IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Hershey PA 17033-1117, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITP4267

Defending Infrastructures Against Information Warfare

Vernon Stagg and Matthew Warren
Deakin University, School of Computing and Mathematics, Australia, {vstagg, mwarren}@deakin.edu.au

ABSTRACT

Information Infrastructures are an eclectic mix of open and closed networks, private and public systems, the Internet, and government, military, and civilian organizations. Significant efforts are required to provide infrastructure protection, increase cooperation between sectors, and identify points of responsibility. The threats to infrastructures are many and various, and increasing daily: Information Warfare, hackers, terrorists, criminals, activists, and even competing organisations all pose significant threats that cannot be sufficiently dealt with using the current infrastructure model. An enhanced National Information Infrastructure model is presented that provides for greater defence against threats such as Information Warfare.

INTRODUCTION

Information Infrastructures are an eclectic mix of open and closed networks, private and public systems, the Internet, and government, military, and civilian organizations (Anderson, 1998; Aberg, 2000). They are important vehicles for the generation of wealth, and can influence the power and capability not only of organizations, but also nations (Westwood, 1996). As the integration of technology into everyday life increases, the reliance on the integrity, availability, and reliability of infrastructures grows accordingly (Luiijf, 1999).

A problem with many infrastructures is that they are excessive, continually growing, regularly reconfigured and reengineered, and lack suitable staff and resources to oversee them (Brock Jr, 2000). With the growing trend for private ownership of critical infrastructure elements, responsibility shifts from government to private organizations and raises issues of who is involved, what their responsibilities and requirements are, and determining a focal point of authority for infrastructure control (PCCIP, 1997b; Waltz, 1998; Cordesman, 2000).

Efforts are required to improve infrastructure protection, increase cooperation between sectors, and identify points of responsibility (Samson, 2000). Based on the threat of Information Warfare, we present an approach that addresses these issues by considering the vertical and horizontal levels of infrastructure, focusing on non-critical elements within the Information and Communications sector.

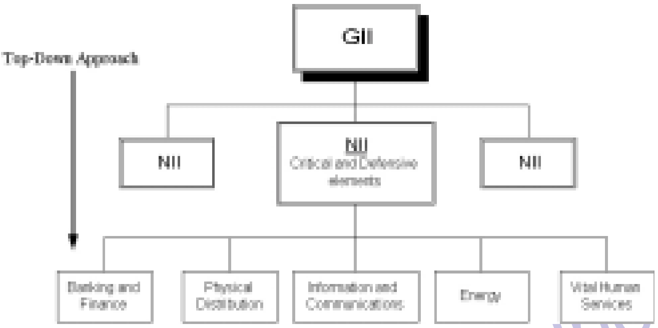
NATIONAL INFORMATION INFRASTRUCTURE

A National Information Infrastructure (NII) has been defined as *a system of high-speed telecommunications networks, databases, and advanced computer systems that make electronic information widely available and accessible* (OMB, 1995). It has also been described as *an inchoate, multidimensional phenomenon, a turbulent and controversial mix of public policy, corporate strategies, hardware and software that shapes the way consumers and citizens use information and communications* (Wilson, 1997).

An NII is considered the physical and virtual backbone of an information society (Cobb, 1998) and is an evolving entity comprised of public and private services, operating as a complex, dynamic system. The United States Presidential Critical Infrastructure Protection Commission (PCCIP) identified five sectors that comprise an NII (PCCIP, 1997a): Information and Communications; Banking and Finance; Energy, including power, oil, and gas; Physical Distribution; Vital Human Services.

A Global Information Infrastructure (GII) is the collective linking of existing NII's (NRC, 1996) whilst within each NII exists a number of parallel infrastructures. The Defence Information Infrastructure (DII), globally links military functions such as mission support, command and control, and intelligence computers through a variety of methods (JCS, 1996). A Critical Information Infrastructure (CII), considers the essential elements of a nation, and implements special hardening, redundancy, recovery, and other protection mechanisms (Anderson et al., 1999; Nash and Piggott, 1999). Figure 1 shows the current infrastructure hierarchy.

Figure 1: Infrastructure levels



INFRASTRUCTURE PROTECTION

Current infrastructure developments focus on top-down approaches that are often unwieldy, difficult to manage, averse to cooperation, and lacking in coordination. Aside from the obvious technical, legal, and financial aspects involved, there are also numerous misunderstandings between organizations and government over what protecting the NII entails (Caloyannides, 2000). An interesting dichotomy arises with organizations wishing to avoid and prevent attacks, whilst governments want to detect, trail, and then prosecute the attackers. This raises numerous liability, information sharing, and vulnerability issues that have been plaguing infrastructure protection since day one.

The finance sector has long understood the necessity of preserving customer confidence and the integrity of business information. The awareness of information security, implementation of policy, and protective measures is especially strong within this sector (Mitchell et al., 1999). The concern within other sectors is that many organizations do not yet realise the sheer scale of the steadily growing threats they face. The approaches they take to protective measures are often closed, secretive, and compartmentalised in nature, and do not take into consideration the impact their systems have on other elements of infrastructure (Cordesman, 2000).

Infrastructure Attacks

The last few years have seen a steady rise in the number and type of attacks against infrastructures, which have had significant impact

This paper appears in *Issues and Trends of Information Technology Management in Contemporary Organizations,* the proceedings of the Information Resources Management Association International Conference. Copyright © 2002, Idea Group Inc.

upon organizations and nations. The nature of these attacks has also changed, from harmless and annoying pranks to menacing and malicious concerted efforts. The attackers themselves have also become more sophisticated and coordinated, often with clear political, social, environmental, religious or financial objectives in mind. The resultant cost, time, and effort required in recovering after an attack can be enormous, and without suitable recovery methods in place, many organizations may not be able to face the challenge.

In 2000 a spate of distributed denial-of-service attacks caused massive disruptions for a number of prominent online companies including Amazon, eBay, and Yahoo. The loss of business has been estimated at over $US1 billion dollars (McCombie and Warren, 2000). Although not fundamentally new in approach, these attacks achieved an effect where hundreds, even thousands, of systems would attack a particular system.

The Love Bug virus swept the world in 2000, affecting over 55 million computers. Numerous companies, government organizations, and educational institutions were forced to shut down their mail servers, many for up to one week. The resultant financial loss of this attack has been mooted at over $US8 billion dollars (Erbschloe and Vacca, 2001) More recently, viruses such as Code Red, Nimda, SirCam, and BadTrans have had similar devastating effects.

Wik (2000) pondered the enormous financial cost that would have occurred had the telecommunications hub and conduits been damaged during the 1993 attack on the World Trade Center (WTC). Theory became reality in September 2001 when the WTC was destroyed by terrorist attacks. A cost close to $US five billion has been estimated just for the financial services infrastructure (Williams and Kennedy, 2001). This figure could have been much higher had it not been for the efforts of organizations in securing their infrastructures during recent years (Rountree, 2001).

Computer hackers, routing through networks operated by China Telecom and servers in the US, gained access to a California power system. Although there was no threat to the power grid, the hackers came close to accessing critical parts of the system and could have disrupted the movement of power (Vatis, 2001).

Attacks against infrastructures are relatively new, shifting the threat focus from low-level attacks on individual, system-level elements to high-level system-wide attacks (Anderson, 1998). These types of network-centric attacks are considered to be a version of an emerging issue known as Information Warfare (Alberts, 1999).

Information Warfare

Information Warfare is still a relatively new issue, not clearly understood in the commercial sector, yet more than just hype or a buzzword (Gershanoff, 2000). Originating from the military sector, a certain amount of disparity exists between the various definitions and concepts of Information Warfare developed amongst various military and defence departments (Gray et al., 1997). Derived from various sources, Information Warfare can be considered as *actions taken to affect a competitor's information, information systems, and information-based processes whilst protecting one's own information, information systems, and information-based processes. These actions may be directed at an individual, a corporation or multinational body, and may occur during peacetime or conflict between nations or societies* (Arquilla and Ronfeldt, 1993; Schwartau, 1994; JCS, 1998).

When considering the Information Warfare threat to an infrastructure, we need to determine the potential adversaries, their motives, and their objectives. Such adversaries could include nation states, criminals, terrorists, hackers, hacktivists, spies, ideological and cultural adversaries, insiders, and competing organizations (Brand, 2000; Luiijf, 2000). By identifying the objectives and motives of attackers, it is possible to qualify the potential effort, skill, and expense the attacker is willing to invest in exploiting a vulnerability (Anderson, 1998).

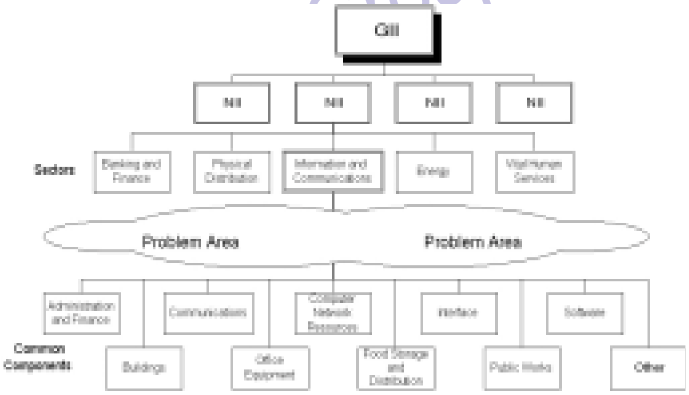
Information Warfare presents significant challenges to those responsible for developing policy regarding the protection of the NII (Ryan and Ryan, 1996). In 2000, a Forrester report found that 89% of companies surveyed saw Information Warfare as a possible risk, with 6% saying they had first-hand experience of such an attack (Prince et al., 2000). Whilst organizations may not be able to defend against large-scale attacks against the NII, they are more likely to successfully defend against attacks on smaller more constrained infrastructures. A report by the Defense Science Board (DSB, 1996) stressed that to understand the Information Warfare process and identify Information Warfare attacks will require a determined effort to collect, consolidate, and synthesize information from various infrastructure elements.

AN ENHANCED NII MODEL

The NII is a diverse and eclectic mix of systems, networks, people, and processes that often cut across work-practices, departments, functions, and organizational borders (Braa and Rolland, 2000). Critical and Defensive Infrastructures are interconnected and interoperable in such a way that they constitute most of what makes up an NII (AGD, 1998). As organizations continue to integrate and utilise information and communications technologies into their operations, there is a significant rise in the reliance on the dependability and reliability of the NII.

The issues of infrastructure protection, Information Warfare threats, attacks, and responsibilities are becoming harder to deal with for organizations that are part of, or connected to, the current infrastructure model. Infrastructure protection cannot simply be addressed by compartmentalised solutions that have derived from methods and practices out of touch, and out of date, with today's sophisticated and complex technologies. Each sector of the NII has a common core component of elements, along with specific requirements for security and protection (Ware, 1999; Mitre, 2001) seen in Figure 2.

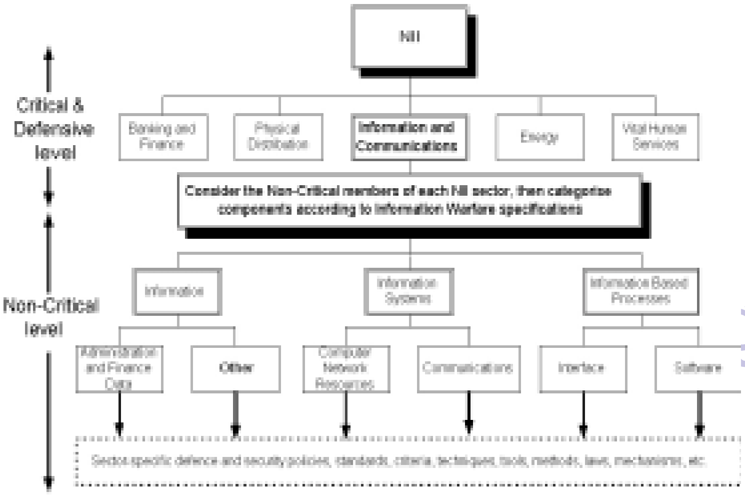
Figure 2: Current infrastructure model



The "problem area" of Figure 2 represents the growing number of non-critical and non-military elements that are becoming part of an NII. Non-critical level (NCL) elements include medium-to-large businesses, large corporations, and other organizations that may be directly or indirectly related to critical elements of infrastructure, be adversely affected by infrastructure attack, or have significant involvement in information and communications technology. With a focus on the Information and Communications sector, Figure 3 outlines the enhanced model.

The three main categories of this model are based on the focal elements of Information Warfare: information, information systems, and information-based processes. This will help categorise infrastructure elements and enable clear and decisive methods of protection based against potential Information Warfare threats. By recognising the important horizontal and vertical relationships that exist within the NII model, along with the interplay that occurs between all sectors (Porter, 1990; Ware, 1999), security can be increased not only in

Figure 3: Enhanced model within ICT sector


NII
Critical & Defensive level
Banking and Finance
Physical Distribution
Information and Communications
Energy
Vital Human Services
Consider the Non-Critical members of each NII sector, then categorise components according to Information Warfare specifications
Non-Critical level
Information
Information Systems
Information Based Processes
Administration and Finance Data
Other
Computer Network Resources
Communications
Interface
Software
Sector-specific defence and security policies, standards, criteria, techniques, tools, methods, laws, mechanisms, etc.

depth (strength in numbers), but also by breadth (additional capabilities) (NATO, 1997; Ackerman, 2001; Kewley and Lowry, 2001).

By determining the NCL elements we can identify crucial support functions that flow vertically (control and cooperation), horizontally (strategy, structure, and rivalry), or both ways (Viitamo, 2001). The efforts in protecting the horizontal elements can consist of methods, policies, and procedures relevant to that sector; many of these will already be in place. The vertical levels can be strengthened with applicable security measures, such as strong encryption, secure channels, redundancy, and recovery systems for the Information and Communications sector.

At the NCL many of the entities involved will have strict rules and procedures in place for information collection, management, distribution, retention, and deletion. These procedures can provide a viable framework for Information Sharing and Analysis Centers (ISAC) to work within (USDOC, 2001). A common hurdle to ISAC's is the unwillingness of organizations to share sensitive information with others (Brock Jr, 2000), especially on a large scale. The proposed model would enable information to be filtered from the horizontal elements to develop statistics and analysis that could then be shared among the vertical levels. This information could also be combined with other infrastructure sectors, along with federal resources, to better protect the NII (Willemssen, 2000).

CONCLUSION

One of the significant differences between offence and defence is that defence is required to ensure against all threats and vulnerabilities, while a successful offence need only exploit one of these (Anderson et al., 1999). This situation is further exacerbated by the continual growth in performance and power of information and communications technologies, the availability and accessibility of information and tools (Stagg and Warren, 2000), and the relative low costs that enable almost anyone to launch an attack against an infrastructure (Luiijf, 1999). On the other hand, the cost to detect, repair, recover, respond, research, and retaliate against such attacks is significantly higher (West-Brown and Kossakowski, 1999).

It is important to realise the growth of infrastructures presents shared risks, which in turn creates shared responsibilities for protection (West-Brown and Kossakowski, 1999). Organizations must work together to safeguard their infrastructure networks, which will further help strengthen the NII. A mass attack on an NII resulting in the total shutdown of systems is not likely without a high level of planning, coordination, skilled personnel, and funds (Cobb, 1997). The possibility of attack on elements of the NII is much more feasible with minimal outlay of technology, funds, and personnel required.

The model presented here focuses on the sectors as defined by the PCCIP and considers the horizontal viewpoints at each level. By addressing the issues inherent in a top-down process, the model provides for integration and cooperation between horizontal elements within each sector to allow for additional capabilities. At the vertical level, greater recognition of responsibilities and requirements is addressed, strengthening the overall model to provide enhanced defences against threats such as Information Warfare.

REFERENCES

Aberg, D. (2000), "A Business Model for the Knowledge-Based Economy", Final Year Project, South Bank University.

Ackerman, R. K. (2001), "Jointness Defines Priorities for the Defense Department's Global Grid" in Signal, Vol 55 No 8,pp. 23-29.

AGD (1998), "Protecting Australia's National Information Infrastructure", Report, Attorney-General's Department.

Alberts, D. S., Garstka, J.J., and Stein, F.P. (1999), Network Centric Warfare: Developing and Leveraging Information Superiority, CCRP Publication Series.

Anderson, K. (1998), "Intelligence-Based Threat Assessments for Information Networks and Infrastructures", White Paper, Global Technology Research Inc.

Anderson, R. H., Feldman, P. M., Gerwehr, S., Houghton, B. K., Mesic, R., Pinder, J., Rothenberg, J. and Chiesa, J. R. (1999), "Securing the U.S. Defense Information Infrastructure: A Proposed Approach", Report MR993, RAND Corporation.

Arquilla, J. J. and Ronfeldt, D. F. (1993) "Cyberwar is Coming!", Comparative Strategy, Vol 12 No 2, pp. 141-165.

Braa, K. and Rolland, K. (2000), "Horizontal Information Systems: Emergent Trends and Perspectives", in R. Baskerville, Stage, R. and DeGross, J. (Ed.), Organizational and Social Perspectives on Information Technology, Kluwer Academic Publishers, pp. 83-102.

Brand, G. (2000), "Protecting the United States Against Information Warfare", Strategy Research Project, Army War College.

Brock Jr, J. L. (2000), "Critical Infrastructure Protection: Challenges to Building a Comprehensive Strategy for Information Sharing and Coordination", Testimony, United States General Accounting Office.

Caloyannides, M. A. (2000) "Encryption Wars: Early Battles", IEEE Spectrum, Vol 37 No 4, pp. 37-43.

Cobb, A. (1997), "Australia's Vulnerability to Information Attack: Towards a National Information Policy", Working Paper, Strategic and Defence Studies Centre, Australian National University.

Cobb, A. (1998), "Thinking About the Unthinkable: Australian Vulnerabilities to High-Tech Risks", Research Paper, Foreign Affairs, Defence and Trade Group.

Cordesman, A. H. (2000), "Defending America: Redefining the Conceptual Borders of Homeland Defense", Final Draft, Center for Strategic and International Studies.

DSB (1996), "Report of the Defense Science Board Task Force on Information Warfare - Defense", Report, Office of the Under Secretary of Defense for Acquisition and Technology.

Erbschloe, M. and Vacca, J. R. (2001), Information Warfare, McGraw-Hill.

Gershanoff, H. (2000) "Information What?", Journal of Electronic Defense, Vol 23 No 12, pp. 10.

Gray, J. V., Barlow, W. J., Barnett, J. W., Gerrity, J. L. and Turner, R. D. (1997), "Information Operations: A Research Aid", Institute for Defense Analyses.

JCS (1996), "Joint Doctrine for Command and Control Warfare", Joint Pub 3-13.1, Office of the Joint Chiefs of Staff.

JCS (1998), "Joint Doctrine for Information Operations", Joint Pub 3-13, Office of the Joint Chiefs of Staff.

Kewley, D. L. and Lowry, J. (2001), "Observations on the Effects of Defense in Depth on Adversary Behavior in Cyber Warfare", Proceedings of the IEEE Workshop on Information Assurance and Security, US Military Academy, West Point, NY.

Luiijf, E. A. M. (1999), "Information Assurance and the Information Society", Conference on European Institute for Computer Anti-Virus Research.

Luiijf, E. A. M. (2000), "Information Assurance Under Fire", SMI Conference on Information Assurance and Data Security, London.

McCombie, S. and Warren, M. J. (2000), "A Profile of an Information Warfare Attack", Technical Report, Deakin University.

Mitchell, R. C., Marcella, R. and Baxter, G. (1999) "Corporate Information Security Management", New Library World, Vol 100 No 5, pp. 213-227.

Mitre (2001) "Cyber Resource Center: Infrastructure Sectors" The MITRE Organization; http://www.mitre.org/research/cyber/sectors/index.html

Nash, C. L. and Piggott, C. K. (1999), "'Help! I've Been Attacked!' Researching Ways to Recover a Command and Control System Following an Information Warfare Attack", 1999 Command and Control Research and Technology Symposium, USA.

NATO (1997), "Change 1 Allied Joint Doctrine", Doctrine, North Atlantic Treaty Organisation.

NRC (1996), The Unpredictable Certainty: Information Infrastructure Through 2000, National Academy Press.

OMB (1995), "NII Security: The Federal Role", Report, National Information Infrastructure Security Issues Forum, Office of Management and Budget.

PCCIP (1997a), "Critical Foundations: Protecting America's Infrastructures", President's Commission on Critical Infrastructure Protection.

PCCIP (1997b), "Critical Foundations: Thinking Differently", Report Summary, President's Commission on Critical Infrastructure Protection.

Porter, M. (1990), The Competitive Advantage of Nations, NY, Free Press.

Prince, F., Howe, C. D. and Voce, C. (2000), "B2B Information Warfare", Report, Forrester Research.

Rountree, D. (2001) "Disaster's Effect on Financial Systems Measured", Bank Technology News, Vol 14 No 10, pp. 7.

Ryan, D. J. and Ryan, J. C. H. (1996) "Protecting the National Information Infrastructure Against Infowar", Colloquy, Vol 17 No 1, pp. 21-25.

Samson, V. (2000), "Defense Against Information Warfare", in J. Anderson (Ed.), Passing the Torch, 77-79.

Schwartau, W. (1994), Information Warfare: Chaos on the Electronic Superhighway, NY, Thunder's Mouth Press.

Stagg, V. and Warren, M. J. (2000), "Computer Hacker Information Still Available on the Internet!", 1st Australian Information Security Management Workshop, Australia, Deakin University.

USDOC (2001), "Commerce Secretary Mineta Announces New Information Technology Information Sharing and Analysis Center", Press Release, United States Department of Commerce.

Vatis, M. A. (2001), "Cyber Attacks During the War on Terrorism: A Predictive Analysis", Report, Institute for Security Technology Studies, Dartmouth College.

Viitamo, E. (2001), "Cluster Analysis and the Forest Sector - Where Are We Now?", Interim Report, International Institute for Applied Systems Analysis.

Waltz, E. (1998), Information Warfare: Principles and Operations, Boston, Artech House.

Ware, W. H. (1999), "The Cyber Posture of the National Information Infrastructure", Report MR-976-OSTP, RAND Corporation.

West-Brown, M. and Kossakowski, K. P. (1999), "International Infrastructure for Global Security Incident Response", Draft Report, CERT Coordination Center, Carnegie Mellon University.

Westwood, C. J. (1996), "Military Information Operations in a Conventional Warfare Environment", Paper Number 47, Air Power Studies Centre.

Wik, M. W. (2000), "Revolution in Information Affairs: Tactical and Strategic Implications of Information Warfare and Information Operations", 3rd Association of Old Crows International Electronic Warfare Conference, Switzerland, Defence Materiel Administration.

Willemssen, J. C. (2000), "Critical Infrastructure Protection: Comments on the Proposed Cyber Security Information Act of 2000", Testimony, United States General Accounting Office.

Williams, F. and Kennedy, M. (2001) "Technology, Planning Came Through After the Attack", Pensions and Investments, Vol 29 No 20, pp. 4.

Wilson, E. J. (1997), "The What, Why, Where and How of National Information Initiatives", in B. Kahin and Wilson, E. J. (Ed.), National Information Infrastructure Initiatives: Vision and Policy Design, MIT Press, Cambridge, MA, pp. 22.