SOME OBSERVATIONS ALONG THE ROAD TO "NATIONAL INFORMATION POWER"

WILLIAM GRAVELL*

I. INTRODUCTION

When examining the technologies associated with information in its many forms, America has truly been blessed—or cursed, depending on your point of view—with an abundance of energy and inventiveness. Through the genius of Bell and Edison, and more recently, the products of RCA, Bell Laboratories, Microsoft, Intel and others, America has consistently held the lead in the invention and application of information technology. The practical advantages of this position have been frequent, numerous and profound. At present, American-designed and manufactured microprocessors, the subatomic particles of computer technology, dominate the global market, at a time when virtually every aspect of life on Earth is hurtling headlong toward expression in informational form. Beyond that, the operating systems and software applications—the rules that cause things to actually happen inside computers—are also totally dominated not just by the ubiquitous Microsoft Corporation,[1] but by America as a whole.

II. EARLY DAYS

It was inevitable that at some point or another, someone would attempt to link this condition of technological leadership to a larger strategy. America's commanding lead in basic technologies and the associated industrial base, added to the appeal of gadgets to many

---

* Captain Gravell's career-long focus has been on governmental activities related to information exploitation, protection, and attack. He was selected to create and serve as the first Chief of the Joint Staff Information Warfare/Assurance Division from 1994 to 1997 and recently completed his assignment as the Special Assistant for Information Policy and Strategy on the staff of the Chief of Naval Operations Executive Panel. Captain Gravell retired from the Navy earlier this year. The views expressed in this Article are strictly those of the author and do not reflect official or policy positions of the federal government or of the Departments of Defense or the Navy.

1. *See* David Rothkopf, *In Praise of Cultural Imperialism? (Effects of Globalization and Culture)*, FOR. POL'Y., Jun. 22, 1997, at 38.

Americans, combined with opportunities created by global trends in adoption of information-based products and services. This alignment of forces created a situation that scholars and futurists came to describe as Information Warfare, or IW.[2] The official and unofficial definitions of IW and its many offspring and relatives are legion, and appear to change daily—I refuse to add to the confusion by citing any of them. For my purposes here, I suggest that a simple way to approach IW would be to view "information" and associated technologies as tools of great importance and power. We should strive to enhance and protect them when they are used by us and our friends; we should seek to attack and degrade them when used by our opponents.[3]

The Department of Defense quickly recognized the power of information.[4] After internal study and debate, concepts began to visibly take shape, especially within the Joint Staff.[5] By 1995, information was judged to hold a "first among equals" status alongside other critical processes and capabilities. The term "information superiority" was coined, and characterized as the lens through which all other critical military processes and capabilities are derived, preserved and executed.[6] Within the military, this characterization resulted from a logical progression from processes and experiences that had been understood and practiced for some time prior to this.[7]

Although it is impossible to cite a single, specific event as the catalyst, most authorities agree that serious efforts to broadly address the protective and defensive aspects of IW within the United States (including their potential effects on non-combatant bystanders) date from about 1994. The qualification of the foregoing sentence is important. Notwithstanding the earlier military efforts focused on the conduct of classic, and primarily offensive, operations, only in 1994 did we see the beginning of processes with extensive organizational

---

2. *See* THE FIRST INFORMATION WAR, at ix-xi (Alan D. Campen ed., 1992).

3. This is usually reflected in the many definitions of IW as some variation on offense vs. defense. At the very end of this article, I will cast these terms in a somewhat different light–one that may be more appropriate for discussions of strategy.

4. *See* THE JOINT CHIEFS OF STAFF, INFORMATION WARFARE: A STRATEGY FOR PEACE (1996).

5. *See generally* THE JOINT CHIEFS OF STAFF, INFORMATION WARFARE: LEGAL, REGULATORY, POLICY AND ORGANIZATIONAL CONSIDERATIONS FOR ASSURANCE (2d ed. 1995).

6. *See* THE JOINT CHIEFS OF STAFF, JOINT VISION 2010, at 16-19 (1995).

7. *See* THE JOINT CHIEFS OF STAFF, COMMAND AND CONTROL WARFARE, Memorandum of Policy No. 30, 2-3 (1993).

participation outside the military, designed to systematically understand and respond to the effects of the Information Age on America.[8]

III. A BRIEF ORGANIZATIONAL HISTORY OF INFORMATION

A Golden Age of IW intellectualization began in 1994. Conferences and symposia too numerous to list were hosted by all who wanted to understand, thought they already did and wanted to convince others, or saw a chance to make a buck off the latest craze. Respected bodies such as the Defense Science Board were commissioned to produce major studies in the field.[9] The National Defense University, the leading academic body of the U.S. defense establishment, created a yearlong graduate School of Information Warfare and Strategy.[10] In a prescient observation made in association with the inauguration of that effort, the Chairman of the Joint Chiefs of Staff predicted that the new school would focus on the information component of national power.[11]

Inside the Joint Staff, a new organization, the Information Warfare Division (J6K), was created inside the directorate responsible for telecommunications and related technologies.[12] J6K quickly assumed responsibility for all Joint Staff efforts related to Defensive aspects of IW.[13] Its first goal was to work toward a broadly based and rigorous understanding of military forces' dependency on information. From that vantage point, it sought to better ensure that the informational "goods and services" required for the conduct of military operations would be available when, where, and in the forms needed.[14]

These defensive aspects of IW soon became more specifically referred to as "Information Assurance." This is an important development in the history of these processes. This subtle change indicates that it may be possible to recharacterize all offensive measures associated with information as a form of state activity, ranging from minor coercion to warfare (due to the tools, practitioners and pur-

---

8. *See generally* THE JOINT CHIEFS OF STAFF, *supra* note 5.

9. *See* OFFICE OF THE UNDER SECRETARY OF DEFENSE FOR ACQUISITION & TECHNOLOGY, REPORT OF THE DEFENSE SCIENCE BOARD TASK FORCE ON INFORMATION WARFARE-DEFENSE 1 (1996) [hereinafter OUSD A&T].

10. *See* NATIONAL DEFENSE UNIVERSITY, SCHOOL OF INFORMATION WARFARE AND STRATEGY, STUDENT HANDBOOK 1 (1996-97).

11. *Id.*

12. *See* THE JOINT CHIEFS OF STAFF, *supra* note 5, at app. A-15.

13. *See id.*

14. *See id.* at 1-1.

poses with and for which it may be employed).[15] As such, to the extent that offensive informational activities are considered necessary or useful to facilitate achieving a desired outcome in support of military or other governmental operations, the responsibility for these activities is exclusively governmental.[16] In contrast, the persons, processes, and, above all, equities of information protection exist far beyond the outer boundaries of the domain of "warfare," or the scope of government authority.[17] To characterize information-protection efforts as being inherently associated with the conduct of "warfare" is to instantly flavor the processes and purposes improperly, and in a way that places them in a cultural and legal position that handicaps useful collaboration between government, writ large, and the commercial sector. I will show later on how that becomes a defining and pacing feature in my discussion.

Elsewhere inside the Department of Defense, efforts of the Information Systems Security Office, under the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, picked up speed.[18] Military services strove to understand the potential of IW and adapt it to their traditional strengths and cultures. The National Security Agency, with responsibility for protection of classified (but not unclassified) government communications,[19] continued to expanded its outreach efforts across a broad front.[20] Among those organizations approached was one of the few at the time with a built-in charter for coordination and information sharing across the government-civil interface, the National Communications System and its executive body, the National Security Telecommunications Advisory Committee (NSTAC).[21] The NSTAC Principals, a group of the Chief Executive Officers of some of the nation's leading telecommunications and information-technology corporations, were sufficiently concerned about the implications for the "integrity of the nation's information systems, both governmental and public," that they sent a

15. *See generally* WALTER GARY SHARP, SR., CYBERSPACE AND THE USE OF FORCE (1999).

16. *See id.*

17. *See* THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, CRITICAL FOUNDATIONS – PROTECTING AMERICA'S INFRASTRUCTURE, at ix-xi (1997).

18. *See* THE JOINT CHIEFS OF STAFF, *supra* note 5, at app. A-7 to A-8.

19. *See* 15 U.S.C. § 278g-3 (1994).

20. *See* THE JOINT CHIEFS OF STAFF, *supra* note 5.

21. *See* THE PRESIDENT'S NATIONAL SECURITY TELECOMMUNICATIONS ADVISORY COMMITTEE INFORMATION ASSURANCE TASK FORCE, ELECTRIC POWER INFORMATION ASSURANCE RISK ASSESSMENT 1 (1997) [hereinafter NSTAC].

letter to the President in March 1995.[22] NSTAC has continued its good works to date, but within some limits.[23] However valuable NSTAC has been as a model of government-civil coordination, its charter is bounded in ways suggested by its name.[24] In its focus on commercial telecommunications and closely related industries in support of specified national security applications, NSTAC was only a partial solution to a much larger problem. Something else was needed.

IV. THE GOVERNMENT-CIVIL INTERFACE TAKES FORM

From the beginning, the most consistent findings from the many IW studies and analytic efforts pointed to the profound vulnerability of commercial, privately owned and operated information infrastructures to serious disruption in the performance of critical functions.[25] At the same time, it became obvious that government operations, from the mundane to the most critical, were dependent upon those same civil information infrastructure processes.[26] This pair of linked conclusions shaped further issue development, both within the government,[27] and among the infrastructures themselves.[28]

At this point, one axis of the government's growing interest in, and concern for, information began to focus on these civil information infrastructures specifically.[29] The President's Commission on Critical Infrastructure Protection (PCCIP) was created by Executive Order.[30] The Commission organized its treatment of the infrastructures into several categories: telecommunications, banking and finance, electric power, oil and gas distribution, transportation, water systems and emergency services.[31] In due course, the Commission produced its report, reiterating the findings of earlier studies regarding the dependency of both critical public and private processes on

22. *Id.*

23. *See* THE JOINT CHIEFS OF STAFF, *supra* note 5, at 2-22 to 2-24.

24. *See* Exec. Order No. 12,382, 47 Fed. Reg. 40,531, 40,531 (1982).

25. *See* THE JOINT CHIEFS OF STAFF, *supra* note 5, at 1-1.

26. *See generally id.*

27. See OUSD A&T, *supra* note 9, at ES-1.

28. *See* NSTAC, *supra* note 21, at ES-2.

29. *See* THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 17, at ix-xi.

30. *See generally* Exec. Order No. 13010, 61 Fed. Reg. 37,347 (1996).

31. *See id.*

information and the vulnerability of these commercial cartels,[32] and providing several recommendations.

After a period of review and staffing of the Commission's report, the Clinton administration framed its response to Information Age threats. Interestingly, it produced not one document, but two, releasing them on the same date. The first of these, Presidential Decision Directive 62,[33] related to methods of countering the terrorist threat.[34] The second, and the primary focus of my attention here, was Presidential Decision Directive 63 (PDD 63), Critical Infrastructure Protection.[35] This approach is interesting because it appears to draw a procedural and organizational line between highly similar processes, in which the underlying equities with both charter and capacity to respond to the problem are totally governmental on one side (counter-terrorism), and primarily civil on the other. PDD 63 split these processes into parallel but separate regimes in spite of the growing awareness in government circles of the convergence between terrorism and information-attack.[36]

PDD 63 emphasizes information sharing, both within government and between government and the private sector.[37] Most of the directed actions relate to the creation of organizational structures designed to mitigate the vulnerability of information infrastructures, and to promote their rapid restoration to full effectiveness after a degrading incident. The Federal Bureau of Investigation (FBI) was established as a focal point for these activities, especially for the collection and dissemination of incident and threat warning.[38]

---

32. *See* THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 17, at ix-xi.

33. *See* Presidential Decision Directive 62. (PDD 62 is classified but is described in the White House press release "Summary of Presidential Decision Directives 62 and 63," dated May 22, 1998, and is on file with the *Duke Journal of Comparative & International Law*).

34. *See id*.

35. The White House, White Paper: Presidential Decision Directive 63—Critical Infrastructure Protection (1998) (on file with the *Duke Journal of Comparative & International Law*).

36. For example, this association had been discussed a year earlier at the Defense Department's annual Worldwide Antiterrorism Conference, held in San Antonio, TX (August 18-22, 1997), and also addressed in a letter from H. Allen Holmes, the Assistant Secretary of Defense for Special Operations and Low-Intensity Conflict, to the author (Nov. 3, 1997) (on file with the *Duke Journal of Comparative & International Law*).

37. *See* The White House, *supra* note 35, at 2-3.

38. *See id.* at 9.

V. THE POLICY ENVIRONMENT

Having completed a rapid historical review, I have caught up to the present. The various actions assigned by PDD 63 are nearing completion. The FBI has set up the National Infrastructure Protection Center (NIPC) to "serve as a national critical infrastructure threat assessment, warning, vulnerability *and law enforcement investigation and response* entity."[39] This law enforcement investigation and response entity serves as the point of departure for the next aspect of the discussion.

At this juncture, if one were to ask, "why are we doing this?," the answer seems obvious, based on the discussion to this point: to ensure the efficient performance of critical public and private functions (and thereby to protect lives and property), and to promote economic health and prosperity.[40]

A second question relates to the scope and bounds of the effort associated with the vitally needed function of infrastructure protection. What are those bounds? The short answer is that there are none.[41] The problem is global in size and unfixed in shape.[42] The condition of vulnerability is permanent, in that even if perfect protection could be achieved (which it almost certainly cannot), it would have to be maintained through constant vigilance, at all organizational levels, from top to bottom.[43] Who is competent and trusted, by all parties to the process, to perform these vital functions?

In terms of the mechanical performance of the role, what are the required inputs? The internal process considerations? The outputs? Bear in mind, these answers must be framed in several dimensions (e.g., not only the type of information required, but the granularity, periodicity, and specificity).

The real question is: can any single actor or agent do this? National information-protection initiatives seek to protect the domestic economy.[44] However, the clear trend is toward economic globalization, such that domestic and international domains are increasingly

---

39. *Id.* (emphasis added).

40. Is it not also possible to characterize these goals as expressions of our "vital national interests"?

41. *See* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, CYBERCRIME, CYBERTERRORISM, CYBERWARFARE: AVERTING AN ELECTRONIC WATERLOO xvi (1998).

42. *See id.*

43. *See id.* at xvi-xviii.

44. *See* OUSD A&T, *supra* note 9, at ES-2.

indivisible.[45] Just as the various "bad actors" have the ability to project their effects to or from any spot on the globe,[46] so it is highly likely that any attack on critical domestic infrastructures that affects economic performance will resonate globally.[47] From this globalization, we can see the development of information warfare from its conceptual beginnings as a nice, tidy matter of domestic law enforcement, into something that must, over time, be drawn inexorably into the realms of international security and management of the global economy. Placing the shoe on the other foot, the military recognized early in its thinking about information that even though forces may be operating in some distant area of the world, the tail of reach-back support associated with those activities extends into these same domestic, commercial networks.[48] As such, the conduct of foreign policy and military operations on the global scene immediately and necessarily engages domestic interests and equities.[49]

Governmental organizations which must think about the terrorist threat, and which have traditionally been prone to seek and engage that threat overseas, are increasingly aware of the vulnerabilities of domestic infrastructures, and of the opportunities available to malefactors to access these "soft targets" via global information networks.[50] The theme has also been picked up within the realms of criminal justice and academia.[51] Knowledge of these vulnerabilities stands as further evidence of how difficult it will be to neatly segregate domestic and international issues in this field, notwithstanding the fact that the charters of federal organizations are split largely along those territorial lines.[52]

---

45. *See* Center for Strategic and International Studies, *New Global Economy Project*, (visited Feb. 13, 1999) <http://www.csis.org/nge/>.

46. *See* Barry C. Collin, *The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge, in* TERRORISM AND THE NEW WORLD DISORDER 3 (Office of International Criminal Justice, University of Illinois at Chicago ed., 1997).

47. *See* OFFICE OF SCIENCE AND TECHNOLOGY POLICY, EXECUTIVE OFFICE OF THE PRESIDENT, CYBERNATION: THE AMERICAN INFRASTRUCTURE IN THE INFORMATION AGE 27-29 (1997); THE JOINT CHIEFS OF STAFF, *supra* note 4, at 2.

48. *See* THE JOINT CHIEFS OF STAFF, *supra* note 4, at 3.

49. *See id.* at 2.

50. *See* William Gravell, *Information Warfare and Terrorism: Changing the Rules* (Briefing to the Worldwide Antiterrorism Conference, San Antonio, TX, Aug. 19, 1997).

51. *See generally* Collin, *supra* note 46.

52. *See* The White House, *supra* note 35, at 8-9. For example, the Department of Justice and the FBI are responsible for law enforcement and internal security while the CIA, the Department of State, and the Department of Defense are responsible for intelligence, foreign affairs, and national defense, respectively, with regard to information warfare. *See id*.

Domestic law enforcement must be seen as one among many centers of organizational concern, *and of skill, training and experience*, in dealing with the set of problems emerging in the Information Age.[53] Just as the information networks at the center of the issue respect no boundaries of jurisdiction, culture or organizational demarcation, the nation's solution must be able to elegantly draw upon the whole range of human skills and organizational capabilities.[54] In their quite proper emphasis on information sharing, the members of the PCCIP clearly had this in mind.[55] Indeed, if one is constrained to meet the need by choosing one of the existing governmental bureaucracies, the decisions reflected in PDD 63 can hardly be faulted.[56] In fairness, PDD 63 may be considered the best approach to get some capability online quickly that was available at the time. The larger question we should now be focused on, however, is whether that approach—staying "in the lanes" of the historic organization of the federal government—best meets the nation's needs in the *long* term.

VI. THE FRIENDLY NEIGHBORHOOD INFORMATION COP

As noted above, PDD 63 assigned to the FBI (through the NIPC) significant responsibilities for information-attack threat collection and dissemination, while (naturally) preserving the parent organization's traditional investigative roles.[57] There is evidence that this duality is causing concern among at least some of the domestic information stakeholders, without whose full cooperation any effort to protect the National Information Infrastructure is dead on arrival.[58]

At a recent seminar strategy game jointly sponsored by a leading consulting firm in this field, a major computer security industry association, and the U.S. Army War College, senior industry representatives worked with government experts to identify and resolve issues associated with a plausible information-attack scenario.[59] A civilian

53. *See* Collin, *supra* note 46, at 4.

54. *See id*.

55. *See* THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 17, at 23.

56. *See id*. at 6.

57. *See* The White House, *supra* note 35, at 9.

58. *See* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at 54-62.

59. *See* ROBERT F. MINEHART, THE INFORMATION ASSURANCE SEMINAR GAME 62 (1998).

governmental expert, whose expertise centers on the commercial side of federal operations, made the following observations:

> Most critical infrastructure industry representatives regard their reaching out to government (including federal law enforcement), "'as adding little or no value' or as 'legal problems to be avoided—at least until the situation the company was experiencing became clearer to the firm's executives.'"
>
> These lessons and the cultural problems of perceptions, attitudes, communications and understanding are valuable. *We, as a nation, need to change our way of thinking about traditional industry-government relations and organize now to face the challenge of building genuine government-industry partnerships for cyber protection of critical national infrastructures.*[60]

At this point, it is important to remember that the Department of Justice, and the FBI in particular, does and must perform absolutely vital functions in any conceivable regime of national/domestic information infrastructure protection. The goal here is neither to malign those functions nor to belittle the contributions of those organizations, but rather to demonstrate that a broader—indeed, universal—view is required. Absent such a perspective, all scenarios tend to be framed within the context and culture of the single/dominant organization.

An example of this point may be found in the National Information Infrastructure Act of 1996 (NII).[61] The Act "raises the bar" on criminalization of information attack in several ways.[62] Notably, this includes new protections for several categories of "information from any protected computer."[63] The term "protected computer" is further defined in the Act to include a computer "which is used in interstate or foreign commerce *or communications*."[64] It is hard to imagine any internet-accessible computer which would not satisfy this definition. As such, the Act does an excellent job of providing for a broad range of criminal and civil penalties in response to many kinds of unauthorized information penetration, destruction, commercial exploitation, or communication of information to unauthorized recipients. Its authors and sponsors are to be commended for patching this gaping hole in the domestic legal structure. However, the legal structure lacks a counterpart understanding of the adjacent equities.

---

60. *Id*. (emphasis added).
61. 18 U.S.C.A § 1030 (West Supp. 1999).
62. *See id*.
63. 18 U.S.C.A § 1030 (a)(2)(C).
64. 18 U.S.C.A § 1030 (e)(2)(B) (emphasis added).

One example of these organizationally adjacent and parallel concerns is found in national security responses involving intelligence or Defense Department capabilities. The default outcome of the current structure is that all incident responses are managed at the outset within a domestic law enforcement paradigm.[65] This leaves the law enforcement community with a clear and actionable charter to treat every incident as within their jurisdiction.[66] However, in so doing, the structure includes law enforcement officers whose experience and training might leave them ill-suited to provide appropriate and timely organizational responses that meet the nation's most pressing needs.

This latter point highlights the issue. It is virtually axiomatic that whatever else any given information attack may betoken, it is against the law. As such, the prospect of a proper law enforcement investigation, leading to the arrest, trial, and conviction of a criminal, hangs over every incident from the outset. This paradigm is likely to coexist with competing interests. Each interest is completely legitimate in its own way, whether it amounts to broadcasting warnings to a broad audience, maintaining secrecy for purposes of intelligence exploitation, or using the information to support planning for military operations.[67] At the risk of appearing facetious, one might contemplate a Cold War parallel where the planned response to the threat of Soviet bombers attacking the United States would be to bring Wrongful Death actions against the Soviet pilots in American courts.[68]

In fairness, it must be pointed out that PDD 63 anticipates that law enforcement interests may need to be subordinated to those of larger national security under unspecified circumstances, "[d]epending on the nature and level of a foreign threat/attack."[69] However, at least to date, these procedures have not always worked smoothly. There are reasons to believe that this is cause for concern. With the National Defense Authorization Act of 1996, Congress recognized the threat of "strategic attack by foreign nations, groups or

65. *See* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at 57; The White House, *supra* note 35, at 10. *See generally* 18 U.S.C. § 1030.

66. *See* The White House, *supra* note 35, at 9-10; CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at 57.

67. *See* THE JOINT CHIEFS OF STAFF, *supra* note 4, at 15-16.

68. *See* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at 41. The CSIS asks specifically about the proportionality of the American response to an IW threat, wondering if the U.S. would "nuke [an IW aggressor] because they turned off our TVs?" *Id.*

69. *See* The White House, *supra* note 35, at 10.

individuals . . . against the NII."[70] Similar concerns regarding strategic attack were repeated by Congress in 1997[71] and also very recently by a highly respected think tank.[72] "Strategic" is emphasized to underline the point that one may readily contemplate Information Age scenarios which far exceed the response capacity of any single organization, particularly organizations with a historically domestic emphasis.

The commercial operators of the private sector represent another group of concerned players adjacent to law enforcement in these matters. Their motives and interests are obvious: continued profitability, economically efficient operations, protection of trade secrets and other intellectual property, and maintenance of a satisfied customer base, among other things. In pursuit of these goals, prudent Information Age corporations closely watch their networks and information systems. However, it has been noted that

> [o]nce law enforcement is introduced to an incident such as an intrusion, the 'rules of engagement' change. For example, once the phone company notifies the FBI of a cyber attack, they would no longer be able to monitor customer transactions because of the rules of evidence. In effect, the phone company would no longer be able to conduct an internal investigation.[73]

One feature of the NIPC is that it provides the single point-of-contact (POC), so long sought after in the world of governmental information protection.[74] While a single POC may be desirable to streamline authority and responsibility in coordination, it is unclear whether choosing a strong, central POC from among the Industrial Age organizational entities of the current federal governmental structure is the best solution. In an interesting contrast to this approach, the government has urged the commercial sector to consider using the highly distributed Centers for Disease Control model to create of an industry-centered Information Sharing and Analysis Center (ISAC).[75] Through its suggestion, government may be implicitly recognizing that "those who believe the solution to national information

---

70. The JOINT CHIEFS OF STAFF, *supra* note 5, at 2-59.

71. *See id*. at 2-39.

72. *See* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at xix.

73. MINEHART, *supra* note 59, at 68.

74. This passion for centralization may devolve from the strong role played in the early days of information protection by the military, wherein "unity of command" is considered essential, and in every undertaking, one can point to the person "in charge" of the entire operation.

75. *See* The White House, *supra* note 35, at 10-11.

vulnerability can be found through declaring any one person or organization to be in charge . . . reveal only their ignorance of the complexity and scope of the issues involved."[76]

It may well be that the model of industrial cooperation, which recognizes limits of authority and respects different organizational cultures, may be instructive in this context. As a nation, we must enfold highly dissimilar processes in our national approach to information and its protection. Statecraft, intelligence, the military, and law enforcement comprise the classic elements of U.S. national security, with an obviously offshore orientation.[77] Our Information Age thinking must expand that set of participants to embrace financial and economic actors, personal health and welfare concerns, and other equities. Indeed, one is hard pressed to think of a national function, either governmental or commercial, which does not have a need for effective and protected information management.

VII. INDICATIONS AND WARNING

Up to this point, this Article has examined, and strongly supported, the findings of all credible practitioners working in this field regarding:

- the criticality of information and its related technologies to virtually all aspects of American domestic and international security, welfare, and prosperity;
- the vulnerability of these critical processes to many sources of attack or disruption;
- the recognition that importance plus vulnerability indicate the need for a serious and thoughtfully constructed strategy to preserve and protect information, including related processes and technologies;
- the need for efficient procedures of trusted sharing and collaboration in pursuit of these goals, not only *between* government and the private sector, but also *within* the government; and
- the need for adaptive organizations, created to effect this type of trusted information sharing in the name of the common good.

---

76. CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at 56 (quoting William Gravell).

77. It has been asserted, however, that "the info-tech revolution is making defense, diplomacy, intelligence and technology indivisible." Paul Mann, *Info Technologies Transform National Security Doctrine,* AVIATION WK. & SPACE TECH., Nov. 23, 1998, at 51.

The discussion now turns to what it will take to put these ideas into practice.

At the heart of this need for sharing is a process known in governmental parlance as "Indications and Warning" (I&W).[78] This capability, under various names, has been called for by virtually every IW study conducted during the period of our review.[79] Even Congress has cited the need for this capability.[80]

A generic I&W model is shown in Figure (1). This graphic is provided to help depict the flow of the process as well as to highlight the relationships between different parties in the enterprise at various stages in the effort.[81]

The central questions in I&W are twofold: (1) what is to be protected and (2) against what threats do we need to protect ourselves? That our answers to these two questions remain limited is one of the most important unresolved aspects of our information strategy. Unfortunately, as will become evident, this Achilles' heel could meaningfully hamstring efforts to achieve our much-needed I&W capability.

If one does enjoy an adequate understanding of the answers to these two questions, one can follow the model through a reasonable process down the left track (intelligence/threat), leading to a final analytic understanding, supported by evidence, of what is happening or about to happen (indications). One may then disseminate that knowledge to any selected group of recipients, in the form of a warning.

---

78. Purists may point out that in intelligence parlance, "I&W" refers to insights gained on a strategic timeline regarding the development of some future threat, while terms like "Tactical Warning and Attack Assessment" (TWAA) describe time-sensitive, reactive processes such as those associated with information attack detection, assessment and restoration. Nonetheless, within the IA community, "I&W" is the term in most common use, and it will be so used here.

79. *See, e.g.*, ROBERT H. ANDERSON & ANTHONY C. HEARN, AN EXPLORATION OF CYBERSPACE SECURITY R&D INVESTMENT STRATEGIES FOR DARPA 9 (1996); OFFICE OF SCIENCE AND TECHNOLOGY POLICY, *supra* note 47, at 27-29; THE JOINT CHIEFS OF STAFF, *supra* note 4, at 9; OUSD A&T, *supra* note 9, at 6-4 to 6-6.

80. *See* National Defense Authorization Act for Fiscal Year 1996, Pub. L. No. 104-106, § 1053(1), 110 Stat. 186, 440-41 (1996) (directing the White House to report to Congress on the state of national policy regarding attacks on American information infrastructure).

81. *See* William Gravell, *National Security in the Information Age: Changing the Rules*, *in* NATIONAL INFORMATION INFRASTRUCTURE PROTECTION IN THE 21ST CENTURY 108, 111-112, F-4 to F-6 (Duke University School of Law Center on Law, Ethics and National Security et al. eds., 1998). This model was shown and discussed at a conference hosted by Duke University in early 1998.

It would be easy to fall into the trap of seeing the term "I&W" as descriptive of a single unit. Indeed, this might well be inferred from the simple ampersand separating them. However, to do so is to fail to recognize that "indications" and "warning" are in fact two quite separate processes, functioning synergistically, each drawing heavily upon the other for its effectiveness, if not its very existence.[82] Note also the horizontal relationships of the model. In some cases, cooperation between equities on each side of the central arrow is needed to perform some required activity (for example, the placement or functioning of sensors in optimal locations). In other cases, one may seek to engage stakeholders early in the process, with a goal of heightening their awareness of the threat, thereby building support for later cooperation. The top-row processes on the model provide examples of this.

The historic case of the North American Aerospace Defense provides an exemplary illustration. Given that the goal of the program was preventing Soviet nuclear weapons (first delivered by bombers, and in later years by missiles) from reaching the North American continent in a surprise attack, the rest of the system, while far from easy, was at least practicable.[83] Understanding the physics, time-distance factors and other variables associated with such an attack permitted the engineering of a specifically-designed system of sensors, analytic and communications capabilities; the creation of tailored policies and standard procedures to be followed in the event of predictable eventualities; and the establishment, a priori, of the necessary working and authority relationships.[84]

The last point is particularly relevant to the discussion. The system is run by the North American Aerospace Defense Command (NORAD); Canada has always been an integral partner, even though it has never possessed nuclear weapons, and the sparsely populated territory of northern Canada was never a likely target for Soviet missiles.[85] The simple fact is that the nature of the threat we were confronting indicated a polar-oriented attack; thus, in order to achieve the maximum warning time, it was highly desirable to install sensors as far forward (that is, to the north) as possible, which meant Canada,

82. Hence the form of expression at the top of Figure (1): "Indications *and* Warning."

83. *See* JAMES MEIKLE EGLIN, AIR DEFENSE IN THE NUCLEAR AGE 57-59, 72-75 (1988)

84. *See* JOSEPH T. JOCKEL, NO BOUNDARIES UPSTAIRS: CANADA, THE UNITED STATES, AND THE ORIGINS OF NORTH AMERICAN AIR DEFENSE, 1945-1958, at 17-18 (1987).

85. *See id.* at 1, 42.

among other places.[86] In the course of negotiations creating the Distant Early Warning Line as a sensory feed to NORAD, considerable accommodations were made to the Canadian government.[87] These concessions provided for extensive partnerships along several lines, including commingled staffing at several levels, up to the Vice Commander, who is always a Canadian.[88] At the center of the relationship is the understanding that without sensory inputs achievable only with Canadian cooperation, attack awareness would either occur late or not at all.[89]

In return for this vital contribution to the NORAD enterprise, Canada was entitled to participate in and receive the fruits of the analysis.[90] Furthermore, the aspect of the response related to its eradication or minimization of the threat before the fact—in this case, through interception by fighter aircraft—has also been a collaborative US/Canadian effort from the outset.[91] In summary, this case presents a coordinated, voluntary effort between two sovereigns to construct a sensory apparatus across jurisdictional boundaries, to collaborate in active negation of specified threats, and to share information related to the status of threats and efforts to reduce those threats, on both strategic and tactical timelines.[92]

The comparison of the case above to the current discussion reveals important contrasts. Recall the two overarching questions of I&W:

What is to be protected? If we are correct in our understanding that the availability of timely, accurate, and uncorrupted information is essential to national security and all other governmental processes, then does it follow that all governmental information requires a similar protective regime? If the NSTAC, PCCIP and others are correct (and I think they most certainly are) regarding the extent of civil ownership of the information infrastructures upon which not only government, but also the health and welfare of our citizens are dependent, does that indicate a similar need to protect all such commercial infrastructures? In short, absent something akin to a national information strategy, on what basis would any public or private in-

86. *See* WILLIAM FRIEDMAN ET AL., ADVANCED TECHNOLOGY WARFARE 51 (1985).
87. *See* JOCKEL, *supra* note 84, at 3, 25.
88. *See id.*
89. *See* EGLIN, *supra* note 83, at 72-74.
90. *See* JOCKEL, *supra* note 84, at 83.
91. *See id.* at 2-3.
92. *See id.* at 91-92.

formational product or service be culled out from the (apparently) needed protective umbrella? And yet we must agree that any suggestion that the government should undertake to protect "everything" can be dismissed out of hand as unmanageably large, expensive, and difficult, to say nothing of the enormous implications for privacy and governmental intrusion into private commerce.

Clearly, what is needed is a strategy, with some rigorous basis, to identify and perhaps even prioritize what is to be protected. Such a strategy would necessarily go beyond the limits of the domestic infrastructures discussed in PDD 63.[93] It would certainly require the coordination of "sensory" information from the commercial sector with governmental intelligence and retaliatory efforts, on a basis of complete and mutual trust and confidence. For government to invite (much less demand) that civil stakeholders provide full and unfettered access to their proprietary information is unreasonable and unworkable. Government must first quantify, specify, and, most particularly, bound the informational need, making a reasoned and open case to see it fulfilled. Such an effort would require, in both creation and operation, the support of virtually the entire economic and political leadership of the nation, as well as broad support from an informed public. It would presumably be an undertaking so broad (but not necessarily large) that no one organization, in or out of government, could manage it alone. PDD 63, notwithstanding its invaluable role in providing for "initial steps" toward meaningful civil and governmental cooperation, falls well short of the scope of what is being described here.

What are we protecting against? This question must be answered in several dimensions. Some progress has been made in defining "cyber attack," as noted above.[94] Similarly, there has been progress in recasting traditional forms of economic crime, such as fraud, in informational terms.[95] However, when the motives and actors of such attacks transcend the traditional scope of domestic criminal and civil misconduct, how well prepared are we to respond as a nation? We do not refer here to any kind of tit-for-tat retaliation in kind, but rather to the historic notion that an attack on the nation may precipitate response by all available means, (within limits of proportionality,

93. *See* The White House, *supra* note 35, at 8.

94. *See* MINEHART, *supra* note 59, at 68.

95. *See, e.g.*, Computer Fraud and Abuse Act of 1986 § 2(d), 18 U.S.C. § 1030(a) (1994) (creating new computer-related fraud offenses).

etc.). How, where, and in what form have we established such a doctrine as it relates to information?

This section of the discussion has led to some disturbing conclusions. Specifically, in the absence of solid answers to the two seminal questions, it appears that it is not possible to create any meaningful I&W regime for national information protection under the purview of any organization or group of organizations. Further, formulating such answers seems to fall outside the bounds of competence or authority of any current government organization.

At its core, this gloomy projection rests upon the impression that the development of an I&W effort broadly embracing domestic equities would most probably require a greater degree of visibilty into the details of the civil information base than has ever been maintained. Not surprisingly, the commercial stakeholders have been reluctant to provide such unconstrained access; the government has not made a case for its right to demand it, nor has the government yet demonstrated the compelling need to stimulate voluntary participation at the required level. We need a new approach.

VIII. DIGGING OUT OF THE HOLE

The required sense of need might emerge from one of only two conditions: desperation or opportunity. Desperation, or a clear and present danger of real and truly painful losses due to information attack, is the approach implicitly favored by those who constantly point to threats of various kinds.[96] Unfortunately, these marketing efforts have only enjoyed limited success to date.[97] Industrial leaders make business-based decisions and take actions within their ability to protect themselves, consistent with their own sense of costs and benefits.[98] Even to this day, some business leaders remain skeptical about the threat, and of the rest, a considerable fraction questions the government's ability to provide anything useful for them individually, even if the government did have the benefit of full and timely knowledge of industrial "information events."[99] The irony is that the skeptics may be correct, but for a different reason. Without the needed inputs to the I&W process, the output cannot be satisfactory. In other words, by their own actions (or inactions), industries can virtu-

96. *See, e.g.*, THE PRESIDENT'S COMMISSION ON CRITICAL INFRASTRUCTURE PROTECTION, *supra* note 17, at x.

97. *See* CENTER FOR STRATEGIC AND INTERNATIONAL STUDIES, *supra* note 41, at 4.

98. *See id.*

99. *See id.*

ally guarantee that their assessment of governmental impotence will become a self-fulfilling prophecy. This leads us to explore the other approach to breaking the information-sharing logjam: recognition of opportunity for personal or organizational benefit.

IX. ENLIGHTENED SELF-INTEREST, AND THE BEGINNINGS OF NATIONAL INFORMATION POWER

The need exists to promote extensive information sharing and to establish a beneficial role for government to justify industrial contributions to that sharing. Even more than that, however, we must respond to the underlying opportunities and imperatives of the Information Age at a strategic level. This could all be achieved by the creation of a national information regime which would go beyond simply protection to some range of positive measures calculated to enhance America's informational position, at home and globally, on a broad and sustained basis.

What is the practical value of America's dominance in the global market of informational goods and services? What opportunities exist for a confluence of public and private interests? What outcomes strengthen those interests, both mutually and separately? Detailed answers to these questions lie outside the scope of this Article. In general, however, the intellectual objective can be captured in a single sentence, from which all else can be logically extrapolated: "What are the Vital National Interests of the United States in the Information Age?"

Absent such an understanding and declaration, we cannot reliably distinguish between individual violations, which may be resolved by domestic processes of criminal and civil law enforcement, and strategic threats to national security. Even more important is the notion that one should seek not just to protect one's vital interests, national or otherwise, but one should aspire to advance them as well. This is where we move beyond the mechanistic *deus ex machina* of dueling hardware and ascend to the level of strategic ideation (which was the real objective from the beginning).

The answer to the above question offers, in principle, the first practical path toward the universally acknowledged desired outcome. A goal of fundamental information sharing on a basis of genuine partnership and mutual benefit should achieve the advancement of total national interests. Any acceptable and comprehensive answer to this question would necessarily engage the leading experts and theorists of traditional national security, leading researchers and aca-

demics of the scientific sector, and industrial and business leaders of the information technology community. Even at that stage, the answer would only exist in draft form. However, it could serve as a point of departure for the necessarily very broad and very public debate that must ensue.

Although it certainly need not be advertised nor conducted as such, the debate would be tantamount to a public referendum on national security and the role of government for the foreseeable future, a move that may well be overdue. In an environment in which 59% of the public lists as the biggest threat to the country in the future "big government," compared with "big business" at only twenty-five percent,[100] what are the people really saying? It seems clear that when any person or organization loses the approval and confidence of his/her associates, there is a sense that one is no longer contributing anything of value to the relationship. Why would anyone want to maintain, much less expand, a relationship which provides no value? When and if the people come to recognize and value the information important to them in their daily lives, and government undertakes to protect it with their support and cooperation, it will at least be a step in the right direction. One thing, at least, is quite obvious: unless and until there is clear consensus on the first two questions on Figure (1)—in other words, until our vital national informational interests can be defined—effective I&W of attacks against those interests cannot be achieved. Such efforts will founder for lack of the needed information-sharing and dissemination agreements, plans, and protocols.

It may be possible to see all this in a common context. Fear of big government and reluctance to share precious information with that bogeyman are mutually supporting phenomena. The inability of government to relate to the needs and concerns of its leading economic citizens—now and in future, the information technology sector—exacerbates the division between the public and private sectors, further inhibiting meaningful communication. The lack of communication increases the risk that the products and services government provides will fall short of the perceived need, thus appearing to confirm the negative impressions held by its critics.

All those who share a belief in the potentially positive role of good government,[101] and have concerns for the growing needs, as well

100. *American Values: Three Decades of Change*, WASH. POST, Dec. 17, 1998, at A18.

101. Which is *not* necessarily synonymous with "big government."

as unmet opportunities, of the Information Age, should see a logical marriage of interests in the acknowledgement of national information power as a component of America's strength.

X. CONCLUSION

The onus is initially on the government, as it must be. In the course of formulating its strategy for the Information Age, government must make a convincing case for the informational input it requires from private sources. In so doing, government must not only indicate what information it needs and how it intends to use that information, it must also demonstrate convincingly its appreciation for the sensitivity of proprietary and personal information. This level playing field is needed to assuage the fears of those who might be concerned about losing competitive advantage. For the commercial participants, this initiative should be framed not so much as a burden, but rather as an opportunity to act in their own self-interest. However, this will only be believed and acted upon once government demonstrates it can and will be a wise steward of sensitive information, as well as an effective advocate for industry's needs. In the same spirit, government must be very thoughtful in selecting its mouthpiece, the interface between the totality of the domestic economy and the entire breadth of government. Selection of any narrowly focused organization to perform this vital function would clearly be unwise.

To build on the momentum of this expanded exchange of information, and hopefully, of ideas and plans, we must pursue progress toward framing the nation's vital national informational interests as a high priority. It should be expected that this process will take time to progress through several iterations in the course of its preparation. It will not be a project for the intellectually limited or the weak of heart.

As the goals, priorities and concerns of the nation take shape on paper and in circles of influence, the proper size and shape of the government's organizational response to those needs should become visible concomitantly. The model may turn out to resemble a combination of several existing departments into an enormous and far-reaching single entity, as some leading thinkers have suggested.[102] At the other end of the scale, very loosely structured and adaptive vir-

102. *See* Stephen Cambone, *A New Structure for National Security Policy Planning* (visited Mar. 1, 1999) <http://www.csis.org/pubs/newstructforwd.html>.

tual organizations, themselves heavily based on information technologies, are being examined as a means to achieve advanced information sharing and decision-aiding in response to crisis.[103] Between these approaches lies a range of other options. One thing appears clear, however: preservation of the status quo runs the risk of continuing the downward trends of the perceived value and relevance of government in the eyes of the public since the 1960s.[104]

Another point that cannot be forgotten is that beyond providing an optimally efficient interface for the receipt of private information, the government's organizational efforts must pay close attention to the ways and means for it to disseminate relevant, timely and ultimately valuable information to the society it exists to serve. This must occur not just in response to threat of attack, but in routine maintenance of "information wellness," to coin a phrase. Without that quid pro quo understanding, clearly established at the outset and reinforced at every turn, there is no reason to believe any organizational model could hope to work.

Once again it must be pointed out that in the context of any comprehensive national information strategy, we must seek opportunities to project America's informational power offshore in pursuit of our vital national interests, informational and otherwise. This is not a veiled reference to offensive IW, but rather to the whole range of national policy influences available through technology transfer, export, intergovernmental information-exchange agreements, trade policy, and other means. Declaratory policies will be needed to document the status of the specified informational equities as being among our vital national interests, and also to provide a visible strategic framework to support the furtherance of America's informational policies and projects.

When all the foregoing has been achieved, or is at least well along, we will have stepped up to full acknowledgement of that which has at least implicitly been recognized already. National information power is a component of America's national strength and a precious resource to be protected as a vital national interest. The opportunity is before the government and the rest of the nation to recognize that the character of the Information Age is so closely aligned with the traditional strengths of the United States and its people, that it is as if the new Age were made for us. Ingenuity, initiative, imagination, in-

103. *See* Brian Sharkey, *Project Genoa* (visited Mar. 8, 1999) <http://dtsn.darpa.mil/iso/programtemp.asp?mode=285>.

104. *See American Values: Three Decades of Change*, *supra* note 100.

vention . . . these strengths abound in us as a people. For better or worse, the technologies spawned by their application will be a dominant force in directing and pacing the progress of human civilization, probably until long past the lifetime of anyone alive today. If we are to secure that future, and our place within it, the time to act is now, not as "the government" or as "the information technology industry sector," but as a nation and a people. The choice is ours, and the clock is ticking.

Author's Note: The International Dimension

This Article attempts to identify and characterize a few of the many important issues of the Information Age, focusing on the opportunities and imperatives for the United States. To those readers more accustomed to—and interested in—rich and rigorous debate of the fine points of international law within these pages, I (a legal layman) offer my apologies. However, I would suggest that although the emphasis of this Article is largely domestic, the nature of the "information revolution" is such that an increasingly international perspective is unavoidable. By challenging traditional notions of territoriality and sovereignty, the Information Age demands attention by legal and public policy scholars.

What some might consider the over emphasis of domestic versus foreign content of this piece does not reflect either disinterest or disregard for international aspects of information attack and protection on the part of the author or editors. However, it must be said that to date, the expenditures of intellectual and other forms of capital in this area steeply favor the United States, notwithstanding the serious efforts of some other nations at present to catch up.

Beyond the disclaimer above, in a journal such as this it is both appropriate and necessary to provide at least an overview of the principal issues guiding and pacing the international political and legal debate in the field. Accordingly, the following *very* cursory overview is offered, in the hopes that it might serve as a primer for further study, and perhaps also the outline of a future, rigorous treatment of this crucial topic in the *Duke Journal of Comparative & International Law*.

THE BIG PICTURE

Within the larger subject of "Information Warfare" (as developed in the accompanying article), practicable international cooperation and agreement is most needed in four areas:[105]

1. Application and/or adaptation of existing definitions, usages and understandings of the material world into a newer, "informational" format.[106]

105. This discussion is drawn generally from WALTER GARY SHARP, CYBERSPACE AND THE USE OF FORCE (1999), LAWRENCE T. GREENBERG ET AL., INFORMATION WARFARE AND INTERNATIONAL LAW (1988), THE WHITE HOUSE, A NATIONAL SECURITY STRATEGY FOR THE NEW CENTURY (1998), and the author's personal experiences, including extensive negotiations and coordination with foreign governments in this field.

2. Agreement on technical formats, standards, and protocols for interoperability of Information Assurance technologies, to include encryption.[107]

3. Improved cooperation in detecting, investigating, and prosecuting information attackers across jurisdictional boundaries.[108]

4. Some international players (or perhaps "wannabees"?) in the IW world have advocated regulatory regimes of various kinds, intended to limit or outlaw all types of information attack.[109] The question of whether it may or may not be in the best interests of the United States to accede to these proposals lies outside the scope of this paper. We ignore such initiatives at our peril. As such, we must "engage" in this area, regardless of the outcome desired.

These few topics represent just the beginnings of the required effort and understanding in the international dimension of the nascent field of "Information Warfare," as practiced by many around the globe, and in many guises.

---

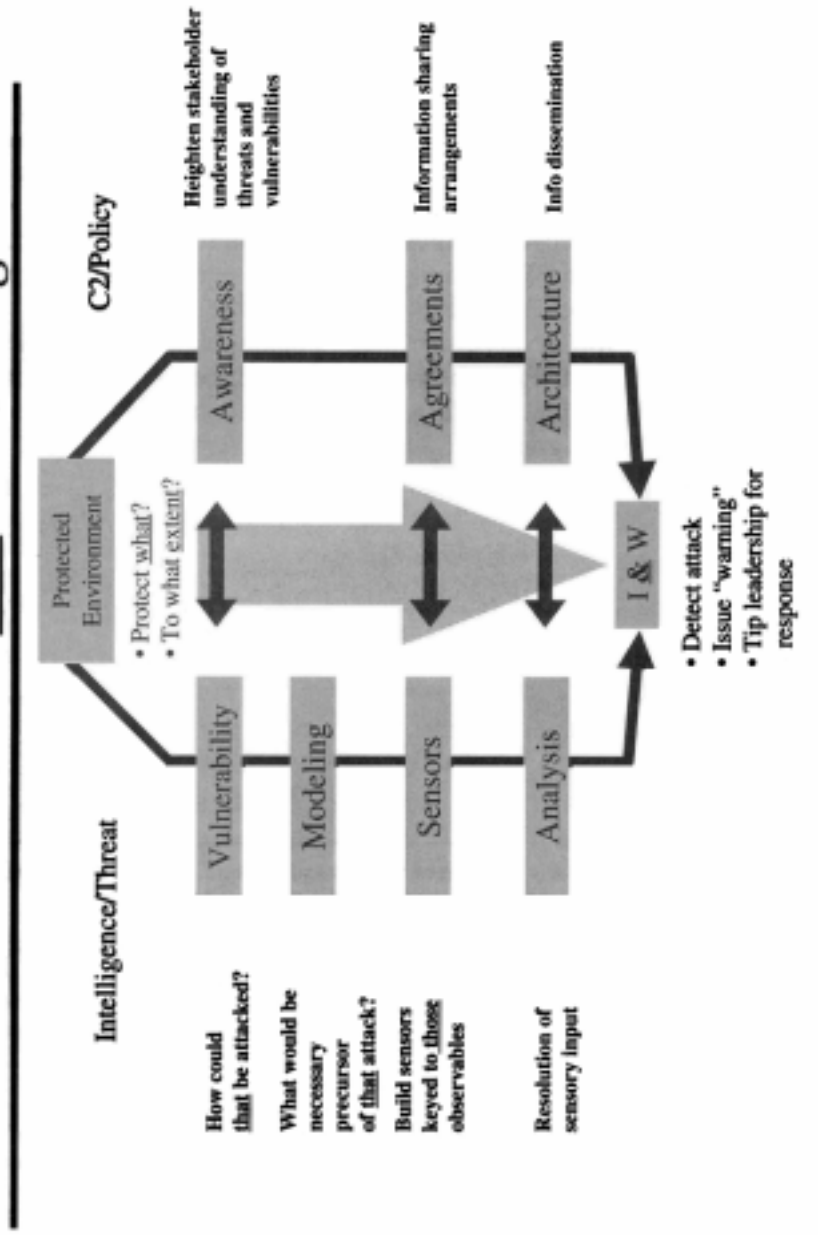
106. One example of this is the need to reevaluate "force," "armed attack," and "self-defense" as defined in the articles two and fifty-one of the United Nations Charter. Sharp's book examines this particular question in detail. *See* SHARP, *supra* note 105.

107. The encryption debate alone requires—and deserves—a small book to develop the various positions adequately. For our purposes here, suffice it to say that to date, no proposal put forward in the international arena has achieved broad acceptance. Therefore, the underlying protective regimes remain a patchwork of dissimilar and generally non-interoperable systems, providing uneven security.

108. This area of need has shown some, albeit limited, progress. That is, the U.S. Department of Justice is working with national and multi-national organizations. *See* THE WHITE HOUSE, *supra* note 105, at 16-18. However, characteristics of the international extradition process permit some states to shield apparently "private" individuals employed as state actors, while in other cases, the portrayal of an information-attack prosecution as a "political crime" is an effective block to extradition. *See* United Nations Crime and Justice Information Network, *Model Treaty* (visited April 24, 1999) <http://www.ifs.univie.ac.at:80/uncjin/unrule17.html>; *see also* JOINT CHIEFS OF STAFF, INFORMATION ASSURANCE: LEGAL, REGULATORY, POLICY AND ORGANIZATIONAL CONSIDERATIONS, 6-4 (3d ed. 1997).

109. *See* SHARP, *supra* note 105, at 5-6.

FIGURE 1: INDICATIONS AND WARNING MODEL[110]



110. *See* Gravell, *supra* note 81.