Scale-free Policy Organizations' Network: Artifact or Phenomenon?

Dighton Fiddner
Political Science
Indiana University of Pennsylvania
fiddner@iup.edu

1.1. Introduction

This paper is the result of research that examined the Federal government's information infrastructure system's national security policy over the decade of the 1990s with particular attention on the Clinton administration's efforts. Such a longitudinal examination was intended to provide continuous empirical evidence of the Federal government's understanding of the information infrastructure system's vulnerabilities, risks to national security, and the policy actions taken to compensate for those vulnerabilities. The research then analyzed why there had been such little policy development in this area from an organizational perspective. The research also discovered that when depicted as a network, the organizational policy structure of these efforts resembled a scale-free network. But, is this structure truly a scale-free network or only an artifact, i.e., a product of artificial character due to extraneous (human) agency [*Webster's*, 1987]?

1.2 Information Infrastructure System Security Policy

Given the salience of information infrastructure system security to U.S. economic well-being and national security, one would expect to find a well-reasoned comprehensive security policy to protect the system. Vulnerabilities of the information infrastructure system as a risk to U.S national security have been included in every annual national security strategy since 1992. President Clinton identified that vulnerabilities of the information infrastructure system posed significant risks to the national security of the nation in the National Security Strategy in 1995. The 2000 national security strategy, *A National Security Strategy For a New Century*, included protection of U.S. critical infrastructures, to include the information infrastructure, as in our **vital interest** and, therefore, important to the survival, safety, and vitality of our nation. The strategy goes on to state "we will do what we must to defend these interests, including, when necessary and appropriate, using our military might unilaterally and decisively"[U.S. White House, 1999].

The National Research Council (National Academy of Sciences, 1989, 1990], the National Communications System, and the President's National Security Telecommunications Advisory Committee all alerted the nation to the vulnerabilities of the system as early as 1989 [U.S. Department of Defense, 1997]. Even the National Security Council (NSC) acknowledged in the 1990 National Security Directive (NSD) 42 that "telecommunications and information processing systems are highly susceptible to interception, unauthorized electronic access, and related forms of technical exploitation.... and shall be secured by such means as are necessary to prevent compromise, denial, or exploitation. The NSD even specified what the U.S. response to such vulnerabilities should be:

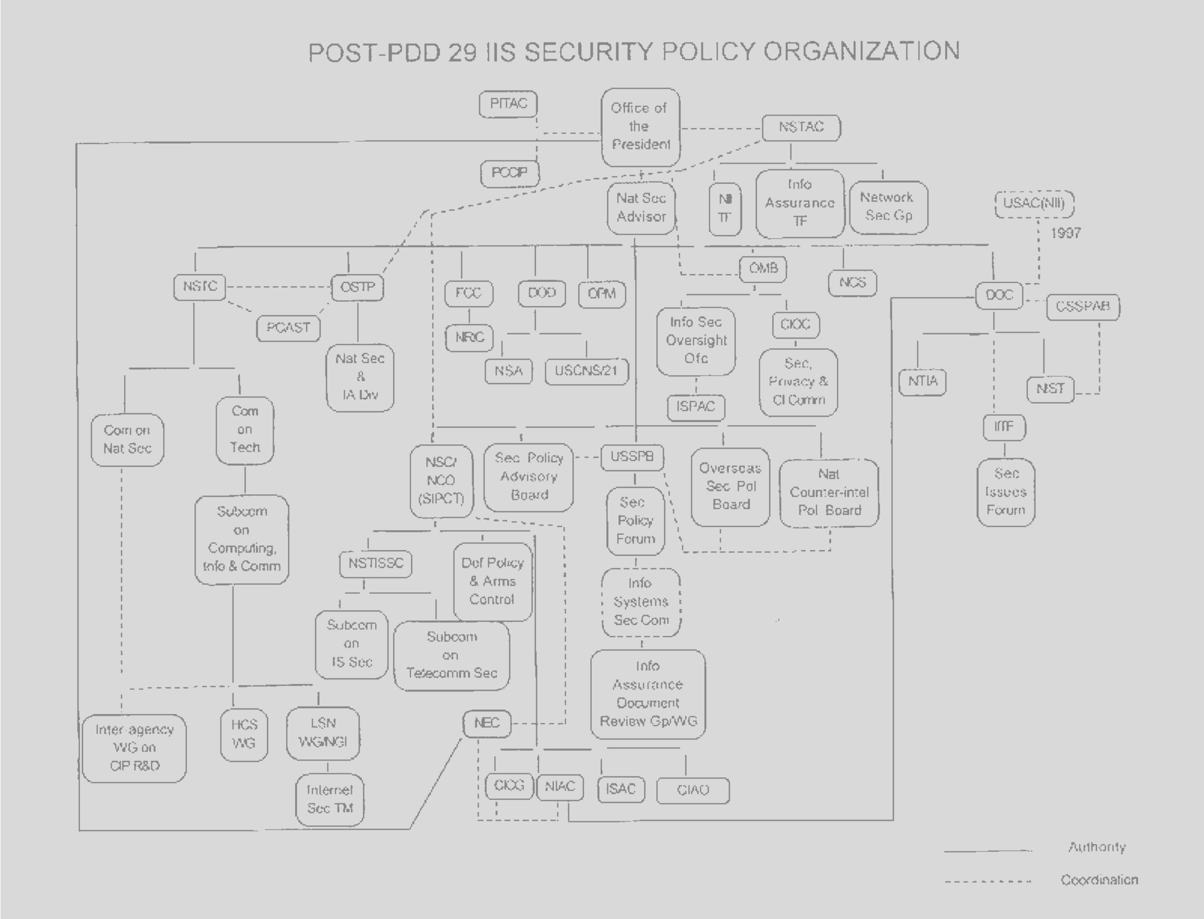
> "A comprehensive coordinated approach must be taken to protect the government's national security telecommunications and information systems (national security systems) against current and projected threats. This approach must include mechanisms for formulating policy, overseeing systems security resources programs, and coordinating and executing technical activities."

The NSD further establishes **"**initial objectives of policies, and organizational structure to guide the conduct of activities to secure national security systems from exploitation; establishes a mechanism for policy development and dissemination; and assigns responsibilities for implementation." Unfortunately, this specified approach has not been followed during the intervening years and, consequently, at the end of 2000 the United States still had no comprehensive national information infrastructure system security policy [National Security Directive (NSD) 42, *National Policy for Security of National Security Telecommunications and Information Systems*, The White House, Washington, D.C., July 5, 1990, in National Academy of Sciences, 1996].

1.3 IIS Security Policy Organizational Structure: The Traditional View

The organizational diagram following, Post-PDD 29 (>1994) IIS Security Policy Organization, depicts the different federal departments, agencies, and advisory panels that currently have a statutorily or administratively mandated role in information infrastructure system security policymaking and their relationships.[1] Any organization that has some mandated responsibility for one or more of the five information assurance objectives at the policymaking, but not implementation, level is included.

[1] Almost all organizations, to include the cabinet level departments and agencies, are intentionally shown as subordinate to the National Security Advisor. The National Security Advisor has been designated statutorily and administratively as the authority that reports to the President on information infrastructure system security policy.


POST-PDD 29 IIS SECURITY POLICY ORGANIZATION
PITAC
Office of the President
NSTAC
PCCIP
Nat Sec Advisor
NII TF
Info Assurance TF
Network Sec Gp
USAC(NII)
1997
NSTC
OSTP
PCAST
FCC
DOD
OPM
NRC
NSA
USCNS/21
OMB
NCS
DOC
CSSPAB
Info Sec Oversight Ofc
CICC
Sec, Privacy & CI Comm
ISPAC
NTIA
NIST
IITF
Sec Issues Forum
Nat Sec & IA Div
Com on Nat Sec
Com on Tech
NSC/ NCO (SIPCT)
Sec Policy Advisory Board
USSPB
Overseas Sec Pol Board
Nat Counter-intel Pol Board
Sec Policy Forum
Subcom on Computing, Info & Comm
NSTISSC
Def Policy & Arms Control
Info Systems Sec Com
Subcom on IS Sec
Subcom on Telecomm Sec
Info Assurance Document Review Gp/WG
Inter-agency WG on CIP R&D
HCS WG
LSN WG/NGI
NEC
Internet Sec TM
CICG
NIAC
ISAC
CIAO
Authority
Coordination

The research and development organizations are included because their mandated responsibilities can be interpreted to provide them with the authority to make security policy as will be shown later in the chapter. Further, their research anddevelopment agendas and priorities are essential to any information infrastructure system security policy since many of the system's inherent vulnerabilities are technical in nature. The success of these agencies' R&D efforts, to a degree, determines the success of any policy that is formulated.[2]

What is striking at first glance about the organizational diagram is the sheer number of organizations involved. Such a picture, even at a superficial level, does not auger well for efficiency or effectiveness. There are obviously too many players with a primary role to execute successfully any action whether it be planning, development, or implementation. Even at the cabinet and independent agency level, the number (13) of departments or agencies is overwhelming; the additional 18 organizations are mandated to serve as advisors on the issue to various other organizations. A total of 31 organizations have some statutory or administratively mandated responsibility for all or part of information infrastructure system security policy development complicating matters even more. Some have direct statutory or administrative authority (e.g., National Security Advisor) while others have a more derived authority (e.g., OMB).

With such an organizational structure, it would be difficult to develop a coherent policy even if other complexities could be resolved or somehow excluded from the policymaking process. By the early 1990s, the entire information infrastructure system security organizational structure was already too confusing for any remedy except complete overhaul. The Joint Security Commission reported in 1994 that there is a "profusion of policy formulation authorities, all of whom are addressing essentially the same issues" at the national level [United States Joint Security Commission, 1999].

"This 'everyone is in charge' arrangement means that no one has responsibility for meeting the vital needs for INFOSEC (information security) for national security" [United States Joint Security Commission, 1999]. This apparent diffusion of authority ("everyone in charge") did, in fact, contribute to the paucity of coordinated, coherent national policy developed during the 1990s. Without a designated policy decision maker, some policy makers and organizations

- were content to do little in a classic example of the "free-rider" phenomenon,
- increased to the point of stagnation bureaucratic competition between

[2] Both the national security strategy for 2000 (United States White House, *A National Security Strategy for A New Century*, Washington, D.C., December 1999) and *Defending America's Cyberspace: The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue* recognize the importance of research and development funding for enhanced security of the information infrastructure system. The national security strategy calls for "increased Federal R&D in information security" (United States White House, *A National Security Strategy For a New Century*, 18). The national plan for information systems protection devotes an entire program (Program 6: Enhance Research and Development in Support of Programs 1-5) that "establishes research requirements and priorities needed to implement the Plan, ensures their funding, and creates a system to ensure that our information security technology stays abreast with changes in the threat and in overall information systems" (United States White House, *Defending America's Cyberspace: The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue* Washington, D.C., 2000).

contending policy organizations, and

- failed to establish burden-sharing responsibilities.

Admittedly, some organizations were more active or accepted a larger role than others.

The Joint Security Commission was reconvened in 1999 to assess progress toward the goals recommended in the original 1994 report and to examine emerging security issues in an environment increasingly dominated by electronic data systems, networks, and communications systems. Unfortunately six years after the initial report, the Commission found that information infrastructure systems national security policy was still "in need of a clear enunciation of principles, goals, and definitions of authorities and responsibilities." As a result, "information system security policy has remained fragmented at the managerial level, with responsibilities poorly defined and spread over multiple bodies." The Commission also found that there was no clearly defined and broadly accepted institutionalized mechanism to issue national-level policy, even when endorsed and approved by the National Security Advisor [United States Joint Security Commission, 1999]. The IIS security policy structure, continued to create overwhelming confusion that is exacerbated even more by the PDD 63 mandates, not only within the federal government over who has the authority and/or power to deal with the issue and to what extent, but also within the public at large and the business community [Zuckerman, 2000].

1.4 ISS Security Policy Organizational Structure: A Network View

The policymaking organizational environment as it still exists is extremely complex. As a result of a diffusion of authority stemming from collaboration, "partnerships," Presidential advisory organizations, bureaucratic competition, etc., the U.S.'s national information infrastructure system security policy organization appears to be morphing into the very the phenomenon it seeks to control as can be seen by the following diagram. It is a replica of the identical agencies and relationships in the earlier diagram drawn as a network instead of in the traditional vertical/horizontal bureaucratic organizational chart.

Even more interesting, as can be seen from IIS Security Policy Network diagram, the policy making network resembles a scale-free network, the very type of network the information infrastructure system's structure exhibits. Upon close examination, one can identify end-users (Info Assurance TF, ISPACs, PCCP, etc.) and highly connected nodes (National Security Advisor, CIAO, DoC, NSTISS, etc.) characteristic of a scale-free network. If the physical laws of a scale-free network are generalizable to the policy environment, one would expect to see a degradation of function (policymaking) as a result of the vital node not performing its role optimally. Such an effect appears to have happened with the dearth of comprehensive information infrastructure national security policy from 1990 to 2000 adding credibility to the model of the policy environment as a scale-free network.

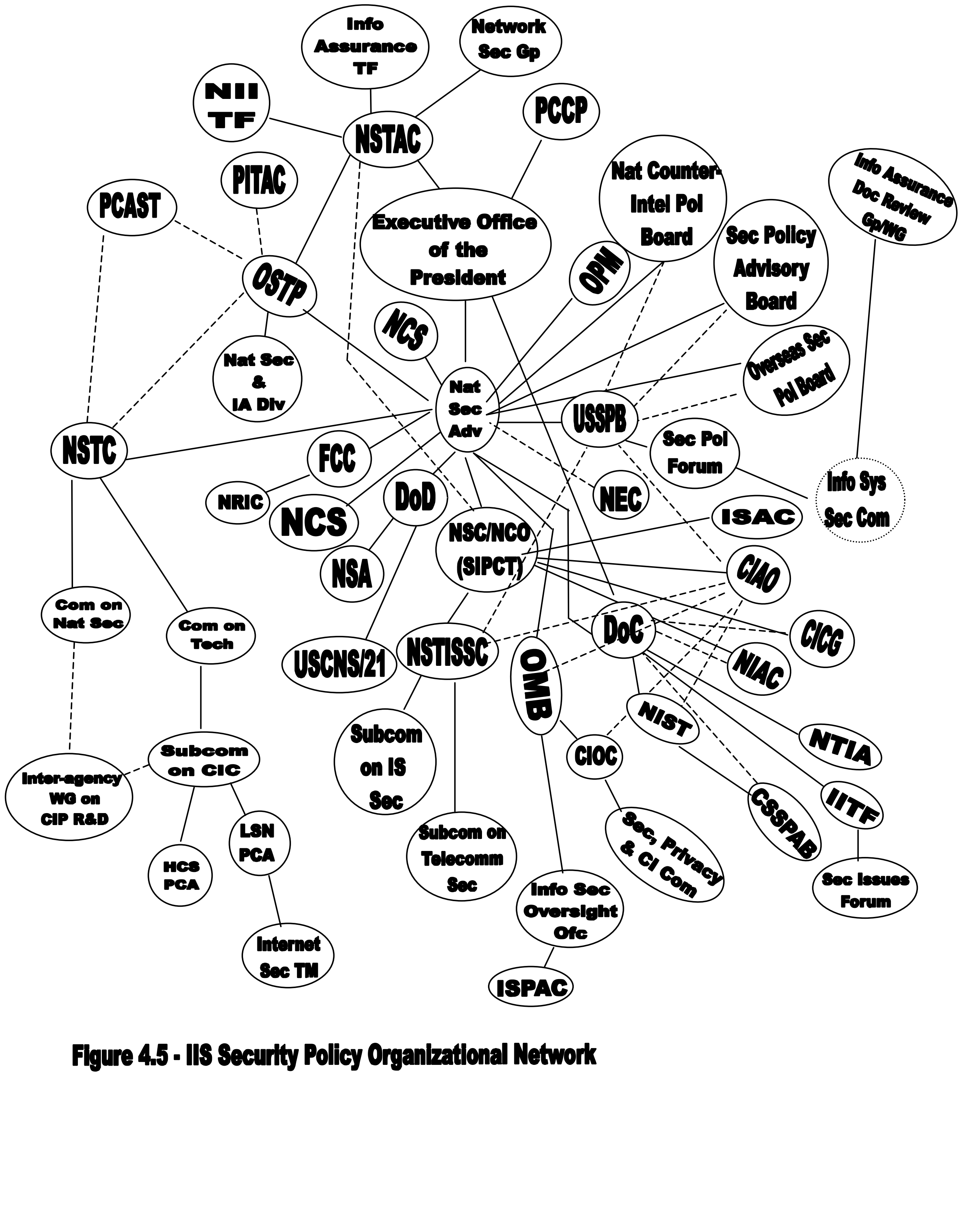


Figure 4.5 - IIS Security Policy Organizational Network

Of the critical nodes are easily identified (DoC, CIAO, NSTISS) but none are more critical than the National Security Advisor (Nat Sec Adv). Given the scale-free network's natural intrinsic vulnerability of critical node functional degradation degrading the overall performance of a system, one could reasonably conclude that inadequate performance (functional degradation) by the Nat Sec Adv critical node was the primary cause of the lack of a comprehensive information infrastructure system national security policy.

The National Security Advisor's failure to take a more active direct role (a degradation of that highly connected node's function) hampered the policy making process by not forcing, through his mandated and perceived authority, subordinate policy decision makers (DoD, DoC, USSPB, NCO(SIP&C-T, etc.) to collaborate effectively.

The CIAO's and NCO(SIP&C-T)'s inability to adequately perform their mission of integrating the other critical infrastructures into the information infrastructure national security policy making environment in a timely fashion further supports the concept of a vital node's importance and the degradation of system function correlated to degradation of a vital node.

In additional to end users and highly connected nodes, scale-free networks also use logarithmic distribution, faster growth ofhighly-linked nodes, and phased transitions of networks [Barabási, 2002]. On the surface, the highly-linked nodes seemed to grow faster so that condition is met. But, the condition of logarithm distribution does not seem to obtain. The degree distributions are:

BOTH Solid & Dashed

Degree	Count
1	23
2	15
3	3
4	3
5	3
6	3
7	1
8	1
9	0
10	0
11	0
12	0
13	0
14	1

1. Degree explains 88.3% of the variance in Count
2. The significance F is very low, 6.1E-07, so the good fit is significant, eg p<0.005
3. BUT the slope of the log-log data is the power =-1.25 ... for scale-free networks, the power is between -2 and -3, so something else is at work here.

JUST SOLID (the DASHED network is not a single component)

Degree	Count
1	28
2	11
3	5
4	1

5	2
6	1
7	0
8	0
9	0
10	0
11	0
12	0
13	1

1. Degree explains 86.3% of the variance in Count
2. The significance F is very low, 4.5E-06, so the good fit is significant, eg $p<0.005$
3. BUT the slope of the log-log data is the power = -1.32 ... for scale-free networks, the power is between -2 and -3, so something else is at work here.

It is not conclusive, but most scale-free networks also have high clustering coefficients and the clustering in these networks is extremely low (arithmetic mean of 0.02305 - it ranges from 0 to 1 - with a standard deviation of 0.04209 for BOTH and mean=0.0019352, stdev=0.00877 for SOLID). There's virtually no clustering here. The problematic node is the National Security Advisor. In both cases, it has a residual (difference between the measured value and the value predicted by the model) on the order of 10 times the residuals of the other Degree data points - both networks look more like an exponential network with an outlier than scale-free networks. This is supported by the lack of any nodes with degrees 9-13 (both) and 7-12 (solid). I suspect that this is because the high degree of this node represents a different kind of relationship than those between the other nodes.[3] Whether the IA policy organization network underwent a phased transition has not been tested at this time so I can not say with certainty whether the network meets the last condition for a scale-free network.

1.5 Conclusions

Even if the policy organization structure is not a scale-free network, the sad fact is that much of this policymaking confusion could have been avoided. Morton Halperin offers an explanation of what might have been. He postulates that "despite the different interests of the participants and the different faces of an issue which they see, officials will frequently agree about what should be done." Such agreement most likely takes place when there is strong Presidential leadership [Halperin, 1971]. Unfortunately, throughout his term President Clinton was much more interested in domestic policy than national security matters and did not provide the strong leadership necessary to clarify the policy environment to resolve the organization competition.

The current Bush administration seems to have cooled to the idea of preparing a national comprehensive information infrastructure system policy. I suspect the administration has decided that other critical infrastructure risks considered more likely to be exploited by terrorists using weapons of mass destruction with more spectacular

[3] I wish to thank publicly Steve Abrams, doctoral candidate in Information and Computer Sciences at University of California, Irvine, for his assistance in helping me better understand the physical properties of networks and for determining the degrees and power of the IIS Security Policy Organization Network depicted.

effects is a higher priority. That determination is understandable given the events of September 11, 2001. However, the vulnerabilities of the information infrastructure system probably pose a greater national security risk for the nation as a whole given the significance of the effects from exploitation of its vulnerabilities than the relatively small-scale terrorist use of weapons of mass destruction. The seemingly overriding difference between the two risks would seem to be the public panic caused by use of weapons of mass destruction from both casualties and the mere threat of and possible presence of menacing nuclear, biological or chemical agents in the nation itself. Use of weapons of mass destruction within the territory of the United States is a direct attack on the core of the nation itself and the effects are much more visible than an attack on something as invisible and abstract as the information infrastructure system, but not more damaging to the nation’s national security.

As the events of September 11 showed, sharing information between such a large number of organizations either efficiently or timely is nearly impossible. One could also argue that the administration has continued the policy pattern established during the 1990s; increasing the complexity of the policy environment. Not only has a new executive position, President's Special Advisor for Cyber security been created, but an entirely new Executive Branch department has been added to the picture without any statutory or administrative relief of the already existing policy structures or processes. The organizational landscape has become even more muddled adding yet other layers and more offices of the federal bureaucracy that have some degree of responsibility for the nation’s national security.

So, to answer the question posed in the title of this article, it does not seem as if information infrastructure security policy’s organizational structure is a scale-free network and is therefore only a product of artificial character due to extraneous (my) agency: an artifact. Even if the organizational structure is not a scale-free network, it may resemble something we international relations analysts call a “regime” – a complex of stated and understood principles, norms, rules, processes, and organizations that together help govern behavior [Goldstein, 2005]. As can be implied from the definition, such an environment is in and of itself extremely complex with few lines of demarcated authority. Such an environment bodes even worse for centralized, comprehensive policy.

References

Barabási, A.-L., 2002, *Linked: The New Science of Networks*, Perseus (Cambridge).

Goldstein, Joshua S., 2005, *International Relations*, 6/Eth edition, Longman (New York).

Halperin, Morton, Why Bureaucrats Play Games, in *Foreign Policy*, volume 2 (Spring 1971), 74.

National Academy of Sciences, 1989, *Growing Vulnerability of the Public Switched Network* National Research Council, National Academy Press (Washington, D.C.).

National Academy of Sciences, 1990, *Computers at Risk: Safe Computing in the Information Age*, System Study Committee, National Research Council, National Academy Press (Washington, D.C.).

National Academy of Sciences, 1996, *Cryptography's Role in Securing The Information Society (CRISIS)*, Committee to Study National Cryptography, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, Academy Press (Washington, D.C.), 620.

United States Department of Defense, January 8, 1997,_*Report of the DSB Task Force on Information Warfare (Defense)*, Section 2.4, "Threat" (Washington, D.C.).

United States Joint Security Commission, August 24, 1999, *Report of the Joint Security Commission II*, "Organizing INFOSEC in the Government" (Washington, D.C.).

United States White House, December 1999, *A National Strategy For a New Century* (Washington, D.C.).

United States White House, 2000, *Defending America's Cyberspace: The National Plan for Information Systems Protection, Version 1.0: An Invitation to a Dialogue* (Washington, D.C.).

Webster's Ninth New Collegiate Dictionary, 1987, Mirriam-Webster, Inc. (Springfield, MA).

Zuckerman, M.J., March 9, 2000, Asleep at the Switch? How the Government Failed to Stop the World's Worst Internet Attack, in *USA Today*.

Appendix 1: Glossary

CIAO - Critical Infrastructure Assurance Office

CIOC - Chief Information Officers Council

CSSPAB - Computer System Security and Privacy Advisory Board

DOC - Department of Commerce

FCC - Federal Communications Commission

HCS WG - High Confidence Systems Working Group

IITF - Information Infrastructure Task Force

INTER-AGENCY WG ON CIP R&D - Interagency Working Group on Critical Infrastructure Protection Research and Development

ISAC - Information Sharing and Analysis Center

ISPAC - Information Security Policy Advisory Council

LSN WG/NGI - Large Scale Networking Working Group/Next Generation Internet

NCSIP&C-T - National Coordinator for Security, Information Protection and Counter-Terrorism

NEC - National Economic Council

NIAC - National Information Assurance Council

NIPC - National Infrastructure Protection Center

NIST - National Institute of Standards and Technology

NRIC - Network Reliability and Interoperability Council

NCS - National Communications System

NSC - National Security Council

NSTAC - National Security Telecommunications Advisory Committee

NSTC - National Science and Technology Council

NSTISSC - National Security Telecommunications and Information Systems Security Committee

NTIA - National Telecommunications and Information Administration

OMB - Office of Management and Budget

OPM - Office of Personnel Management

OSTP - Office of Science and Technology Policy’s

PACHPCCITNGI - President’s Advisory Committee on High Performance Computing and Communications, Information Technology, and the Next Generation Internet

PCCIP - President’s Commission on Critical Infrastructure Protection

PCAST - President’s Committee of Advisors on Science and Technology Policy

PITAC - President’s Information Technology Advisory Committee

USAC (NII) - United States Advisory Council on the NII

USSPB - United States Security Policy Board