Integrated Security: The Protection of Planetary Networks

Recommended Citation

Ronald J. Deibert, "Integrated Security: The Protection of Planetary Networks", Global Problem Solving Information Technology and Tools, December 10, 1999, https://nautilus.org/global-proble--solving/integrated-security-the-protection-of-planetary-networks-3/

Ronald J. Deibert

University of Toronto

DRAFT - Please do not quote or cite - DRAFT

Internet and International Systems: Information Technology and American Foreign Policy Decision-making Workshop

Nautilus Institute, San Francisco, December 10, 1999

Introduction

One of the most dynamic areas of international relations theory over the last two decades has been the debate about the nature and re-definition of "security." Particularly since the end of the Cold War and the dissolution of the bipolar global security structure, a variety of alternative notions of security have proliferated. Among those that have captured public and academic attention include economic security1; comprehensive security2; environmental security3; and human security4. Even more conservative state-centered theorists of security have re-considered the nature of the threats that the state now faces in the post-Cold War environment. While this debate is interesting and important, it is lacking in one very important way. Arguably the most important and consequential notion of security that has emerged in recent years is entirely invisible from these debates - the securing of flows of information through global communication networks.

A superficial probe of the issue-area suggests that something important is being overlooked. For

example, if one were to enter the term "security" on any major Internet search engine, the vast majority of matches would not refer to any of the alternative notions of security alluded to above. Nor would the more traditional state-centric ideas rise to the top of the responses. Instead, the matches would overwhelmingly pertain to the securing of electronic commercial transactions, flows of information within corporate information networks, and the defense of government and military computing and communications systems. A more detailed probe of the links would uncover websites of companies that provide network security services to corporations, governments, and others - a service industry that did not exist two decades ago but is now considered one of the fastest growing in the most dynamic sector of the economy overall. Such a development is not difficult to understand considering the extent to which information and communication technologies have become vital to just about every sector of life today, from economics to defense to culture. Yet very little is known about the world political implications of the security practices that are emerging in today's hypermedia environment.

In this paper, I examine those security practices relating primarily to the securing of transnational flows of information in the global political economy, and in particular those that have emerged in the area of transnational business information management, global financial services, and the burgeoning world of E-commerce. This set of security practices - what I will refer to as the "network security" paradigm -- is largely distinct from those relating to military "information-warfare" concerns alluded to above, though of course there are important overlaps between the two that I will examine. However, there are three main reasons to focus exclusively on the network security paradigm in this paper. First, the literature on and evolving nature of info-war state security practices is large and complex, and deserves a separate treatment in its own right - a task that others have undertaken elsewhere.5 Second, the network security paradigm is deeply bound up with possibly the most important sector driving world politics today - the global economy. E-commerce transactions alone - one vital object of the network security paradigm -- are estimated to amount to over $1 trillion by 2003.6 How information and communication flows are being secured in this sector alone will have obvious implications for world politics as a whole. Third, as will be shown below, there are important differences between network security and military and state info-war practices and ideas that suggest an important source of friction between state intelligence and defense agencies and private actors that should be highlighted. Folding the two paradigms together in one analysis would obscure, rather than illuminate, these important differences.

The paper will proceed as follows. First, I will discuss the theoretical approach and analytical lens that will be employed in this paper, derived from the emerging "critical security studies" literature.7 As I will explain below, this approach is particularly useful for analyzing new social practices in periods of transformation, such as that which characterizes the network security paradigm today. Second, I will analyze the major components of the network security paradigm, including the main threats, objects of security, policy prescriptions, and type of world order that is being promoted by this paradigm. In doing so, I will describe some of the ways that this paradigm differs from more traditional state-defense notions of information security alluded to above. To conclude, I will assess the prospects for the continued flourishing of the network security paradigm and what this flourishing may mean for the changing landscape of world politics

Theorizing Security

What does "security" mean in the context of the Internet, and new information and communication technologies generally? Can the creation of a great "Firewall" by the Chinese state, the intentions of "hacktivists" to bring down the Echelon state surveillance system, and the development of sophisticated "Digital Immune Systems" to protect currency trading networks, be reconciled all within the same paradigm?8 Is the Internet a security "threat"? Or is it the Internet itself that must

be protected or secured? A quick glance at some of these different - indeed, in some cases antithetical - approaches to security and networked technologies suggests there exists not a single consensus of ideas, but rather a maelstrom of competing collective images that need to be untangled and differentiated.9

It may be useful, then, in setting the stage for this study to make a distinction, following Robert Cox, between two different approaches to theorizing, in this case about security.10 The first type of approach is called problem-solving theory. This type of approach takes the world as it exists unproblematically, and tries to find the best way to cope within it given the resources and objectives at hand. Problem-solving theory begins with certain shared assumptions that go unquestioned about the nature of political rule and the type of order that is desirable, and then deliberates about the means or strategies that would best serve that order. It tends to be conservative, in the sense that its raison d'être is the function and maintenance of the existing system rather than some alteration to it in its core principles or a broader understanding of the system in an historical context. In the sphere of security, for example, problem-solving theory might help identify new threats, or different or more effective responses to traditional threats, while leaving unquestioned what it is, exactly, that requires protection or securing - i.e., the state.

During the Cold War, international security studies was dominated by problem-solving theory - particularly in the United States -- as illustrated by the prevalence of rationalist and game-theoretic approaches to arms control and strategic studies during the 1960s and 1970s.11 Treated pragmatically within a historical context, problem-solving theory obviously serves an important function in society. Treated uncritically, however, problem-solving theory can become rigid and ahistorical, reifying assumptions and furthering the status quo while being incognizant of important shifts in those underlying assumptions. Examples of both can be gleaned from that particular historical period.12

The second type of approach is called critical theory. Critical theory takes as its starting point that which is assumed away by problem-solving theory. It puts into focus and situates into an historical context the very presuppositions that problem-solving theory takes for granted. In doing so, critical theory underscores the historical variability of world orders, the contingencies involved in shaping them, and the possibilities that are opened up for alternative paths of development in the future. It also offers a tool to help dissect and untangle the type of new social practice that is under consideration here. It examines that social practice as a whole - from the outside-in, so to speak - rather from a perspective within that social practice whose end is the functioning and maintenance of the system, as it is in problem-solving theory.

Taking this perspective helps illuminate political questions that are typically assumed away by problem-solving theory, such as what type of world order is promoted by this set of social practices? Who benefits by them? Who loses? Or, to zero in more closely to the type of questions that are of interest here, what is to be secured, by what means, and to what end? In other words, critical theory underscores the constitutive nature of "collective images" of security. Ideas and theories of what constitute a security "threat," in other words, promote and reproduce a particular type of political system by implicitly or explicitly privileging a particular set of policy responses, and an object or referent that is to be secured. "Security" is, from this perspective, always a "social construction."

Recent contributions to the critical security studies literature have focused on a variety of different issue-areas, or new security "problematics," including ethnic conflict, environmental security, and arms control.13 While these contributions differ to some extent, they all employ a similar methodology that can be reduced to the following main framework questions:

(1) What is seen as presenting a security "threat", and by whom?

(2) Whom 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 political system or set of political values are promoted and (re)produced by #'s 1, 2, and 3, above?

These questions will be employed in this paper as an analytical lens to help illuminate the network security paradigm. As I will show below, the network security paradigm is a novel reformulation that fundamentally challenges many of the traditional notions of state security to which international relations theorists have become accustomed, including the relationship between security and public authority, territoriality, and inter-state cooperation.

Network Security

The origins of the network security paradigm can be traced back to the very first applications of digital-electronic information and communication technology to commercial and financial practices in the United States, Great Britain, and other major industrialized countries.14 As computing became more practical, and as more vital business information - such as personnel and financial accounting records - was gradually entrusted to computing systems, attention began to be paid to the methods by which such systems were to be secured from theft, corruption or unauthorized manipulation. Although encryption and other software security programs began to be developed for these purposes at this time, a great deal of the actual securing of the information relied on physical protections, such as secured entries to computing rooms and guarded buildings. Computing and information technologies were still very much within the universe of mainframe computing15, in which information remained confined within the computers that housed them, which in turn occupied a distinct, bounded space typically within a secured office complex.

All of that began to change, however, with the shift to distributed and increasingly mobile and portable forms of micro-computing and communications, a shift that has its origins in the early development of the Internet itself.16 Although these changes in the paradigm of communications percolated throughout all sectors of society, they had perhaps the most far-reaching consequences in the way that business was undertaken, and in particular in terms of the organization of production and the movement of finance. By the early 1980s, the business management literature was beginning to recognize the benefits of "networked" forms of corporate organization - a management gestalt shift away from centralized-hierarchical control that reflected the increasingly dispersed forms of production outsourcing that was occurring among major industrialized firms, particularly in high technology, financial services, and telecommunications sectors.17 As a result, computer security specialists who once had to worry primarily about fixed mainframe systems were now charged with the problem of how to secure "the Mainframe to Micro link."18 Access to mainframe computers from remote sites, primarily PCs and minicomputers, and the increasing interconnection among mini- and micro-computers, began to extend the information security architecture. No longer was it simply a matter of protecting the physical access to mainframe computers; the distributed flow of information along network systems - no matter their location -- had to be safeguarded as well.19 The shift also signaled a growing importance of information security from what was at one time a rather incidental consideration to a much more significant management priority.

We can see now that what was occurring in the early 1980s was merely the first wind of a hurricane of change 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.20 Today, not only have business practices become more dispersed along multiple and overlapping dense networks with information and networks playing a central role, perhaps more importantly, the networks themselves have become increasingly transnational -- indeed, planetary in scope. The evidence of what many see as this fundamental, epochal shift in the global economy is increasingly well known:

* Worldwide outflows of foreign direct investment (FDI) have increased nearly 29 percent a year on average since 1983, three times the growth of world exports. According to the 1999 UNCTAD World Investment Report, FDI outflows among developed countries increased by 46% alone last year to a record US $595 billion.21
* Most of this FDI is attributable to the world's 60,000 transnational corporations (TNCs), who now produce about a quarter of world economic output. Their foreign affiliates had combined sales of about US $11 trillion in 1998 compared with world exports of US $7 trillion, an indication of the size of transnational production relative to international trade.22
* As of September, 1999 the value of cross-border mergers and acquisitions - a driving force of the rise in FDI - was already 1.3 times the value of the entire previous year.23 * Daily turnover of foreign exchange transactions are now well over $1.5 trillion.24

The consequences of these transformations in the global economy for the paradigm of information security have been enormous. Rather than protecting physical access to the computers that contain information, security has now broadened and extended to encompass a planetary "network of networks" that forms the nerves or infrastructure of the global information economy. Network security thus has both a material and virtual component.25 It means protecting both the networks themselves from physical destruction (e.g., trunk lines, satellites, receivers, etc) as well as the integrated flow of digital information from systems "crash," theft, disruption, and/or corruption. As this network now, by its very nature, extends around the planet in a dense web of distributed digital-electronic-telecommunications, the relationship between "security" and "territory" within the virtual component of the network security paradigm is almost entirely absent.

There are two related objects of security in the network security paradigm. The first centers on protecting the integrity of data and the flow of information within and among corporations. As corporate restructuring has evolved away from hierarchical organizational structures and fixed locations towards adaptable networks and multi-locational flexibility, ensuring the rapid and reliable flow of information, as well as the integrity of such flows, has become fundamentally important. Such concerns are particularly important given the extent to which the number of network "attacks" experienced by corporations has increased in recent years.26 One strategy to secure these flows has been for corporations to lease their own private networks from telecommunications providers, called "intranets".27 Detached from public Internet traffic, intranets provide considerable protection for information flows, but they are not completely invulnerable to attack. So the intranets are, in turn, protected by a variety of technologies, such as firewalls, digital immune systems, virus-protection software, logging and real-time alarms, and various forms of encryption and smart card authentication systems.28

Although many corporations still regularly lease private networks, the costs are enormous. As a consequence, there is increasing pressure to integrate "internal" corporate networks to the wider Internet, a pressure that has given rise to what are known as "Virtual Private Networks" (VPNs). Using sophisticated encryption and firewall technologies, VPNs provide a way for corporations to "tunnel" through and send data around the globe using public networks instead of expensive leased lines. 29 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."30 To help service these needs, a market for network security has exploded. The worldwide market for such services and products was estimated to reach nearly $7 billion by 2001.31 Site Patrol International Services, for example, provides corporations not only with the relevant firewall and encryption systems but real-time 24-hour network monitoring to track incidences, identify potential security breaches, and provide rapid responses as well.32

The second dimension of this image centers on securing flows of information between producers and

consumers (including business-to-business transactions), 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.33 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.34 The widespread use of smartcards, stored value-devices, and other digital credit systems for consumer transactions and other services around the world have also entailed attention to network security protocols and mechanisms as well.35

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.36 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 they have not received widespread acceptance to date.37 Nonethess, a marketplace on the World-Wide Web is indeed arising, particularly in those areas -- such as financial services and software -- that lend themselves to networked communications.38

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, and the information that flows through it, 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.39

The Politics of Network Security

It is important to be clear that the network security paradigm described above, as with all paradigms, is more of an ideal-type than a rigid set of concrete practices. Although discernable as a social force, in practice actors make statements and adopt policies that at times correspond to the network security paradigm while at other times corresponding with other, perhaps competing paradigms. As outlined at the beginning of this paper, such as the confused situation of the Internet-security problematique that under the rubric of security conflicting policies can be adopted and promoted without appreciation of the contradictions in underlying principles.

One such potent contradiction exists between the network security paradigm and the security practices of state intelligence and military organizations -- what we might call the "state-defense" collective image. Organizations such as the Central Intelligence Agency, the National Security

Agency, and the Federal Bureau of Investigations in the United States, or the Communications Security Establishment and the Canadian Security and Intelligence Service in Canada, (to name a few), all have very strong views on the relationship between new information technologies and security. In some respects, this state-defense collective image overlaps with the network security paradigm. As with the latter, the state-defense collective 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. The colossal public attention generated around the so-called "millennium bug" or "Y2K" issue, for example, is an area of direct overlap between the two. Like the network security paradigm, 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 paradigms distinct. First, with the network security paradigm 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' intelligence and defense agencies, 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.

Such differences have important practical and political consequences. Because those actors who operate in the network security paradigm are concerned with securing the flows of information through non-territorial spaces -- indeed, through numerous state (and non-state, in the case of outer space) jurisdictions -- the task of providing security for these actors cannot be entrusted to a single state authority. Even more prohibitive is the fact that since the end of the Cold War, many state intelligence agencies have ranked economic and industrial espionage high on their lists of priorities. Transnational corporations have to be concerned about industrial espionage not only from private competitors, but from state agencies acting in alliance with their nationally-based competitors as well. For both of these reasons, the task of providing network security -- especially with respect to securing information flows -- has increasingly been charged to private actors.

Second, the network security paradigm 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.40

The state-defense 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. In some cases, the volume and velocity of flows presents a

formidable threat in and of itself insofar as increases in traffic make the task of information surveillance that much more difficult for state intelligence agencies.

The differences are most strikingly apparent in the respective positions taken on encryption policies. Encryption technologies touch 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.41 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 legislative restrictions.

Network Security and World Order

The overlap between the two paradigms -- particularly in the area of securing the hard physical infrastructure that supports networks within individual state jurisdictions -- is not insignificant. It suggests that there will be formidable support in many states for the allocation of public funds towards protecting information systems within individual state jurisdictions. At a minimum, in other words, both the network security and state-defense paradigms converge in the view that electronic infrastructures require securing. In spite of their overlap, however, the two images conflict in important ways that provide alternative conceptions of world order.

With its strong support for de-regulation of encryption policies, the privatization of security services, and the intensification of transnational flows of information, the world order promoted by the network security paradigm is a system of highly-integrated, "internationalized" states, especially among the Northern industrialized countries that dominate the global economy. With strong regulations against encryption and deep domestic and international electronic surveillance practices, on the other hand, the state-defense paradigm presents a much more classic "Westphalian" model of world order in which states are insulated from one another. These two paradigms are schematized in Figure 1. Which of these two paradigms will fare better in the long run is a difficult question to answer, since so many contingencies are involved, and institutional support for both is strong.

Figure 1. Network Security and State-Defense Paradigms

Paradigm Main Object of Security Relevant Institutions and Actors Perspectives on Computing and Information Public Policy Form of State Promoted Form of World Order Promoted State-Defense The state, defined broadly to include the government and the total territorial space, infrastructure, resources, and people under its control State defense, law enforcement, and intelligence agencies Strong regulations on encryption technologies; push for "key escrow" and "back-door" for law-enforcement. Strong, public interventionist national security state Classic "Westaphlian" international system Network Security The planetary "network of networks" through which information flows Large Transnational Corporations, Global Financial Services, Entertainment Industries Complete de-regulation of encryption policies; privatization of telecommunication and computer/ information security services Liberal-capitalist or republican, "transmission-belt" state Increasing integration among Northern-industrialized states; liberal-capitalist system

One way to begin to answer this question, however, is by examining the material properties of the broader communications environment in which both are embedded. Communications environments -

- defined as the material properties of communication technologies and the political and economic context in which such technologies are embedded -- facilitate and constrain social forces, collective images, and ideas. They place obstacles and constraints in the face of some paradigms, while providing intensity and dynamism to others.42 In the words of Thomas Rise-Kappen, "ideas do not float freely" but are, rather, embedded in a specific material context that either supports or constrains them. An examination of the communications environment can thus help illuminate which of the two paradigms will predominate over time and, in doing so, help to trace the changing contours of world order. Three characteristics in particular point to an expeditious environment for the network security paradigm while a constraining one for the state-defense paradigm.

a. The packet-switching, non-linear architecture of the Internet environment. One of the major constraints of the state-defense paradigm 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 state-defense paradigm 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.43 Although it is possible for states to completely detach themselves from 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-defense paradigm? 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.44 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 diffuse development of highly sophisticated public key encryption systems. Today, encryption software that would be resistant for decades to even the most advanced network of Cray supercomputers at the service of government security agencies are widely available and distributed worldwide. 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."45 At best, prohibitions against encryption use and "key escrow" schemes are contrivances to buy time in a losing battle.

c. Post-Industrial Global Capitalism. A further boost to the network security paradigm is provided by

changes in the global political economy, particularly the transnationalization of production and the globalization of finance. Among other things, these changes have generated a large constituency of powerful interest groups who support the network security paradigm. 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.46 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 paradigm will likely wither in importance and influence.

Conclusion

The purpose of this paper has been to identify and describe a new form of security emerging in world politics, called "network security." This paradigm of security has arisen in the late twentieth century in conjunction with the development of planetary digital-electronic-telecommunications, or what I have elsewhere referred to as "the hypermedia environment." Network security practices are distinguished by the focus on securing the "network of networks" and the information that flows through them. The primary "threat" is the potential for systems "crash," loss, theft, or corruption of data and the interruption of information flows. Policy responses include the development and distribution of highly sophisticated encryption technologies, the contracting out of security services to private actors, and the deregulation of telecommunication services. The tools employed to provide security include 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. As described above, there are good reasons arising from the material properties of the communications environment to suspect that this particular notion of security will flourish in years to come. This suggests that theorists of world politics need to analyze in more detail the practical and political implications of this security paradigm at least as much as other notions of security in circulation today.

Perhaps the most interesting aspect of this collective image of security is how different it is in many respects to traditional state-centric notions of security. In world politics, "security" in the classic sense has typically been associated with what Paul Chilton calls "metaphors of containment" -- that is, state surveillance of, and territorial defense from, "external" or "outside" forces.47 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.48 In the network security paradigm, however, security is employed with reference to insuring the validity of purchase transactions, detecting network viruses, and preventing system "crashes" -- measures designed to free up and intensify the circulation of information across borders and around the world. In short, security means integration.

The flourishing of the network security paradigm supports several trends in world politics identified by others. First, it creates a large constituency in support of the privatization of security in one very vital and important area of world politics. Although it is certainly true that states still maintain

formidable commitments to national defense in a traditional sense, the burrowing out of transnational, non-territorial, private spheres of security is a clear contribution to what John Ruggie has called the "unbundling" of sovereignty.49 As such spheres become more dense, complex, and deeply entrenched, it will be difficult for states to "turn the clock back" and return to the status quo ante. Indeed, such a development suggests that among the core industrialized states of the North - what Dan Deudney calls the liberal "free world complex"50 - the trends begun in the Cold War towards greater integration and confederation among liberal capitalist states will continue, in spite of the collapse of the Soviet Union.

End Notes

1 See John Maggs, "Are There Lessons From East Timor?" National Journal, (September 18, 1999), pp. 2634-2635.

2 Jessica Tuchman Mathews, "Redefining Security," Foreign Affairs, (Vol. 68, No. 2, Spring 1989).

3 Daniel H. Deudney and Richard A. Matthew, (eds.) Contested Grounds: Security and Conflict in the New Environmental Politics, (New York: SUNY Press, 1999).

4 John Geddes, "Mission: 'Human Security'", Macleans, (April 26, 1999), p. 112.

5 A useful bibliography of material in this area can be found in Timothy L. Sanz, "Information-age Warfare: A Working Bibliography, part II," Military Review, (Vol. 78., No. 5, Sept-Nov 1998). I have analyzed these issues in more depth in Ronald J. Deibert, "Circuits of Power: Security in the Internet Environment," in J.P. Singh and James N. Rosenau, (eds.) Information Technologies and Global Politics: The Changing Scope of Power and Goverance, (forthcoming, 2000).

6 See Carol Glasheen and John Gantz, "The Global Market Forecast for Internet Usage and Commerce: Based on Internet Comerce Market Model, Version 5," International Data Corporation Report #19262-June 1999).

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

8 For Digital Immune Systems, see http://www.symantec.com/specprog/dis/index.html.

9 "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 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.

10 Ibid.

11 For a useful critical overview of the relationship between strategic studies, problem-solving approaches, and the Cold War, see Bradley S. Klein, Strategic Studies and World Order, (New York:

Cambridge University Press, 1994).

12 Compare, for example, Quincy Wright, A Study of War, (Chicago: University of Chicago Press, 1965) with Kenneth Waltz, Theory of International Politics, (New York: Random House, 1979).

13 See the contributions in footnote 7 (above) for examples.

14 In fact, communication technologies and commercial security have been closely intertwined in other historical periods. For example, in ancient Sumeria written records on clay tablets were used to keep records of agricultural production and financial transactions. The network security paradigm under consideration here, however, begins with the computing and information revolutions of the twentieth century. But it may not be the only such paradigm in history.

15 For one example of a proposal to secure mainframe computers, see Ronald Paans, "A Topology for Secure MVS Systems," Computers and Security, (Vol. 3, Issue 4, 1984).

16 Paul Baran's pioneering theoretical treatment of distributed communications is especially interesting in this light. See Paul Baran, "On Distributed Communications," Memorandum RM-342--PR, August 1964, the Rand Corporation.

17 For a discussion of this shift, see David Harvey, The Condition of Postmodernity: An Enquiry into the Origins of Cultural Change, (Cambridge: Blackwell, 1989), Part II: The political-economic transformation of late twentieth-century capitalism.

18 For a sample of initial discussions, see Betty Feezor, "Mainframes to Micros: The Missing Link," National Underwriter, (Vol. 88, Issue 7, Feb., 1984); Lori Caradonna, "Users Finally Realize PC's Potential by Tapping Mainframe Data Stream," Bank Systems and Equipment, Vol. 22, Issue 12, December 1985); Glen Horback, "Callback Security Unit Protects Switched Data Communication System," Computer Technology Review, Vol. 5, Issue 4, December 1985).

19 For a good illustration of a study that recognized the importance of the shift from securing mainframe computers to securing distributed networks, see Ben Harrison, "Hidden Risks Threaten the Well-Being of the Network," Telecommunication Products and Technology, Vol. 3, Issue 12, December 1985).

20 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.

21 See the United Nations Conference on Trade and Development, World Investment Report, 1999.

22 Ibid.

23 See William Francis, "Mergers May Lift Foreign Direct Investment to More than $800 bn," Financial Times, (September 28, 1999), p. 4.

24Bank for International Settlements, Central Bank Survey of Foreign Exchange and Derivatives Market Activity, 1998

25 See David Mussington, "Throwing the Switch in Cyberspace," Jane's Intelligence Review (July 1996), pp. 331-334.

26 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.

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

28 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..

29 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.

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

31 "Net Security Products Set to Expand," Financial Times (London), (October 8, 1997), p. 13.

32 See the Site Patrol International Services website at http://www.bbn.com/groups/security/offerings/sitepatrol.htm

33 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.

34 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.

35 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/.

36 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

37 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).

38 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

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

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

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

42 For an extended discussion of this theoretical approach to communication environments, see Ronald J. Deibert, Parchment, Printing and Hypermedia: Communication in World Order Transformation, (New York: Columbia University Press, 1997).

43 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 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).

44 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.

45 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).

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

47 Paul Chilton, Security Metaphors: Cold War Discourse from Containment to Common House, New York: Peter Lang, 1995).

48 John Herz, "Rise and Demise of the Territorial States," World Politics 9 (July 1957), pp: 473-493.

49 See John Gerard Ruggie, 'Territoriality and Beyond: problematizing modernity in world politics', International Organization 47 (1993), pp. 139-174.

50 Daniel Deudney, "Firming the Foundations: Constitutionalizing and Memorializing the Free World Complex," in Josef Janning et al., (eds.) Civic Engagement in the Atlantic Community, (Germany: Bertelsmann Foundation Publishers, 1999).
