanings of concepts can vary depending on their use in specific historical and cultural contexts. The specific policy responses activated by and associated with the term "security" can conceivably shift over time, in other words. To stretch the analogy further, it is as if the specific bodily reactions associated with a dose of an anti-bacterial agent varied depending on who received them and when.

If a conventional diagnosis of the questions listed above is lacking, where do we turn? A first cut at answering these questions is suggested by several perspectives falling within the rubric of so-called "critical" studies of security.[4] Although diverse in focus

[4] See Keith Krause and Michael Williams, (eds.) Critical Security Studies, (Minneapolis: University of Minnesota Press, 1996); Ronnie Liphshutz, (ed.) On Security, (New York: Columbia University Press, 1995); Jef Huysmans, "Security! What Do You Mean? From Concept to Thick Signafier," European Journal of International Relations, (Vol. 4, No.2, 1998), pp. 226-255; and Michael C. Williams, "Identity

and theoretical perspective, together these studies provide two basic analytical points that make them especially attractive to this study. First, they emphasize the "historicity" of notions of security -- that is, that "security" is not a notion that is fixed and transparent, but something produced in history and changes over time.[5] Second, they underscore the *constitutive* nature of "collective images" of security.[6] Ideas and theories of what constitute a security "threat," in other words, promote and reproduce a particular type of world order by implicitly or explicitly privileging a particular set of policy responses, and an object or referent that is to be secured. Assessments of whether some issue or actor is a security threat, in other words, always presuppose an object that requires securing and a type of political order that is valued. Although the latter has traditionally centered on the nation-state, it need not necessarily be so, and can conceivably encompass other actors or objects in the future.

These two points have important consequences for how a study such as this should be approached. Rather than analyze the Internet itself as a possible threat to Canadian security, the focus must broaden to compare and contrast alternative "paradigms" of the Internet and security as a whole. As alluded to above, and will be

---

and the Politics of Security," European Journal of International Relations, (Vol. 4, No.2, 1998), pp. 204-255.

[5] As Krause and Williams put it, "To understand security from a broader perspective means to look at the ways in which the objects to be secured, the perceptions of threats to them, and the available means of securing them (both intellectual and material) have shifted over time." Keith Krause and Michael Williams, "From Strategy to Security," in Krause and Williams, (eds.) Critical Security Studies, p. 49.

[6] "Collective Images" is a term I borrow from Robert Cox. He defines "collective images" as "differing views as to both the nature and legitimacy of prevailing power relations, the meanings of justice and public good, and so forth. Whereas intersubjective meanings are broadly common throughout a particular historical structure and constitute the common ground of social discourse (including conflict), collective images may be several and opposed. The clash of rival collective images provides evidence of the potential

shown in more detail below, there are several different senses in which the notion of "security" is being employed in the context of the Internet today, each with radically different -- in some respects, diametrically opposed -- normative and political consequences. The answer to the question of whether or not, or in which way, the Internet is a "threat" to "Canadian security" will thus depend on which of these alternative paradigms is adopted. Seeing the Internet as a "security threat" from perspective *A*, in other words, may work at cross-purposes with perspectives *B* and *C* and so forth. A proper diagnosis must begin with a comparative analysis of the collective images themselves; what constitutes the "disease" in each case will vary.

The paper will proceed in the following way: First, I will review the notion of "security" in the context of world politics, emphasizing its variability and contingency. I will then examine four collective images of security in the Internet environment: national security, state security, private security, and network security. Lastly, I will conclude with some observations about which of these collective images will likely predominate, and what the consequences of that predominance will mean for Canadian and world politics. It is hoped that through this analysis a much broader perspective can be put forth with which to formulate Canadian information and security policy.

---

for alternative paths of development..." Robert Cox, "Social Forces, States, and World Orders," in Robert Keohane, (ed.) NeoRealism and Its Critics, (New York: Columbia University Press, 1986), pp. 218-219.

I. The Changing Scope and Theory of "Security"

What does the term "security" summon forth? In the sphere of world politics, It evokes weighty issues involving the highest levels of state concern. To attract attention on the state security radar screen is to be placed within a grid of paramount significance. It is for this reason that so many today see it as a concept with such discursive power. To speak of an issue in the language of security is to boost its significance into the realm of "high" politics -- into concerns about war, peace, and survival.

Beyond having the imprimatur of weightiness, however, security in world politics tends to imply a specific focus on one particular actor: the state. When one speaks of security in world politics the concept is usually assumed to refer to the state, and not some other social group or actor. Indeed, the cases for exceptions involving *human* security, *common* security, *planetary* security, or *ecological* security stand out as challenges precisely because they seek to move beyond the assumption of security as the security of the state and the state alone.[7] The explicit reference to some other object of security differentiates these as exceptions to the rule.

Lastly, the notion of security tends to elicit images of war, inter-state military rivalry, guns, bombs, missiles, and corporeal violence. Those within the state who deal with issues of "national security" are not concerned with all those issues that may be

categorized as weighty or of utmost importance, but only those of a particular type: those concerning issues of war and peace. Hence, the high correlation between those who deal with issues of security and the involvement of defense and military organizations and personnel. Hence also the traditional focus of security "studies" within the international relations field on questions of war and military strategy.[8] If the primary referent of security has traditionally been the state, the primary threat to that security has been of a military nature emanating from other states in the international system.

What is noteworthy about the preceding discussion is that so much of that which is associated with the term security operates on the level of shared assumptions. For many, security is taken for granted. To be sure, there are disagreements as to the precise threats at any one time, what responses should be taken to different threats, and the trade-offs between national security and other values. But operating below these disagreements is a set of shared assumptions -- an intersubjective agreement -- about the primary referent of security (the state), the primary threat to security (war), and the relative importance of security in the ranking of state values (high).

Although these tripartite assumptions might seem like common sense today, it is important to remember that they are historical constructs whose meanings have varied over time. A clear illustration can be found simply by examining some of the many

---

[7] See, for example, Richard Ullman, "Redefining Security," International Security, (Vol. 8, No. 1, 1983), pp. 129-153; and Jessica Tuchman Mathews, "Redefining Security," Foreign Affairs, (Vol. 68, No. 2, Spring 1989), pp. 162-177.

different senses in which the term has been employed in the past. In Leviathan, for example, Thomas Hobbes provides perhaps the clearest statement of the familiar ranking of security in the hierarchy of values as fundamental and logically prior to all others:

> Whatsoever therefore is consequent to a time of war, where every man is enemy to every man, the same consequent to the time wherein men live without other security than what their own strength and their own invention shall furnish them withal. In such condition there is no place for industry, because the fruit thereof is uncertain: and consequently no culture of the earth; no navigation, nor use of the commodities that may be imported by sea; no commodious building; no instruments of moving and removing such things as require much force; no knowledge of the face of the earth; no account of time; no arts; no letters; no society; and which is worst of all, continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short.[9]

For Hobbes, writing as a spectator of the English civil war, the absence of security correlated with the condition of war and violent death. Yet in this account, early in the modern period, the referent object of security was not the state but the "individual." The state, or Leviathan, was seen as a vehicle to that end and not an object of security itself.

---

[8] See Stephen Walt, "The Renaissance of Security Studies," International Studies Quarterly, 35 (1991), pp. 211-39.

In the opening pages, for example, Hobbes speaks of the state as an institution *designed* primarily for *salus populi*, or "the people's safety." Later, in speaking of the social contract among individuals, he notes that "the motive and end for which this renouncing and transferring of right is introduced is nothing else but the security of a man's person, in his life, and in the means of so preserving life as not to be weary of it." The idea that the state itself should be proper object of security was not yet in Hobbes' time fully entrenched. Here, security is a primary value, protection from war and corporeal violence its intent; yet the primary referent is not yet the state, but the individual.

In Edmund Burke's writings on the French Revolution some one and a half centuries later, we find in some passages the referent of security to be the state but the primary threat to it conceived as not war *per se*, but the demise of "opinion" upon which the European monarchical states-system is legitimated:

> The policy of this general doctrine, so qualified, is evident enough. The propagators of this political gospel are in hopes that their abstract principle (their principle that a popular choice is necessary to the legal existence of the sovereign magistracy) would be overlooked, whilst the king of Great Britain was not affected by it. In the meantime the ears of their congregations would be gradually habituated to it, as if it were a first principle admitted without dispute. For the present it would only operate as a theory, pickled in the preserving juices of pulpit eloquence, and laid by for future use. *Condo et compono quae mox depromere*

[9] Thomas Hobbes, Leviathon, Edited by Michael Oakeshott, (New York: Collier Books, 1962).

possim. By this policy, whilst our government is soothed with a reservation in its favor, to which it has no claim, the security which it has in common with all governments, so far as opinion is security, is taken away.[10]

In other passages, however, the primary referent of security is not the state but the liberty of the individual from the arbitary power of the state itself:

> The people of England will not ape the fashions they have never tried, nor go back to those which they have found mischievous on trial. They look upon the legal hereditary succession of their crown as among their rights, not as among their wrongs; as a benefit, not as a grievance; as a security for their liberty, not as a badge of servitude.[11]

If the notion of security has such historical variability, when and how did its more familiar associations outlined above take root? It is only in the twentieth century, with the professionalization of the International Relations field and the framing of a predominant discourse, that these associations began to gel. Prior to World War II, the prevailing concern in the study of security was with the prevention of war between states -- a reflection of the massive destruction and loss of life of World War I. The references to "security" in Quincy Wright's magisterial A Study of War, for example, emphasize its collective dimension in such institutions as the "balance of power," "diplomacy," and

---

[10] Edmund Burke, Reflections on the Revolution in France, (New York: Dolphin Books, 1961).
[11] *Ibid.*

"sovereignty."[12] "For Wright," David Baldwin notes, "war was primarily a problem to be solved, a disease to be cured, rather than an instrument of statecraft."[13] After World War II, and particularly with the onset of the Cold War, the focus shifted away from collective prevention towards the logistics of war as a tool of national policy. Analyses narrowed, in other words, in the direction of the strategic dimensions of national security.

This narrowing was intensified by three convergent factors: the development and recognition of the awesome destructive power of nuclear weapons, the predominance of the neo-realist paradigm, and the diffusion of the positivist method in the study of international relations. The first heightened concern over the relative influence of weapons deployments, force structures, and issues of command and control.[14] The second made the theoretical case for the predominance of the state as a unitary rational actor seeking survival above all other values.[15] And the third focused analysis on measurable, empirical phenomena, as opposed to normative concerns underpinning security as a political value. The state as the object of security, war as the primary threat, and its priority ranking in the hierarchy of values all faded into the background as shared assumptions with attention now centered on the logistics of war. That these biased dovetailed with U.S. threat perceptions at a time when the International Relations field

---

[12] Qunicy Wright, A Study of War, (Chicago: the University of Chicago Press, 1942).
[13] David Baldwin, "Security Studies and the End of the Cold War," World Politics 48 (October 1995), pp. 117-41.
[14] See, for example, Glenn Snyder, Deterrence and Defense: Toward a Theory of National Security, (Princeton: Princeton University Press, 1961).
[15] See, for example, Kenneth Waltz, Theory of International Politics, (New York: Random House, 1979).

was dominated by Americans should not come as any surprise.[16] The end of the Cold War, the emergence of several new "non-traditional" threats, and the entry into the International Relations field of a larger "international" contingent of theorists, has cracked open the security paradigm. Today, neither the referent, the threat, nor the appropriate responses to them can be safely assumed.

What this brief digression should reveal is the rather obvious malleability of the notion of security. The term has no fixed meaning, no concrete referent that fixes it permanently in time and space. Like all concepts, it floats and stretches; it shrinks and narrows. It undergoes metamorphosis depending on the social and historical context in which it is deployed. Of course, there are limitations to this variability, mostly having to do with the constraints of shared opinions and the accumulation of habits. I cannot alone craft a radically alternative definition of security and hope to have it change peoples' outlooks in an instant. Concepts become firmly entrenched and deeply embedded in social practices. They develop a referential "stickiness" that makes them resistant to change.[17] During these times, much of the ambiguity surrounding a term such as "security" drops out of the picture, and analysis can focus on the relatively technical process of comparing and contrasting alternative "threats" in relation to it.

---

[16] Kalevi J. Holsti, The Dividing Discipline: Hegemony and Diversity in International Relations Theory, (Boston: Allen and Unwin, 1985).

[17] For discussion in the context of International Relations theory, see Ronald J. Deibert, "Exorcismus Theoriae: Pragmatism, Metaphors, and the Return of the Medieval in IR Theory," European Journal of International Relations, (Vol. 3, No. 2, June 1997), pp. 167-192.

But -- as shown above -- concepts do indeed mutate over time, particularly in moments of institutional change. In times such as these, the intersubjective agreements that sustain prevailing conceptions break down and multiple, competing referents, threats, and policy options emerge, circulate, and compete for attention and predominance. Shared assumptions become unglued; everything is up for grabs. Moreover, the various collective images that circulate are all potentially *constitutive* forces, in the sense that adopting one or the other of them has important political -- as opposed to simply strategic -- ramifications. By narrowing in on a particular referent and particular threats, they implicitly or explicitly favour a specific set of policy responses and thus a particular type of political system. In Hobbes' worldview, the solution to the security *problematique* is the collective deference among the population to a single, overarching public authority -- the Leviathon. For Burke, it is the restraint of radically unchecked republican opinions. Today, it is one of several different competing approaches each with subsequently different political consequences.

A critical approach to the question of whether the Internet is a security "threat" must, then, focus on these alternative collective images as a whole. It must highlight their differing threat perceptions, policy prescriptions, objects or referents of security, and type of political or "world order" promoted. The following section employs this framework to investigate four different collective images of security in the Internet environment.

III. Collective Images of Security in the Internet Environment

The Internet phenomenon is well known, even if its characteristics and social and political implications are not fully understood. Several histories have been written about its origins in the United States military-industrial complex, and the unique architectural principles out of which it has evolved.[18] Its rapid growth and increasing penetration into society -- facilitated by cheaper and easier-to-use technological developments -- is now well established with more in store for the future. Such growth and penetration have capped a century or more of radical and fundamental changes in communication technologies, which have re-shaped nearly every aspect of society, economics, and politics on a global scale.[19] At the end of the twentieth century, we live in a hypermedia environment of planetary digital-electronic-telecommunications.

Amidst this new environment, new communities are forming, while others are being undermined. Bundles of interests and values are coalescing and competing with each other, re-defining the boundaries of power and authority on a global scale. Circulating through these bundles of interests and values are several collective images of how "security" is being challenged and/or transformed in the Internet environment. A vast literature has been spawned that extends across several economic, political and

---

[18] See especially, Jeffrey Hart, Robert R. Reed and Francois Bar, "The Building of the Internet," Telecommunications Policy, (November 1992), 666-689; Martin Campbell-Kelly and William Aspry, Computer: A History of the Information Machine, (New York: Basic Books, 1996); and Katie Hafner and Matthew Lyon, Where Wizards Stay Up Late: The Origins of the Internet, (New York: Simon and Schuster, 1996).

[19] For an attempted comprehensive overview, see Manuel Castells, The Information Age: Society, Economy, and Culture Vols. I,II, and III. (Oxford: Blackwell, 1996).

military spheres. Overlapping in some areas, while colliding in others, the ideas that inform the Internet-security problematic present rival perspectives on the nature and legitimacy of prevailing power relations, and the meanings of justice, public good, and order.[20] This swarm of collective images is the site out of which the contours of future Internet development and world order will be shaped.

To help disentangle these competing collective images, an analytical template or framework derived from "critical" approaches to security is particularly helpful. This framework includes the following questions:

(1) In what ways is the Internet seen as presenting a security "threat"?

(2) Who or what is presumed to be the object of security in this regard?

(3) What specific policy measures are deemed necessary in response to that threat?

(4) What type of world order is promoted and (re)produced by #'s 1, 2, and 3, above?

Four "collective images" will be assessed using this interpretive framework: national security; state security; private security; and network security. It should be emphasized that these collective images are "ideal-types" and not rigid divisions actually existing in practice. States hold positions and elites makes statements that fuse together elements of all four. Additionally, there are potential compatibilities between each of them. As ideal-

[20] Cox, "Social Forces, States, and World Order," pp. 218-219.

types, however, they help focus analysis on differences, tensions, and contradictions between dominant collective images of security circulating today in the Internet environment. More importantly, they provide a clear framework with which to assess Canadian options for security policies in the Internet environment.

A. *National* Security

The historical relationship between the formation of national identities and communication technologies is well known. As theorists ranging from Harold Innis and Marshall McLuhan to Benedict Anderson have observed, the development of mass printing technologies in western Europe was critical in freezing linguistic drift and cementing collective identities around shared vernacular languages.[21] Further developments in mass media, such as radio and television, amplified collective cohesion through centralized broadcasting. The integration of mass broadcasting technologies with state interventionist policies over content thus resulted in a hyper-modern fusion of *nation* and *state*. It is for these reasons that throughout the twentieth century such a high premium has been placed, both theoretically and in practice, on state control over mass media as a pillar of political development. Among totalitarian regimes such controls are absolutely enforced and rigidly applied. But even among the most benignly liberal-democratic states, "public" broadcasting has been widely perceived as a state responsibility to cultivate, nurture, and preserve a shared *national* view of the world.

[21] For Anderson, see Imagined Communities: Reflections on the Origins and Spread of Nationalism, (London: Verso, 1983).

The emergence of the Internet as an alternative paradigm of communications presents technological challenges to the maintenance of this historical relationship. Although nations are widely perceived by those who identify with them as deeply entrenched, there is a realization that their vitality is nonetheless contingent on a variety of political protections in the communications field. Language laws in Quebec, television and radio content regulations in Canada, film and video regulations in France and Iran, the outright banning of television in Afghanistan by the fundamentalist Taliban, all attest to the perception that national identity and communication technologies are closely intertwined.[22] As new modes of communication have emerged that are based on principles other than the mass broadcasting paradigm these types of protections and regulations have increased. Protecting culture and identity has become a critical concern for states as globalization has become more intense.

To date, the major challenge confronted by these regulations has been the proliferation of television and radio channels and the accompanying globalization of the sources of content. While it is debatable whether or not these regulations have been effective, it is almost certain that they will not in the networked world of the Internet. To understand why this is so, consider content regulations. The Canadian broadcasting act requires private television licensees to achieve a yearly Canadian content level of at least 60% overall, measured over the broadcast day, and 50% between 6 p.m. and midnight.

[22] Ironically, the same fundamentalist Taliban has its own website, at http://www.taliban.com/index.html. There, one can read why "[p]rohibition of TV, VCR was essential to save the society from destruction."

(As the national broadcaster, the CBC must ensure that at least 60% of its program schedule consists of Canadian productions.) Such a system of regulations can be enforced because the channels through which broadcasters operate are a scarce resource requiring government allotment and licensing. If a broadcaster defied the content regulations, the broadcasting license could be revoked and the broadcaster would be unable to reach the audience.

In the Internet environment, however, there is no scarce resource equivalent to the broadcasting spectrum requiring allocation of channels. Channels are potentially limitless. Moreover, the audience comes to the "broadcaster" rather than the other way around. And "broadcasters" (meaning website owners) are located around the world, rather than within the jurisdiction of Canada. To extend television content regulations into the Internet environment would thus require a transformation of the Canadian state into a planetary totalitarian regime -- a remote possibility, however desirable the outcome might be for some.

In the meantime, however, the intent of the regulations are gradually undermined since anyone connected to the Internet can watch whatever television broadcasts are made available over the World-Wide Web. Today, the technology is relatively primitive, though vastly superior to what was available just a year or two ago. Dozens of sites offer choppy "realvideo" broadcasts that range from BBC and CNN news to pornography. It is not unrealistic to assume that current trends will continue to the point where thousands of

quality-produced "television" programs from around the world are made available over the World-Wide Web, though obviously varying in content and sophistication. Radio broadcasts are following a parallel trajectory. Should the "integration" of media continue to the point that the Web subsumes television and radio entirely (a realistic prospect), the point of continuing broadcasting regulations would seem negligible. The public broadcaster would be but a whisper in an arena of screams.

From the perspective of this collective image, then, the primary "threat" that the Internet poses is its potential undermining of collective national identities. The primary object of security is presumed to be "the nation" -- the imagined community of people who share a distinct language or ethnicity. Of the four collective images under study here, this collective image is the one with the least visible support. Several countries (or ministries and departments within these countries), such as Canada, France, Iran, Iraq, Germany, Vietnam, China, Syria, and Myanmar have made official pronouncements that showed a sense of concern about threats to cultural identity in the Internet environment.[23] With some, such as Canada and France for example, the sense of concern seems clearly centered on national and cultural identity as traditionally understood. In others, however,

[23] See "Syria's on Net, and on Guard," Wired News (10 July 1998). A spokesman for the Syrian Computer Society said that "Our problem is that we are a traditional society and we have to know if there is something that cannot fit with our society." Ta Ba Hung, Vietnamese Minister of Science, Technology, and Environment, said that "information flow might affect badly the cultural identity of the nation." See Keith B. Richburg, "Future Shock: Surfing the Net in 'Nam," Washington Post, (November 19, 1995). For Iran, see Neil MacFarquhar, "With Mixed Feelings, Iran Tiptoes to the Internet," New York Times, October 8, 1996). For an excellent overview of communications regulation in Canada in the interests of protecting cultural sovereignty, see Marc Raboy, "Cultural Sovereignty, Public Participation, and Democratization of the Public Sphere: The Canadian Debate on the New Information Infrastructure." Paper delivered to the National and International Initiatives for Information Infrastructure symposium, January 25-27, 1996, Harvard University, Cambridge Mass, USA.

notably China, Vietnam, Iraq, Iran, Syria, and Myanmar, the concern with national and cultural identity is difficult to disentangle from a concern with *state* or *regime* security, a collective image that will be dealt with in the next section and one that should be kept distinct. Despite the ambiguity of these cases, it is clear that there is a constituency across several countries that views the Internet as a potential threat to cultural security.

The specific policy responses that are forming around this collective image have varied from country to country. Among liberal-democratic states, such as Canada and France, for example, there is a principled reluctance to censor or block out communications with the rest of the world.[24] An important exception is the willingness to censor communications that violate norms of "decency," a measure that has been attempted over the Internet with uneven success by the United States, Germany, and others.[25] Apart from censoring indecent communications, the primary policy response appears to be active state *support* to ensure a "national voice" has a "presence" on the Internet. For example, the Canadian Heritage Ministry states as its goal to "increase the creation, production and distribution of high quality Canadian content in both official languages to sustain a strong Canadian presence in conventional and new media."[26] This has and supposedly will entail capital investment in Canadian media and entertainment

---

[24] For a good overview of Canadian communications policy with special reference to the Internet, see Eli Turk and David Johnston, "Competitiveness, Access, and Canadian Content: The Three Pillars of Canadian Internet Policy." (Paper delivered to the Impact of the Internet on Communications Policy conference, December 3-5, 1997, Harvard University, Cambridge, Massachusetts, USA. Found online at: http://ksgwww.harvard.edu/iip/iicompol/Papers/Johnston.html

[25] See David Hudson, "Germany's Internet Angst," Wired News (11 June 1998); Stephen Labaton, "Computer Stings Gain Favor as Arrests for Smut Increase," New York Times, September 16, 1995).

[26] See Strengthening and Celebrating Canada for the New Millennium, Canadian Heritage Portfolio -- Overview of Priorities, (Canadian Heritage, 1998).

industries and the extension of the Internet into more Canadian communities. Along similar lines is *PaddyNet*, a World-Wide Web site dedicated to the dissemination of Irish voices and perspectives.[27] Numerous other similar examples could be cited as well.[28] The intent of these policies appears to be to provide the nation with financial and technological life-support systems so that it will survive into the Internet environment.

A second policy response among liberal-democratic regimes has been tentative steps towards forming "cultural alliances" in order to build up widespread support for regulations and protections of culture in trade regime negotiations. For example, in July 1998, cultural ministers from several countries (with the notable exception of the United States) met to discuss strategies to form an international alliance of cultural ministries, and have plans to meet in subsequent years as well.[29] Here, the efforts are directed in a more conventional way towards building regulatory fences to control communication flows. The cultural alliances are the novel aspect, though one whose prospects appear dim in the face of more powerful alliances oriented in precisely the opposite direction. Opening the market for trade in "cultural products" has been the focus of several recent trade negotiations and a major concern of United States' trade policy.

Found online at http://www.pch.gc.ca/mindep/misc/millenium/e-9.html

[27] www.paddynet.com

[28] See, for example, "France's Chirac Pledges Computer, Literacy Drive," CNN Online, (March 10, 1997); "French Launch Cyberspace War Against English," London Times, (April 14, 1997); and Victoria Shannon, "Online Via the French Connection: It Takes a Global Village," Washington Post, (June 16, 1997).

[29] See "Culture Forum Eyes CNN Rival," The Toronto Star, (July 1, 1998). The cultural ministers also discussed plans to create a global news organization to rival CNN.

Among more authoritarian and conservative regimes, on the other hand, the policy responses veer much more towards the censoring end of the spectrum with, in some cases, complete isolation and containment of the population from exposure to the Internet. Iraq, for example, has banned access to the Internet, calling it a tool of American imperialism.[30] In Myanmar, not only is the Internet outlawed but mere possession of a computer laptop is a criminal offence punishable with a 15 year sentence.[31] Other states have taken a similar route, believing that the best way to protect cultural identity from the Internet environment is to isolate the cultural group altogether from it. To repeat, it is difficult to determine with certainty whether such a strategy is more a mechanism for *state* or *regime* survival or genuine concern with national and cultural identity. But the policy responses are, nonetheless, identical in each case.

In sum, the national security collective image portrays the Internet as a potential security threat to collective identities, with the nation or culture perceived to be the primary object of security. While this collective security image certainly does not dominate the landscape on Internet politics, it has colored the perspectives of several government ministries and countries around the world. The policy options pursued as a function of this collective image have ranged from complete isolation and containment to active state intervention and promotion of national expression on the Internet. The world order promoted by this collective image is a relatively insular system of *nation*-states.

---

[30] "Iraq: Internet Yet Another Tool of American Domination," CNN Online (February 17, 1997).

B. State Security

While the national security collective image may not dominate the world political landscape, one that is gaining significantly more exposure is characterized by a traditional concern with threats to the power and authority of the state apparatus. Particularly in the United States, though having echoes that reach across the world, concerns have been raised about the potential use of the Internet for strategic-military purposes. These concerns are embedded in a highly elaborate debate within miltary-intelligence circles -- again, based primarily in the United States -- about the changing nature of warfare, although the latter issue has far greater scope in terms of topics covered.[32] A second major related concern is the loss of state power and authority because of the unique properties of the Internet, particularly the widespread use of encryption technologies. While this collective image thus has several inter-related dimensions, each perceives the object of security to be the state, defined broadly to include the government and the total territorial space, infrastructure, resources, and people under its control.

The first dimension of this collective image sees the Internet as a potentially new medium of warfare in which states are actively planning to operate. Several studies, primarily within the United States security community, have suggested states are actively

---

[31] See Joshua Gordon, "East Asian Censors Want to Net the Internet," Christian Science Monitor, (November 12, 1996).

[32] For sample discussions, see John Arquilla and David Ronfeldt, "Cyberwar is Coming!," Comparative Strategy, (Vol. 12, 1993), pp. 141-165; and "The Future of Warfare," The Economist, (March 8th, 1997).

engaged in military preparations for Internet warfare. In a recent report to the U.S. Senate the director of the CIA, George Tenet, said that China, Russia, and other states have undertaken "extraordinary" steps to develop an Internet warfare capability.[33] It is difficult to determine the veracity of these reports, however, since heightened and distorted threat construction is a common practice within U.S. military-intelligence circles. What is clear is that the United States itself is actively engaged in such preparations, having gone to great lengths to ensure they receive widespread media exposure.[34] Given the extent of financial, commercial, and other interdependencies between states, however, the prospects of two large states actually assaulting each other in full-blown "electronic warfare" seem remote. Scenarios involving stock exchanges being targeted by *states* with sophisticated electronic tools of warfare fail to account for the "blowback" that would be unleashed on the initiating state itself, as the ripple effects of recent financial crises in Asia demonstrate. More realistic, perhaps, would be sporadic low-level electronic disruptions undertaken by so-called "rogue" states, terrorists, and other non-state actors.

Indeed, numerous and increasing incidents of the latter sort have contributed the most fuel to the rise of this collective image. The most sensational (but least severe) of them have involved the de-facing of webpages, including those of NASA, the CIA, and

---

[33] See "A Prelude to InfoWar," Reuters (24 June 1998).
[34] See James Der Derian, "Global Swarming, Virtual Security, and Bosnia," The Washington Quarterly, (Vol. 19, No. 3, 1996), pp. 45-56; and Douglas Waller, "Onward Cyber Soldiers," Time (August 21, 1995), pp. 30-38.

various government and corporation sites around the world.[35] More consequential and disruptive have been the attacks on electronic infrastructures, the spread of viruses, the delivery of malicious coding, and the theft or destruction of data by underground computing groups known as "hackers" and "crackers". Again, precise estimates are difficult to come by because of the nature of the issue-area. Both corporations and state agencies are generally reluctant to report incidences of computer intrusions because of the possible loss of confidence in their capabilities. But the episodes that have been reported suggest a growing trend, with increasing recognition among government officials of their potential severity.[36]

In February 1998, for example, the U.S. Defense Department reported that it had been the object of a concerted hacker offensive, which turned out to be three teenagers: two Americans and one Israeli. The latter, going under the codename "Analyzer," claimed that he had access to 400 Department of Defense computers, though officials maintained no sensitive information was compromised or destroyed.[37] In 1997, a Swedish hacker jammed the 911 emergency phone system in west-central Florida.[38]

---

[35] "NASA Web Site Briefly Closed Due To Hackers," CNN Online, (March 7, 1997).

[36] Jacques Gansler, the U.S. undersecretary of defense for accquisition and technology, said that teenage crackers pose a "real threat environment" to national security. See Wayne Madsen, "Teens a Threat, Pentagon Says," Wired News (2 June 1998). See "Pentagon Reports Cyberattack," Wired News (25 February 1998);

[37] See James Glave, "Hacker Raises Stakes in DOD Attacks," Wired News (4 March 1998). The teen, Ehud Tenebaum, was eventually arrested by Israeli National Police for "illegally accessing computers belonging to the Israeli and United States governments, as well as hundreds of other commercial and educational institutions in the United States and elsewhere."

[38] Robert Trigaux, "Crackers -- the bad apples among hackers -- find government and business easy prey." Toronto Star, (4 July 1998).

Numerous other episodes could be cited as well.[39] In all, the General Accounting Office reported that the U.S. Department of Defense experienced as many as 250,000 hacker attacks in 1995 alone.[40] An indication that such isolated incidences could conceivably become better organized with a clear political agenda was the theft and destruction of Indian nuclear-related information from the Bhabha Atomic Research Centre by anti-war computer hackers in July 1998.[41] The perception is that while such instances have been mostly undertaken by thrill-seeking computer experts still in their teenage years, there is a real possibility that the attacks could become better organized and funded and directed towards a clear political agenda. Moreover, the scope and scale of the attacks could increase, with major infrastructures -- such as stock exchanges, telecommunications systems, air traffic control networks, and other vital conduits -- being targeted and crashed causing massive disruptions.

Apart from direct threats to physical infrastructures, a second related dimension of this collective image is the possible loss of state power and authority. Contributing to this perception is the spread of various anonymizing technologies -- and in particular publicly distributed encryption software -- that undermine the law enforcement and intelligence capabilities of states. The encryption issue is complex, deeply contested, and

---

[39] As this paper is being written, yet another hacker incident occurred, this time of the U.S. Coast Guard computer systems by a disgruntled officer. See Laura DiDio, ""U.S. Coast Guard Beefs Up Security After Hack," CNN Online (July 22, 1998), http://cnn.com/TECH/computing/9807/22/coastguard.idg/index.html

[40] Trigaux, "Crackers."

[41] See James Glave, "Crackers: We Stole Nuke Data," Wired News (3 June 1998). http://www.wired.com/news/news/technology/story/12717.html

involves high stakes for several major societal interests.[42] Traditionally, states have monopolized and tightly controlled sophisticated encryption technologies for law enforcement and intelligence purposes. Their relatively greater pools of capital and computing expertise ensured the maintenance of technological superiority over individuals and other private actors.

Gradually, however, developments in computing technologies have led to the widespread availability of increasingly sophisticated encryption systems, many of which are shared freely over the Internet. Fueling this development has been a demand among large corporations and businesses driven, in part, by the need to ensure the privacy of their communications vis-à-vis each other, and, in part, by a desire to unleash commerce over the Internet -- a topic that will be taken up in more detail below.[43] Today, encryption systems are available over the Internet that are practically impossible to break even for states with access to the most powerful supercomputers.[44] For law enforcement and intelligence officials, such developments pose a fundamental challenge to traditional levers of power, particularly various forms of information surveillance, such as signals

---

[42] For an excellent overview, see Diana Saco, "Colonizing Cyberspace: 'National Security' and the Internet," (book chapter, get proper citation).

[43] Corporate spying is a major factor in the private development of encryption technologies. For discussion, see Adam L. Penenberg, "Corporate Spies," Forbes Digital Tool, (04.03.98), online at: http://www.forbes.com/asp/redir.asp?/tool/html/98/apr/0403/feat.htm

[44] "In July 1997, it took 78,000 volunteered computers on the Internet 96 days to crack a message encrypted with DES (the Data Encryption Standard), a secret key algorithm that uses a 56-bit key. It is estimated that it would take the same computer resources 67 years to crack a secret key algorithm using a 64-bit key and well over 13 billion times that age of the universe to crack a 128-bit key." Government of Canada, A Cryptography Policy Framework for Electronic Commerce, Task Force on Electronic Commerce, Industry Canada, (February 1998).

intelligence (SIGNIT). More broadly, they also present problems for the enforcement of a variety of state regulations that, in turn, could facilitate organized crime and fraud.[45]

These concerns in the encryption arena are simply one element of a broader threat the Internet poses to state power. For example, the control of information flows in and out of states for ideological reasons, such as that undertaken by China, Singapore, Iran, and others, becomes increasingly difficult. Once connected to the Internet, it is almost impossible to prevent from a central node access to information that is available over the wider network. According to Froomkin, "[s]hort of cutting off international telephone service or concluding an international agreement with all industrialized countries to discontinue telephone service with foreign countries that harbor remailers, there is little that one can do keep out messages from any other country, or indeed to keep citizens from sending messages wherever they like."[46] Not surprisingly dissident groups within and outside these countries have organized on the Internet providing access to politically outlawed publications and material and reporting violations of human rights.[47] Even among liberal-democratic states, similar sentiments have been raised about the potential broad-based loss of state control over the political agenda to non-state actors.[48]

---

[45] For an overview, see Vic Sussman, "Policing Cyberspace," U.S. News and World Report, (January 23, 1995); M.B. Gayle, "Virtual Chaos," Washington Times, (May 8, 1995); Pat Cooper, "Organized Crime Hackers Jeopardize Security of U.S." Defense News, (October 3, 1994); Michelle Celarier, "What a Tangled Web," Euromoney, (October 1996).

[46] Froomkin, "The Internet as a Source of Regulatory Arbitrage."

[47] See, for example, Michael Clough, "Cyberspace: Why Nations Could Fear the Internet," Los Angeles Times, (February 4, 1996); Michael White, "Now We're Watching Big Brother," The Guardian, (August 3, 1996); Gregory Katz, "Zapatistas," The Dallas Morning News, (March 12, 1995); and Faiza S. Ambah, "Dissidents Tap the 'Net' to Nettle Arab Sheikdom," Christian Science Monitor, (August 24, 1995).

[48] A particularly illuminating illustration in this respect are the views on anonymous re-mailers contained in Paul A. Strassman and William Marlow, "Risk-Free Access Into the Global Information Infrastructure Via

The policy responses associated with this collective image have varied widely. In response to the possibility of attacks on electronic infrastructures, the United States has taken the lead in focusing on studies, organizational adaptations, and counter-measures.[49] One of the most visible of these was the creation in 1996 of the President's Commission on Critical Infrastructure Protection to assess vulnerabilities and threats to critical infrastructures across all government agencies.[50] Additionally, all of the armed forces have engaged in wide-ranging studies and, in some cases, operational changes to meet the challenges of information and electronic warfare.[51] Numerous other non-governmental and quasi-public organizations have emerged in the computer and information security area, though their existence bridges at least two of the collective images under scrutiny here (state and network security). Although no other state has gone to the lengths of the United States in this area, other major powers, such as Russia, China, Japan, Great Britain, and France, have followed a similar, albeit scaled-down, course.

Anonymous Re-Mailers." Paper delivered to the Symposium on the Global Information Infrastructure: Information, Policy, and International Initiatives, January 28-30, 1996, Harvard University, Cambridge Mass, USA. See also Charles Swett, "Strategic Assessment: the Internet," Office of the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict (Policy Planning), 17 July 1995.

[49] See the report, "Information Security -- Computer Attacks on Department of Defense Pose Increasing Risks," Government Accounting Office, (May 1996) for an early study and recommendations.

[50] See the website for the PCCIP at http://www.pccip.gov/. Its first major report, entitled Critical Foundations (1997), provided a glimpse of some of the conceptual difficulties that surround adopting traditional notions of security in the new Internet environment, particularly the blurred distinctions between military, civilian, domestic, and foreign infrastructures. The report stated that "[f]ormulas that carefully divide responsibility between foreign defense and domestic law enforcement no longer apply as clearly as they used to. "'With the existing rules, you may have to solve the crime before you can decide who has the authority to investigate it.'" For reactions to the report, see Chris Oakes, "A New Crypto Furor," Wired News (7 November 1997).

[51] See "Security Team Finds Pentagon Computers Unsecured," CNN Online (April 16, 1998) for details on counter-intelligence efforts at the Pentagon and elsewhere.

In response to the loss of state power and authority -- the second dimension of this collective image -- the policy measures undertaken have varied as well depending on the state concerned. In the United States and among most other liberal-democratic states, concern has focused on controlling the unlimited spread of encryption technologies that do no permit access for law enforcement.[52] The formula that has been adopted with little success to date has been the push for so-called "key-escrow" encryption software as the industry standard -- a measure that has been vigorously resisted by businesses and privacy advocates alike. Although the specifics of various proposals differ, all key-escrow systems allow "back door" access for states to encrypted documents and data. States have also begun to take tentative steps to collaborate internationally on encryption policies under the auspices of the Organization for Economic Cooperation and Development, the G7 forums, and elsewhere.[53]

Among non-liberal democratic states, the policy responses have varied depending on the state's interest in global commerce. For those who do, policy responses have been characterized by a precarious balancing-act that reveals the contradictions of promoting connections to global information infrastructures for economic reasons while maintaining political controls over the flow of information.[54] Singapore, for example, characterizes

---

[52] See the report Cryptography's Role in Securing the Information Society, Computer Science and Telecommunications Board, National Research Council, National Academy Press, 1996 for a detailed overview. See also, "German Minister Demands Keys to Unlock Internet Codes," CNN Online (April 28, 1997);

[53] See the report OECD, Cryptography Policy: The Guideliness and the Issues, (1997) available online at http://www.oecd.org/dsti/sti/it/secur/prod/GD97-204.htm. See also the report of the OECD Emerging Market Economy Forum: Workshop on Cryptography Policy, (Paris 9-10 December 1997), available online at http://www.oecd.org/dsti/sti/it/secur/act/emef.htm

[54] See Leslie Helm, "Asia Wary of Being Wired," Los Angeles Times, (February 3, 1996).

itself as an "intelligent island" and prides itself on having one of the deepest penetrations of information technologies in society. Yet it also attempts to maintain vigorous controls over access to certain types of information.[55] In the Internet environment, such controls have taken the form of strong restrictions on Internet service providers, and punishment and fines for those who are caught violating them. Certain websites, listserves, and newsgroups are also blocked out though it is unclear with what effectiveness. China has responded by attempting to minimize the access points, or "nodes," to the global Internet -- in effect, creating a national "intra-net" or what some have termed "the Great Firewall."[56] Chinese authorities have also passed sweeping regulations similar to those in Singapore against computer hacking, viruses, the leaking of state secrets, and the spread of "harmful information" over the Internet.[57] In announcing the regulations, the Assistant Minister for Public Security, Zhu Entao, said that the Internet "has...brought about some security problems, including manufacturing and publicizing harmful information, as well as leaking state secrets" and that the regulations were necessary to "safeguard national security and social stability."[58] Whether or not these types of responses will be technologically effective is, of course, a separate matter. Among non-liberal democratic states not so concerned with global commerce, on the other hand, the response has been

---

[55] For a good overview, see Froomkin, "The Internet as a Source of Regulatory Arbitrage"; See also Darren McDermott, "Singapore Unveils Sweeping Measures To Control Words, Images on Internet," Wall Street Journal, (March 6, 1996).

[56] See Rone Tempest, "China Puts Roadblocks on Information Superhighway," Los Angeles Times, (September 6, 1996); Steven Mufson, "Chinese Protest Finds a Path On the Internet," The Washington Post, (September 17, 1996); Angela Li, "Complete Control of Internent 'Unlikely'" South China Morning Post, (January 11, 1997); and Philip Shenon, "2-Edged Sword: Asian Regimes on the Internet," New York Times, (May 29, 1995).

[57] "China Issues New Net Controls," Wired News (30 December 1997).

[58] *Ibid.*

much more simply formulated. In Myanmar, Iraq, Syria, and elsewhere, access to the Internet is either strictly forbidden altogether or very tightly controlled.

In sum, from the perspective of this collective image the primary "threat" of the Internet is the way that it facilitates new non-traditional forms of warfare and violence, particularly from non-state actors and terrorists. A related threat is the potential loss of state control over information flows in and out of the country. The primary object of security is the territorial state or government. Policy responses have ranged from attempts to create territorial "firewalls" that funnel Internet communications through official nodes (China) to coercive pressures on Internet Service Providers and citizens to restrict their access and distribution of information (Singapore) to the promotion of "key escrow" encryption technologies (United States). The world order promoted by this collective image is a system of sovereign *states*.

C. Private Security

The concern with safeguarding privacy has been an integral component of modern liberal thought and practice since at least the 19th century, though obviously having important intellectual and social precursors prior to that time. Its basic thrust has been directed towards the protection of the private sphere from what are perceived as the potentially oppressive public forces of state bureaucracies and mass democracy. The concern with privacy is, perhaps, most visible in the United States experience, with its

provisions for individual rights and numerous check and balances against government power. However, it is a concern that is reflected in all liberal-democratic states around the world and is generally considered a fundamental human right.

Although perceived threats to privacy are nothing new, advocates around the world have argued that new information and communication technologies, including the Internet, have raised the stakes considerably. Information about individuals, which at one time might have had to be manually gathered, filed, and stored, can now be digitized and shared among massive computer databases. Moreover, as more and more aspects of society and economy are folded into the hypermedia environment, an increasing amount of personal information is folded in as well. As Lyon puts it, "In numerous ways what was once thought of as the exception has become the rule, as highly specialized agencies use increasingly sophisticated means of routinely personal data, making us all targets of monitoring, and possibly objects of suspicion."[59]

Today, transaction patterns, periodical subscriptions, health and education records, loan and credit card data, and other types of information help create an electronic profile of individuals that is then shared among businesses and government ministries.[60] Such information can then be combined with aerial and space-based surveillance imagery to create sophisticated topographical maps, called geographic information systems, that

[59] David Lyon, The Electronic Eye: The Rise of Surveillance Society, (Minneapolis: University of Minnesota Press, 1994), p. 4.
[60] For a detailed overview, see Lyon, The Electronic Eye; and Oscar Gandy Jr. The Panoptic Sort: A Political Economy of Personal Information (Boulder: Westview Press, 1993).

provide electronic profiles of entire neighborhoods on such topics as disease, crime, income levels, and other factors.[61] Many companies offer such services directly over the Internet.[62] On the Internet, personal information, such as email addresses and surfing histories, can be captured from surfers by computer programs located in websites, which is then used to generate electronic mailing lists for advertising purposes or to alter site advertisements to match consumer profiles.[63] Coupled with the widespread use of more dispersed centers of surveillance, such as security, hand-held video, and web cams, the image that emerges is of a dense electronic cage in which individuals are totally enmeshed and their lives completely transparent.[64] No wonder, then, that Jeremy Bentham's eighteenth century design for an all-seeing prison, called the Panopticon, has struck such a resonant chord with so many adherents to this collective image.[65]

The proponents of this collective image include both state and non-state actors alike. Among many liberal-democratic states, privacy commissioners or ministries have been created that have, in turn, constructed laws and regulations to protect privacy. Probably the most elaborate of these is the European Data Protection Directive, which

---

[61] David Martin, Geographic Information Systems and their Socioeconomic Applications, (London: Routledge Press, 1991).

[62] See, for example, Analytical Surveys Incorporated, at http://www.anlt.com/. The description of the services is as follows: This innovative and rapidly growing company uses a variety of advanced technologies to convert paper-based maps, aerial photography, tax records and other "geo-referenced" information into a digital format. Once in a computerized form, the information can be combined in layers to form a geographic information system (GIS), or "intelligent map." A GIS is a powerful and flexible analytical tool that is easily accessed, analyzed and updated by users in a broad range of decision making processes.

[63] See Denise Caruso, "As Privacy Grows Scarcer on the Internet," New York Times, (June 3, 1996); and Pete Slover, "Cyber Crumbs: Do Internet Cookies Leave a Trail That Could Threaten Your Privacy?" The Salt Lake Tribune, (Friday, July 31, 1998).

[64] See Lili Berko, "Surveying the Surveilled: Video, Space, and Subjectivity," Quarterly Review of Film and Video, (Vol. 14, Nos. 1-2, 1992), pp. 61-91.

will go into effect in October 1998.[66] The Directive creates a bundle of rights and protections for privacy that include stringent measures against personal information trade with companies or countries outside of Europe that do not abide by the conditions of the privacy regime. Some countries, like China for example, have no privacy regulations whatsoever, while others, like the United States, have only minimal ones. Many expect the EU Directive to cost corporations billions of dollars in lost business or additional costs to meet the requirements of the regime.

In addition to official privacy commissioners, several high-profile non-state actors orbit around the privacy issue as advocates. Numerous transnational non-governmental organizations have emerged that share and publicize information and lobby governments and corporations, including Privacy International, the Electronic Frontier Foundation, the Electronic Privacy Information Center, and the Global Internet Liberty Campaign, among many others. These groups act as large umbrella networks for the numerous other smaller and more specialized interest groups who share a concern with privacy in the Internet environment. The latter range from groups committed to human rights to cyber-libertarians and anarchists. Indeed, a strong anti-authority/anti-state streak still looms large in the Internet culture, particularly among many of those influential in the early evolution of the Internet.

---

[65] Gandy, The Panoptic Sort.
[66] See Simon Davies, "Europe to U.S.: No Privacy, No Trade," Wired News, (May 1998).

Apart from the official privacy regulations alluded to above, the common policy element that unites electronic privacy advocates is for the complete de-regulation of encryption technologies -- a move that pits them directly against state law enforcement and intelligence agencies. In what appears to be a paradoxical position, electronic privacy advocates lobby hard against any government attempts to regulate encryption even while arguing that "the genie is out of the bottle" and that the Internet, by its very nature, is immune to state regulation. Nonetheless, the numerous and detailed webpages maintained by these groups have provided a highly visible touchstone in the ongoing encryption battles. The formal and informal coordination among these groups -- as in the very prominent "blue ribbon" campaign for Internet free speech -- is impressive and suggests a formidable collection of interest groups. Other technologies that preserve the privacy of Internet surfing, such as anonymous remailers and browsers and various software shields, are also developed and advocated by these groups.

In sum, from this collective image the "threat" posed by the Internet and other information technologies is the potential invasion of privacy by states and corporations. The primary object of security is the individual. The policy responses emerging out of this collective image include strict privacy regulations and rules that protect personal data and place strictures against how such data can be used as well as total de-regulation of encryption technologies. The world order promoted by this collective image is a system of liberal states constituted on the basis of strong human rights' and individual privacy protections.

D. Network Security

One of the more novel perspectives of security emerging in the Internet environment arises out of the increasing importance of networked information technologies for all aspects of post-industrial economics, including transnational production and global finance. Recent changes in information technologies, including the Internet, are inextricably bound up with, and have contributed to, fundamental changes in the nature of economic organization, from the structure of individual firms to the location of production to the movement and character of money and finances.[67] As this penetration has increased, and as more and more aspects of society become dependent on networked information infrastructures, a new image of security is emerging that focuses on protecting the networks themselves from systems "crash," loss, theft, or corruption of data, and the disruption of information flows.

This network security image has two related dimensions. The first centers on protecting the integrity of data and the flow of information internal to specific businesses and corporations. As corporate restructuring has evolved away from hierarchical organizational structures and fixed locations towards adaptable networks and multi-locational flexibility (a development itself fundamentally bound up with new information technologies), ensuring the rapid and reliable flow of information, as well as the integrity of such flows, has become fundamentally important. Although many corporations

regularly lease their own private networks, called "intranets," to ensure the speed and reliability of their data flows, there is increasing pressure to integrate internal networks to the wider Internet.[68] Securing the flows has thus become a major concern, particularly as the number of network "attacks" has increased.[69] Firewalls, virus-protection software, logging and real-time alarm systems, and various forms of encryption and smart card authentication systems have been vigorously developed and applied by corporations.[70] With reliable encryption packages, for example, "virtual private networks" (VPNs) can be developed which deliver data around the globe using public networks instead of expensive leased lines.[71] To give one example, the General Electric Corp. plans to have, by 2000, "all 12 of its business units purchasing its non-production and maintenance, repair and operations materials … via the Internet, for a total of $5 billion."[72] To help service these needs, a market for network security has exploded. Site Patrol International Services, for example, provides corporations not only with the relevant firewall and

---

[67] Part of the shift in corporate strategies has been the adoption of collaborative, networked business models. See Manual Castells, The Information Age: Economy, Society, and Culture, Vol. 1, The Rise of the Network Society, (Oxford: Blackwell Publishers, 1996), particularly chapters three and four.

[68] See David Greenfield, "Global Intranet Services: Patchy But Promising," Data Communications, (March 21, 1997).

[69] More than half the network managers at 205 Fortune 1,000 companies say they have detected attempted break-ins during the past 12 months. Nearly 60 percent of those who know they have been hacked admit to 10 or more break-ins during the same period. "Security," Data Communications, (August 1997), p. 175.

[70] For various examples, see the following: Lee Bruno, "Plugging Security Holes," Data Communications, (February 1998), pp. 29-32; Lee Bruno, "Firewall Protection Without the Pitfalls," Data Communications, (March 1997), pp. 31-32; Rodney Thayer, "Bulletproof IP," Data Communications, (November 21, 1997), pp. 60; Charles Cresson Wood, "Logging, Auditing and Filtering for Internet Electronic Commerce," Computer Fraud and Security, (August 1997), pp. 16..

[71] See "Security," Data Communications, (August 1997), p. 176; and Joyce Harvey, "The VPN Puzzle," America's Networks, (April 1, 1998), pp. 43-47. See also, Tina Bird, "Building VPNs: the 10-Point Plan," Data Communications, (June 1998), pp. 123-132. Bird notes that VPNs can be up to 80 percent cheaper than private leased lines.

[72] Cited in United States Department of Commerce report, "The Emerging Digital Economy," (April 1998), found online at: http://www.ecommerce.gov/emerging.htm

encryption systems but real-time 24-hour network monitoring to track incidences, identify potential security breaches, and provide rapid responses as well.[73]

The second dimension of this image centers on securing flows of information between producers and consumers, a concern that is at the heart of ongoing attempts to commercialize the World-Wide Web but is bound up with broader changes in the marketplace towards informatization. Almost all banks, for example, have invested in and promoted electronic access for customers.[74] Partly justified for "customer convenience" and competitive pressures, but no doubt related also to the potential downsizing benefits as well, most every banking transaction can be done either through electronic tellers, over the telephone, or through computer access with software packages supplied by the banks themselves. Each step, however, has necessitated an increasing investment in security protocols that includes not just software and hardware (modem pools, compact discs, leased lines, secure servers, access control mechanisms, etc), but computer security consultants as well.[75] The widespread use of smartcards, stored value-devices, and other

---

[73] See the Site Patrol International Services website at http://www.bbnplanet.com/products/security/sitepat.htm

[74] Illustrating the financial depth and global scope of such activities, ScotiaBank Inc. of Canada is an international financial institution with $200 billion in assets that services 4 million customers in 50 countries. See Lee Bruno, "Banking on Trust," Data Communications (May 21, 1998): 43-49 for an overview of its extensive network security provisions.

[75] In its transition to electronic access services, ScotiaBank Inc. hired a team of "ethical hackers" who worked from a remote site in Palo Alto, California that staged a multi-pronged computer attack on the mainframe, operating systems, and Web servers. See Bruno, "Banking on Trust," p. 45. For 48 hours of hacking, the price: $35,000.00. The total cost of ScotiaBank Inc.'s deployment of electronic access services was $2,007,000.00. The market for network security products and services was projected to grow by 70% in 1997. See Charles Cresson Wood, "Status of the Internet Electronic Commerce Security Market," Computer Fraud and Security, (September 1997), p. 8. See also J.H.P. Eloff and Suzi van Buuran, "Framework for Evaluating Security Protocols in a Banking Environment," Computer Fraud and Security, (January 1998), pp. 15-19; Laura DiDio, "Private-key Nets Unlock E-Commerce," Computerworld, (March 16, 1998), pp. 49-50.

digital credit systems for consumer transactions and other services around the world have also entailed attention to network security protocols and mechanisms as well.[76]

This convergence of commercialization pressures and new information technologies in both dimensions has created a vortex of interest on the Internet. The pressures and expectations surrounding the commercialization of the Internet and World-Wide Web have been large. Predictions have been made for several years about an enormous market for Internet commerce emerging, ones that so far have not been fully reached.[77] The main stumbling block has been precisely the lack of security for transactions. Consumers have been generally reluctant to use their credit cards over the Internet thus stifling the growth of Web commerce. To improve security and unleash the dream of "friction-free" commerce, massive investments have been made in encryption technologies and electronic payment schemes. Several electronic cash systems have emerged, such as Digicash, First Virtual Holdings, NetCash, and Cybercash, although

---

[76] See Alan Laird, "Smartcards -- Is Britain Smart Enough?" Computer Fraud and Security, February 1997), pp. 11-15; Ivars Peterson, "Power Cracking of Cash Card Codes," Science News, June 20, 1998). As online stock and investment transactions have become more common, security concerns have increased there as well. For one example, see Ellen Messmer, "Investment Firm Buys Into Public-Key Encryption," Network World, (May 4, 1998), pp. 57-60. See also Sharon Machlis and Jana Sanchex-klein, "Will Smart Cards Replace ATMS?" CNN Online, (July 30, 1998), http://www.cnn.com/TECH/computing/9807/30/homeatm.idg/.

[77] See Gordon Arnaut, "The Holy Grail of Internet Commerce," The Globe and Mail, (November 14, 1995); and Steve Lohr, "The Great Mystery of Internet Profits," New York Times, (June 17, 1996). For an overview of how businesses are using the Internet for marketing and selling products, see Marios C. Angelides, "Implementing the Internet for Business: A Global Marketing Opportunity," International Journal of Information Management, (Vol. 17, No. 6, 1997), pp. 405-419. While expectations of a market for consumer transactions have not panned out as fully as some predicted, that for business-business transactions has exploded. The United States Department of Commerce report, entitled "The Emerging Digital Economy," forecasts $300 billion in Internet commerce between businesses by the year 2002 based on current traffic trends. The report is located at http://www.ecommerce.gov/emerging.htm

they have not received widespread acceptance to date.[78] Nonethess, a marketplace on the World-Wide Web is indeed emerging, particularly in those areas -- such as financial services and software -- that lend themselves to networked communications.[79]

In each of the dimensions noted above – that is, in intra-corporate communications and corporate-customer communications -- ensuring that information networks function efficiently and without corruption is of paramount importance. The network itself is the object or referent of security. The scope of the network is largely non-territorial, though of course the policy deliberations that concern it are centered in several state jurisdictions. The "threats" to network security include a wide range of activities, including: programming errors that could lead to systems crashes or vulnerabilities; computer fraud and theft, such as the re-direction of electronic finances; disgruntled "insiders" and employees, who intentionally sabotage computer systems; loss of supporting physical infrastructure through fire, power failures, bombs, floods, etc; malicious hackers or "crackers"; industrial or corporate espionage, including the theft of product information; and malicious coding and software, such as viruses, trojan horses, and worms.[80]

---

[78] See Alasdair Murrary, "Digital Money Opens Way to Cashless Global Trading," The Times, (January 9, 1996); Neil Gross, "E-Commerce: Who Owns the Rights?" Business Week, (July 29, 1996).

[79] See Andrew Allentuck, "Financial Services That Delight, Amaze," The Globe and Mail, (November 14, 1995); and Vanessa O'Connell and E.S. Browning, "Stock Orders on Internet Poised To Soar," Wall Street Journal, (June 25, 1996). The Dell Corp was selling as much as $6 million worth of computer equipment and software each day during 1997. See the U.S. Department of Commerce report, "The Emerging Digital Economy," at http://www.ecommerce.gov/emerging.htm

[80] For an overview, see CSL-Computer Systems Laboratory Bulletin, (March 1994), found online at http://www.nsi.org/Library/Compsec/compthrt.txt

In some respects, this collective image overlaps with the state security collective image outlined earlier. As with the latter, the network security image has focused attention on preventing the illegal penetration of computer systems, the malicious use of computer viruses, and the potential disruption of major electronic-dependent infrastructures, such as stock exchanges or air traffic control systems. Like the state security collective image, this image has also contributed to the creation of a variety of governmental and non-governmental organizations devoted to safeguarding computer and information security, and the allocation of large amounts of public expenditures towards such ends. It is for these reasons that the two collective images are often intertwined in analyses of information security.

Important differences stemming from the referent of security in each case, however, warrant keeping the two collective images distinct. First, with the network security collective image the primary concern is with ensuring the integrity of information flows internal to firms and between firms and consumers. As production processes have diffused across territorial boundaries, and as capital markets become increasingly globalized, these issues have taken on a fundamentally non-territorial dimension. Salomon Brothers Inc., in other words, is concerned with safeguarding its transactions regardless of the specific jurisdictions in which those operations are located. States, on the other hand, are fundamentally concerned with ensuring the security of information infrastructures within a particular territorially delimited space, and only then as a larger function of the protection of the state itself. In some cases, networks in other

national jurisdictions might even be the *target* of disruption as part of inter-state competition.

Second, the network security image is fundamentally oriented towards reducing the friction and enhancing the velocity of information flows. The following quotation from an industry periodical shows the double concern with security *and* speed:

> In teaming up with NSTL Inc. … to evaluate six leading hardware-based VPN (virtual private network) devices, we found that all were up to the security challenge, able to fend off more than 200 types of attack. And in most cases, managing devices remotely was easy. But performance? It proved problematic, especially for links of T1 (1.544 Mbit/s) or higher. In worst-case stress testing, devices dropped anywhere from 50 percent to 85 percent of offered loads—and for applications that rely on lots of short packets (like corporate intranets), dropped packets can lead to lots of retransmissions. Say so long to savings on bandwidth.[81]

The state security image, on the other hand, is concerned with restricting, collecting, and blocking information flows, should such flows been seen as a threat to the state. The velocity of flows is either incidental, or of a subordinate concern.

[81] "VPNs: Safety First, But What About Speed?" Data Communications, (July 1998).

The differences are most strikingly apparent in the respective positions taken on encryption policies. As mentioned above, encryption touches at the heart of the state's surveillance capacity. It is for this reason that most states' intelligence and law enforcement agencies have attempted to maintain tight controls over the export of sophisticated encryption technologies. In some states, the domestic use of cryptography is tightly controlled as well.[82] Corporations, on the other hand, have come to view access to encryption as absolutely vital to ensuring network security in both senses outlined above – that is, to protect the integrity of their "intranet" flows as well as to ensure the security of transactions in the emerging electronic marketplace. It is for this reason that the giants of the corporate and computing world have invested billions of dollars in developing Internet security protocols, including encryption, and have been at the forefront of attempts to block government restrictions.

In sum, from the perspective of the network security collective image the primary "threat" of the Internet is the potential for systems "crash," loss, theft or corruption of data, and interruption of information flows. The primary object of security is *the network.* Policy responses include the development and distribution of highly sophisticated encryption technologies, systems of secure access, Virtual Private Networks, Intranets, and "digital immune systems." The world order promoted by this collective image is a system of highly-integrated "internationalized" states embedded within a dense network of transnational communication flows.

---

[82] See the exhaustive survey on state cryptography policies at the Global Internet Liberty Campaign website, http://www.gilc.org/crypto/crypto-survey.html. As the report indicates, Belarus, China, Israel,

IV. Collective Images in the Hypermedia Environment

The four collective images outlined above circulate as alternative paradigms of Internet organization and, by extension, world order. Which of the four predominates will have significant consequences for the nature of politics, authority, and community into the twenty-first century. While the analytical framework derived from a critical security studies approach helps illuminate the normative content of these collective images, and thus provides a more clear basis to formulate Canadian policy options, it does not provide any clues as to which of them will likely predominate over the others. Before concluding this analysis, it is helpful to consider some properties of the material context -- the communications environment -- in which these collective images circulate, compete, and are facilitated and constrained.

Obviously, given the considerable support that exists for each of the collective images above, we should not expect one of them to prevail fully over the others in the short-term. The institutional inertia and material interests surrounding all of these collective images ensure that none will wither immediately. Shifts in world order -- though abrupt in historical terms -- occur gradually, often spanning generations. Three elements of the communications environment, however, suggest that the network security collective image will thrive over time while national and state -- and to a somewhat lesser extent, private -- security collective images will be constrained:

Pakistan, Russia, and Singapore all maintain tight domestic controls on cryptography use.

a. *The packet-switching, non-linear architecture of the Internet environment.* One of the major constraints of the national and state security collective images is the very architecture of the Internet communications environment itself. As Froomkin notes, "The Internet is not a thing; it is the interconnection of many things--the (potential) interconnection between any of millions of computers located around the world." Each of these computers adheres to a common interconnection standard, known as TCP/IP. This standard enables the use of packet-switching, which is how information is transmitted through the Internet. In packet-switching, messages are broken up into discrete units, or "packets," that are then routed through the network and re-assembled once they reach their destination. With packet-switching technology and the distributed TCP/IP network, the data that comprise a single message take multiple independent routes to reach their destination. Hence the common description of the Internet as a "decentralized, anarchic network." The constraint that this architecture presents to the national and state security collective images is that as the network spreads and as communication flows become more dense and swift, the difficulties of filtering out or blocking particular types of information mounts. There are no single "choke-points" or nodes through which all information passes, for example. Nor is there any single route through which particular messages travel. Information is scrambled and distributed across numerous independent trajectories along the network.[83] Although it is possible for states to completely detach themselves from

[83] A U.S. National Research Council report noted: "When an interceptor moves onto the lines that carry bulk traffic, isolating the bits associated with a particular communication of interest is itself quite difficult. A high-bandwidth line (e.g., a long-haul fiber-optic cable) typically carries hundreds or thousands of different communications; any given message may be broken into distinct packets and intermingled with

the network and prevent citizen access altogether, once they opt to connect the constraints of the network for censorship and other forms of communication regulation loom large. Certainly coercion, threats, and intimidation are employed -- perhaps even successfully. From a technological perspective, however, the architecture of the Internet makes them much more difficult to enforce.

b. *Advanced Encryption Technologies*. Although the packet-switching architecture of the Internet may make it difficult to filter out or censor particular types of information, do not digital computing technologies actually *facilitate* state surveillance -- an integral part of the state security collective image? Certainly the tools of electronic surveillance available to states have grown significantly in recent years, specifically artificial intelligence programs employed in network surveillance systems, such as the American Financial Crimes Enforcement Network, or FinCEN.[84] In fact, the digital character of information and the ever-increasing computing power integral to the Internet would actually make the job of state surveillance enormously more effective were it not for a second property of the communications environment: the wide dissemination of easily accessible and highly-sophisticated encryption technologies. Once the province of state military and intelligence agencies, the mass popularity of computers and improvements in computing technologies have led to the

---

other packets from other contemporaneously operating applications. The traffic on the line may be encrypted "in bulk" by the line provider, thus providing an additional layer of protection against the interceptor. Moreover, since a message traveling from point A to point B may well be broken into packets that traverse different physical paths en route, an interceptor at any given point in between A and B may not even see all of the packets pass by." Kenneth Dam and Herbert Lin, (eds.) Cryptography's Role in Securing the Information Society, National Research Council (1996).

diffuse development of highly sophisticated public key encryption systems. Today, encryption software with keys in the 1000-bit range are freely distributed over the Internet -- a level of sophistication that would be resistant for decades to even the most advanced network of Cray supercomputers at the service of government security agencies. Although states may set regulations that prohibit the use and export of such technologies, the consensus among most is that "the genie is out of the bottle."[85] At best, prohibitions against encryption use and "key escrow" schemes are contrivances to buy time in a losing battle. The encryption properties of the communications environment clearly "favor" the privacy and network security collective images outlined above.

c. *Post-Industrial Global Capitalism.* A further boost to the network security collective image is provided by changes in the global political economy, particularly the transnationalization of production and the globalization of finance. Although the full details of the latter are beyond the scope of this paper, they are well documented elsewhere. What is of relevance, however, is that these changes have generated a large constituency of powerful interest groups who support the network security

---

[84] For an excellent analysis along these lines, see Eric Helleiner, "Electronic Money: A Challenge to the Sovereign State?" Journal of International Affairs, (Vol. 51, No. 2, Spring 1998), pp. 387-409.

[85] See "Titanic Meeting Stuck at Dock," Wired News (10 June 1998). Of the availability of complex encryption codes outside of the United States, Microsoft CEO Bill Gates said "That's a change in the world of spying and law enforcement that we cannot effect" -- meaning, precisely, that the clock cannot be turned back on encryption technologies. Likewise, the U.S. National Research Council's report, "Cryptography's Role in Securing the Information Society" concluded that " Because cryptography is an important tool for protecting information and because it is very difficult for governments to control, the committee believes that the widespread nongovernment use of cryptography in the United States and abroad is inevitable in the long run." Kenneth Dam and Herbert Lim, (eds.) Cryptography's Role in Security the Information Society. National Research Council, (1996).

collective image. Transnational corporations, particularly in the "knowledge" and financial services sectors such as banking, insurance, telecommunications, and entertainment, not only command enormous sums of wealth, but have a material interest in the development of secure global networks. As their corporate structures move further in the direction of flexible, just-in-time production arrangements dispersed across multiple national locations involving mobile and wireless communications, their dependence on the network rises in importance. This has generated not only a structural pressure on states, but a powerful constituency actively lobbying for the relaxation of encryption regulations and generating a vast market of ever-sophisticated network security products as well.[86] As more states mold their policies according to liberal-capitalist principles and in the direction of so-called "knowledge economies" (partially as a product of the structural pressures of transnational capital) the constituencies resisting or contradicting the network security collective image wither in importance and influence. Advocates of privacy, though having a largely independent set of concerns, gain in the wake created by this constituency's support of encryption technologies, though not enough on their own to override the latter's hegemony.

Although the four collective images outlined above can all be discerned across various states, the environment in which they circulate and compete is not a "level-playing field." The properties of new information and communication technologies, as well as the social

[86] See "Group of Companies to Lobby Globally on Internet Concerns," Wall Street Journal, (December 11, 1996).

and political context in which these technologies are embedded, "favour" the network security and, to a lesser extent, the private security collective images. At the same time, the national and state security collective images face formidable constraints that will likely loom larger in the future.

V. Conclusion

This analysis points to several conclusions. First, although the notion of "security" is indeed relevant to the Internet environment, there is no single set of threats, policy prescriptions, and values that are covered by the term. Indeed, quite the contrary. Rather than a unified field, the Internet-security discourse is characterized by an array of competing paradigms, some of which conflict in several important respects. For example, the diffusion and advanced development of encryption technologies is vital to the network and private security collective images, but presents a major challenge to the state and national security collective images. This suggests that there is no simple solution to the Internet-security problematic that will satisfy all constituencies with a stake in the issue. Tough choices will have to be made that will entail losses for some and gains for others. There is no clear "middle-way."

Second, this disunity suggests that those who begin to embrace the idea that "security" is a priority for Internet communications must be careful to understand fully what particular type of "security" image they have in mind. Those who endorse security for Internet commerce, in other words, may not fully understand the extent to which the full ramifications of this paradigm may undermine values that they hold dear in other areas -- for example, cultural identity or state security. This is especially significant considering that the properties of the emerging communications environment appear to favor private and network, while constraining national and state security collective

images. The "default" option for Internet security, in other words, is increasingly leaning in the direction of the network security paradigm with all of the subsequent ramifications that flow from it in other areas of politics and society. Those who embrace either the national or state collective images will face a tough uphill battle.

Lastly, this clash of values implies that there is no simple formula for determining whether and in what ways the Internet is a "security threat" because the latter is contingent on the perspectives of several competing paradigms each of which perceives the Internet, Canada, global communications, and world order from different perspectives. Ultimately, such a determination reaches well beyond the technical and political issues surrounding the Internet to the question of the nature of the Canadian polity itself. How shall we order the Canadian state? What type of political system should we promote? It is these "first-order" questions of the nature of the "good life" upon which the Internet-security problematic rests and which are too far often either ignored or assumed away as unproblematic. Until these questions are settled and made explicit, there will be no simple, straightforward diagnosis of whether and how the Internet is a "security threat."