INFORMATION WARFARE IN THE CONTEXT OF SECURITY-RELATED ISSUES
Where could we go from here?

Dr W. Stein
Forschungsgesellschaft für Angewandte Naturwisschenschaften, Germany

ABSTRACT

The goal of this paper is to find orientations, helpful illustrations as well as definitions, and perhaps critical factors that can help to open a gate for more cooperation in research, development, and education in the area of today's information security-related issues. This area includes Information Security (INFOSEC), Information Warfare (IW) and Critical Infrastructure Protection (CIP). One can find many traditional factors impeding understanding and cooperation that may include different term s and definitions, economic competition, and interests of national security. It turns out that there exists a common problem area in the context of information warfare, with challenges for a new level of cooperation in science, engineering, and education.

INTRODUCTION

It has been well accepted meanwhile that the information and communications sector with its information systems and infrastructures is central to all other sectors of modern societies, indeed to essentially every aspect of national and international functioning. Attacks on information systems are already a fact of life in the information age. Almost daily, hackers explore vulnerabilities in our global information infrastructures and in computer systems. Various ideological and cultural adversaries - individuals, guerrilla and terrorist groups - are on the way to discover 'Information War' as a major means to disrupt operations in government, military, and corporate sectors. As a consequence, information operations (Info Ops) have changed from conceptual thinking into reality and are on the way to become a hot topic, in military areas, in government areas, and in corporate areas. Governments, armed forces, and society as a whole need to be prepared, in order to counter these information threats and attacks. But currently there seems to exist a lack of awareness about information security and infrastructure vulnerabilities.

Although a small portion of these attacks result in significant loss or damage, the vast majority of them result in little or no damage - the crime equivalents of trespassing, public nuisance, minor vandalism, and petty theft. It has been estimated that more than 90 percent of these attacks are perpetrated using available tools and techniques (based upon incidents reported to CERT), that only 1 attack in 20 is noticed by the victim, and that only 1 in 20 gets reported (these last two statistics were a result of a Defense Information Systems Agency (DISA) study and similar rates have been reported by others). However, it appears that reporting rates may be on the increase. As we can see, there is (nearly) nothing new in this area. As a consequence, the interest in securing information, computers, and networks arose early and the first report dates back to 1970 [24]. After the emergence of the Critical Infrastructure Protection (CIP) program during the last five to ten years, we are faced now with three security-related areas with interrelated challenges: Information Security (INFOSEC), Information

Warfare (IW) and Critical Infrastructure Protection (CIP) [1/ 18/ 23/ 24]. While screening the security-related issues, we can find various terms, sometimes redundant definitions, and overlapping areas (different between communities, nations etc.), e.g. security, assurance, and protection of information and/or infrastructures; as well as information warfare and information operations [23]. These heterogeneous and diverse components can make cooperation difficult or even impossible. Figure 1 shows the areas of Information Warfare (IW), Information Security (INFOSEC), and Critical Infrastructure Protection (CIP) as well as their potentially interrelated sub-areas. Although the three areas have many common subjects (e.g., in problem areas, methods, tools; partly using the same infrastructures, having similar research and development goals, using similar analysis frameworks etc.) the degree of cooperation in research and development seems to be very limited.

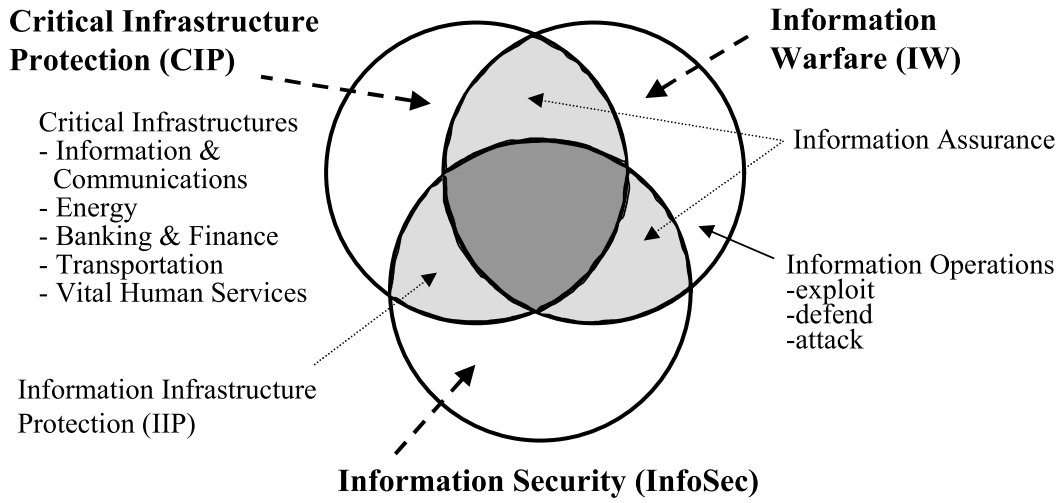

Figure 1: Areas and interrelated Sub-Areas of Information Warfare, Information Security, and Critical Infrastructure Protection.

The term 'information security' (INFOSEC) has been around for at least two or three decades. A US federal standard defines it as "The protection of information against unauthorized disclosure, transfer, modification, or distraction, whether accidental or intentional." By contrast, the term 'information assurance' is relatively new [4]. A 1996 US Department of Defense directive defines it as "Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities." Defensive information warfare is closely related to both concepts but is concerned only with intentional attacks. Information security and information assurance also address unintentional threats, e.g., errors, accidents, and natural disasters [4].

Thus information assurance is based on an Info Ops definition and has a somewhat broader meaning than information security. The term information assurance can be found meanwhile in various government areas, e.g., Department of Defense, Critical Infrastructure Protection, and National Security Agency [14]. Various definitions of information operations (Info Ops) are

presented in [23]. NATO defines Information Operations as [10]: “Actions taken to influence decision makers in support of political and military objectives by affecting other's information, information based processes, command and control (C2) systems, while exploiting and protecting one's own information and/or information systems. There are two main categories of Info Ops: defensive Info Ops and offensive Info Ops, depending upon the nature of the actions involved”.

SECURING NETWORKED INFORMATION SYSTEMS

As figure 2 indicates, today's challenge is on securing networked information systems, in civil as well as in military environments. Consequently the NSA Information Systems Security Organization (NSA/ISSO) has defined an information system (IS) as: “The entire infrastructure, organization, personnel, and components, for the collection, processing, storage, transmission, display, dissemination, and disposition of information”, and information systems security (ISS) as: “Protection of information systems against unauthorized access to or modification of information whether in storage, processing or transit, and against the denial of service to authorized users, including those measures necessary to detect, document, and counter such threats.” Securing networked information systems requires an overall system perspective. Security is tightly coupled with safety and reliability, and must not be ignored or relegated to incidental concerns. We take a broad view here of the problems of attaining security and safety, and consider these problems as a unified global system/network/agency problem. The securing procedure indicated in figure 2 can be applied to a single computer platform as well as to the IT systems and infrastructures of a national-scale level [1].

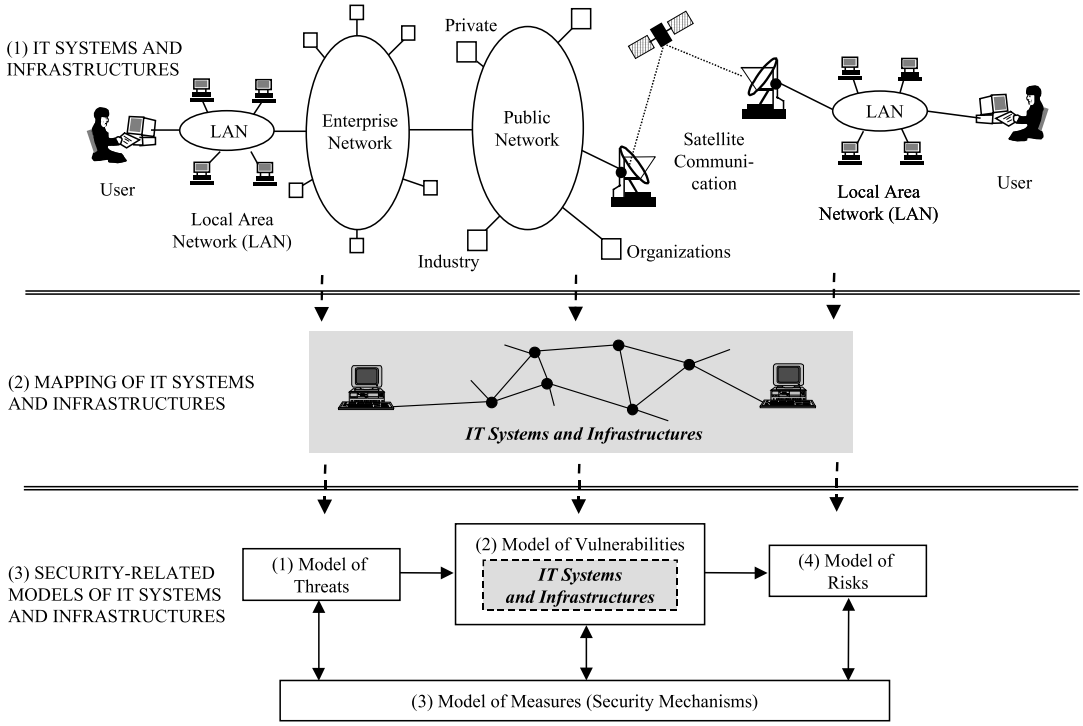

Figure 2: Steps in Securing Networked Information Systems: Analyzing Vulnerabilities, Threats, and Risks.

Security vulnerabilities (figure 2) are ubiquitous. Most computer operating systems have weak authentication and are relatively easy to penetrate. Most such systems have weak access controls and tend to be poorly configured, and are as a result relatively easy to misuse once initial access is attained. These systems often have monitoring facilities that are ill adapted to determining when threats are mounting and what damage may have occurred. Consequently, misuse by outsiders and insiders is potentially easy to achieve and sometimes very difficult to detect.

Threats to security (figure 2) are ubiquitous. The range of threats that can exploit these vulnerabilities is enormous, stemming from possible terrorist activities, sabotage, espionage, industrial or national competition, copycat crimes, mechanical malfunctions, and human error. Attacks may involve Trojan-horse insertion and physical tampering, including retributive acts by disgruntled employees or former employees or harassment. Denial of service attacks are particularly insidious, because they are so difficult to defend against and because their effects can be devastating. Systems connected to the Internet or available by dial-up lines are potential victims of external penetrations. Even systems that appear to be completely isolated are subject to internal misuse. In addition, many of those seemingly isolated systems can be compromised remotely because of their facilities for remote diagnostics and remote maintenance.

Risks are ubiquitous (figure 2). The consequences of these vulnerabilities and associated threats imply that the risks can be very considerable. Computer-related misuse may (for example) result in loss of confidentiality, loss of system integrity when systems are corrupted, loss of data integrity when data is altered, denials of service that render resources unavailable, or seemingly innocuous thefts of service.

INFORMATION SECURITY-RELATED ISSUES

Information security (INFOSEC) is the fundamental and in some respect already classical part of the three security-related issues. Information security (or computer security, as it was initially called) was first definitively characterized in a Defense Science Board report in 1970, but practical and operational experience, in particular incorporation of security safeguards into systems, commenced much later [24]. Computer security as a discipline was first studied in the early 1970s, although the issues had influenced the development of many earlier systems. The decade of the 1970s was devoted largely to research funded by the Department of Defense, notably the US Air Force and DARPA. According to [24], real-world experience did not begin until the publication of "Department of Defense Trusted Computer System Evaluation Criteria" commonly known as "The Orange Book" or the TCSEC. Throughout the 1970s and 1980s, INFOSEC efforts were focused on non-networked, trusted computing security evaluation criteria (TCSEC) and communications security (COMSEC) for national and military communications. Even then, systems incorporating security safeguards were not installed until the late 1980s. The subject of information operations was developed in experiments by US forces, mainly in the years between 1985 and 1995 [5/ 8/ 10/ 13/ 19/ 21/ 22/ 23/ 25]. Beginning in the late 1980s, there has been increased interest in protecting the critical infrastructures upon which society depends against physical and information attacks. The Critical Technologies Institute (managed by RAND) was created in 1991 by an act of Congress and studied and defined the issue of Critical Infrastructure Protection (CIP) [1/ 18/ 23/ 24.]

INFORMATION SECURITY

Intuitively, the natural-language meaning of security implies protection against undesirable events. System security and data security are two types of security. INFOSEC can be defined at two levels [23:] At the policy level, INFOSEC is the system of policies, procedures, and requirements to protect information; at the technical level, INFOSEC includes measures and control that protect the information infrastructure against denial of service, unauthorized disclosure, and modification or destruction of information infrastructure components (including data). INFOSEC includes the totality of security safeguards needed to provide an acceptable protection level for an infrastructure and for data handled by an infrastructure. More recently, the aspect of survivability (the capacity to withstand attacks and functionally endure at some defined level of performance) has been recognized as a critical component of defenses.

A comprehensive system- and network-wide set of realistic requirements is desired, encompassing security, reliability, fault tolerance, performance, and any other attributes necessary for attaining adequate system and network survivability. The most general topic of system requirements is dependability (in [11] survivability is discussed instead). Dependability (or survivability) includes the component requirements (A) security, (B) reliability, and (C) performance. The primary properties of security are (1) confidentiality, (2) integrity, and (3) availability. Survivability is the ability of a networked information system to satisfy and to continue to satisfy certain critical requirements (e.g., requirements for security, reliability, real-time responsiveness, and correctness) in the face of adverse conditions. Survivability must be defined with respect to the set of adversities that are supposed to be withstood. Types of adversities might typically include hardware faults, software flaws, attacks on systems and networks perpetrated by malicious users, and electromagnetic interference. As is often done for reliability, survivability could alternatively be defined as a probabilistic measure of how well the given requirements are satisfied. But mostly a non-quantified definition is preferred. There are clear links between the concept of system survivability and dependability. The three primary attributes of security are (1-3), whereas additional three attributes (4-6) in common use too:

(1) Confidentiality protects the existence of a connection, traffic flow, and information from disclosure.

(2) Integrity assures that information and processes are secure from unauthorized via methods such as encryption, digital signatures, and intrusion detection.

(3) Availability provides assurance that information and services will be accessible and usable when needed.

(4) Authentication assures that only authorized users have access to information and services.

(5) Non-repudiation assures that transactions are immune from false denial of sending or receiving information by providing reliable evidence that can be independently verified to establish proof of origin and delivery.

(6) Restoration assures information and systems can survive an attack and that availability can be resumed after the impact of an attack.

Security includes both system security and information security. It must anticipate all realistic threats, including misuse by insiders, penetrations by outsiders, accidental and intentional interference (e.g., electromagnetic), emanations, covert channels, inference, and aggregations. There is much more to security than merely providing confidentiality, integrity, and availability. Reliability is generally defined as a measure of how well a system operates within its specifications. For, example, fault tolerance can enable a variety of alternatives, including real-time, fail-safe, fail-soft, fail-fast, and fail-secure modes of operation. Performance is a critical requirement. In some cases, adequate performance may be critical to the survivability of an enterprise or an application. On the other hand, in most cases, performance is itself dependent on survivability and availability. If a system is not survivable, adequate performance cannot be achieved. What is immediately obvious is that close interrelationships exist among the various requirements.

Here we resume the steps of securing networked information systems (figure 2) as they are described by Waltz [23]. Security analysis must be applied to determine the degree of risk to the system, to identify design, configuration, or other faults and vulnerabilities, and to verify compliance with the requirements of the security policy and model. The analysis can range from an informal evaluation to a comprehensive and exhaustive analysis.

The first step in the analysis process includes an assessment of the threats to the system, based on intelligence and extrapolations of technology capabilities. The vulnerability assessment hypothesizes the areas of likely access (internal and external) and assesses the relative vulnerability (or security weaknesses) to attack. Vulnerabilities can be attributed to failures in analysis, design, implementation, or operation of the network or system.

The result of the threat and vulnerability assessment is a threat matrix that categorizes threats (by attack category) and vulnerabilities (by functions). The matrix provides a relative ranking of the likelihood of threats and the potential adverse impact of attacks to each area of vulnerability. These data form the basis for the risk assessment.

The risk management process begins by assessing the risks to the system that are posed by the risk matrix. Risks are quantified in terms of likelihood of occurrence and degree of adverse impact if they occur. On the basis of this ranking of risks, a risk management approach that meets the security requirement of the system is developed. Security can be quantified in terms of risk, including four components: (1) percent of attacks detected; (2) percent detected and contained; (3) percent detected, contained, and recovered; and (4) percent of residual risk. This phase introduces three risk management alternatives:

> (1) Accept risk: If the threat is unlikely and the adverse impact is marginal, the risk may be accepted and no further security requirements imposed.
>
> (2) Mitigate (or manage) risk: If the risk is moderate, measures may be taken to minimize the likelihood of occurrence or the adverse impact, or both. These measures may include a combination of OPSEC, TCSEC, INFOSEC, or internal design requirements, but the combined effect must be analyzed to achieve the desired reduction in risk to meet the top-level system requirements.

(3) Avoid risk: For the most severe risks, characterized by high attack likelihood or severe adverse impact, or both, a risk avoidance approach may be chosen. Here, the highest levels of mitigation processes are applied (high level of security measures) to achieve a sufficiently low probability that the risk will occur in operation of the system.

When the threats and vulnerabilities are understood, the risks are quantified and measures are applied to control the balance of risk to utility to meet top-level security requirements, and overall system risk is managed. The design stage then implements the design, which must undergo design analysis and security verification testing. In addition, an independent red team may also be chosen to conduct the security verification testing, which implements the threat model in an attack engine to conduct simulated attacks on the system to evaluate actual security performance. Red team attacks (also called "penetration testing") target the physical and operational security as well as the technical aspects of the system. The results of the red team verification may result in design changes to assure compliance with the system security requirements.

INFORMATION WARFARE

As with security and assurance of information, we have to think about definitions and meaning first, since information warfare has come to mean a number of different things - perhaps a combination of them all; and what it means really depends upon someone's particular bias. (1) The pure information warrior sees information warfare as a war without bombs or bullets; a conflict of any magnitude waged anywhere, motivation independent. (2) The next group to come along believes in 'Information in Warfare'. Many of these people feel that conventional war fighting capability can be increased through the advent of better information technologies. (3) Knowledge-Based Warfare is a nascent smart-extrapolation of the last concept and makes a distinction between information and the subjective increased value of knowledge. Ultimately, Information Warfare is about the convergence of military and civilian security issues and how people deal with them in a rapidly changing world.

The objective of information-based warfare is ultimately to achieve military goals with the most efficient application of information resources [23]. Offensive information operations are malevolent acts conducted to meet the strategic, operational, or tactical objectives of authorized government bodies; legal, criminal, or terrorist organizations; corporations; or individuals. Offensive information attacks have two basic functions: to capture or affect information. Information superiority is the capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same. If information operations are performed in the context of a strategy, they have a desired objective (or end state) that may be achieved by influencing a target (the object of influence).

Information operations are defined by the U.S. Army as Continuous military operations within the Military Information Environment (MIE) that enable, enhance and protect the friendly force's ability to collect, process, and act on information to achieve an advantage across the full range of military operations; information operations include interacting with the Global Information Environment (GIE) and exploiting or denying an adversary's information and decision capabilities.

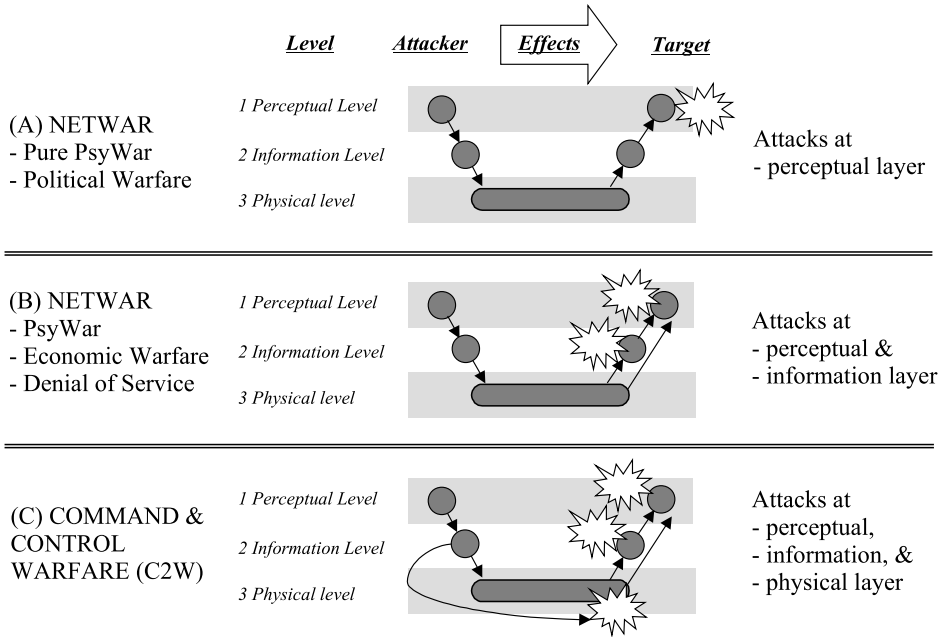

Figure 3: Three-Level Model of Information Operations [23] .

A simple functional model is presented (figure 3) to form the basis for future discussions of operations and the techniques employed [23]. The model is an extension of the basic conflict model and includes concepts that recognize three conceptual domains of information operations activity. The model recognizes that targets exist in (1) physical space, (2) cyberspace, and (3) the minds of humans. The highest level target of information operations is the human perception of decision makers, policymakers, military commanders, and even entire populations. The ultimate targets and the operational objective are to influence their perception to affect their decisions and resulting activities.

The information operations model (figure 3) distinguishes three levels or layers of functions on both the attacker and the target sides. The layers are hierarchical, with influence flowing downward on the attacker side and upward on the target side. The objective of the attacker is to influence the target at the perceptual level by actions that may occur at all levels of the hierarchy. The three layers follow the cognitive model, dealing with knowledge at the highest level, information at the intermediate level, and data at the lowest level.

The first layer is at the perceptual or psychological level, which is abstract in nature and is aimed at management of the perception of a target audience. At this level, the strategic objective defines the desired actions of the target and the perception(s) that will most likely cause those actions. If the desired action is termination of aggression, for example, the objective perception for targeted leaders may be "overwhelming loss of control, disarray, and loss of support from the populace". If the desired action is disengagement from a military action, the objective perception for targeted military commanders may be “lack of logistic support to sustain operations.” These perception objectives may be achieved by a variety of physical or

abstract (information) means, but the ultimate target and objective is at the purely abstract perceptual level, and the effects influence operational behavior.

The second layer is the information infrastructure layer, which includes the abstract information infrastructure that accepts, processes, manages, and stores the information. This is the layer that is most often considered to be the 'cyberspace' dimension at which malicious software and infrastructure exploitation (hacking) attacks occur. Attacks on this intermediate layer can have specific or cascading effects in both the perceptual and physical layers.

The third layer is the physical system level, which includes the computers, physical networks, telecommunications, and supporting structural components (e.g., power, facilities, environmental control) that implement the information system. Also at this level are the human administrators of the systems, whose physical influence on the systems is paramount. Attacks at this layer are also physical in nature.

Attacks may occur directly across the perceptual layer (e.g., a direct meeting between leaders in which human discourse is used to influence the perception of a target, or to collect intelligence), or they may target lower layers with the intent of having consequent influences on other layers.

The model illustrates how operational elements must consider each level of the model. Consider, for example, how intelligence collection for indications and warning, targeting, and battle dam-age assessment must consider all three levels.

In figure 3, the attack threads through the information warfare model for three categories of information warfare are illustrated. Exploitation of the physical and information layers purely for purposes of perception management, or psychological warfare (PSYWAR), is illustrated at the top of the figure. Command and control warfare (C2W), in which attacks occur at all three layers, is depicted at the bottom of the figure. These distinctions are representative only, recognizing that in real-world conflict, attacks will occur at all levels to varying degrees. Large-scale netwar, for example, may be supported by small-scale but crucial physical attacks on infrastructure or personnel to accomplish overall objectives.

CRITICAL INFRASTRUCTURE PROTECTION

Within the last five to ten years there has been increased interest in protecting the critical infrastructures upon which society depends against physical and information attacks. The NSA Information Systems Security Organization (NSA/ISSO) defines: "Critical infrastructures are those physical and IT-based systems essential to the minimum operations of the economy and the government." We have to consider different types of infrastructures: (1) the critical national infrastructures, (2) information infrastructures such as the Internet, or whatever may replace it - a National Information Infrastructure (NII), or a Global Information Infrastructure (GII) - and (3) underlying computer systems and networking software. Important from the present perspective is the recognition that very serious vulnerabilities and threats exist in these critical infrastructures. Perhaps equally important is the recognition that these critical infrastructures are closely interdependent and that they all depend on underlying computer-communication infrastructures.

For a particular country, a characteristic set of critical infrastructure sectors may be found by identifying the attributes of the country, its structure, its institutions and organizations that inherently contribute to resilience, and derive an estimate of the present level of resilience. According to US views [11], these infrastructures initially subsumed eight major sectors: information and communications, electric power, finance and banking, water and sewage, transportation, oil and gas, emergency services (e.g., police, fire, medical), and essential government services. As the commission proceeded, it revised, slightly modified, and aggregated these sectors into five: (1) Information and Communications; (2) Energy; (3) Banking and Finance; (4) Transportation; and (5) Vital Human Services. Many of these critical infrastructures are becoming increasingly more international. This is a logical consequence of the increasing globalization.

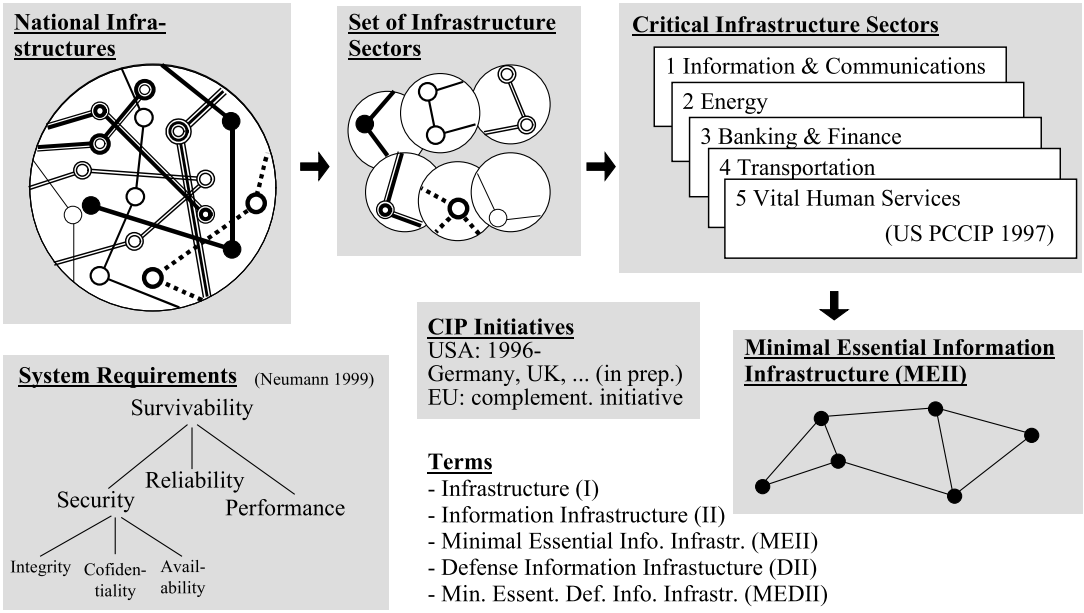

Figure 4: Approach to Critical Infrastructure Protection (CIP).

The concept of a minimum essential information infrastructure (MEII) addresses the survivability and assured availability of essential information infrastructures, particularly in the face of various forms of information warfare attack [1]. The concept has been proposed in the critical infrastructures community to ensure that some essential functionality would continue to exist despite a reasonable range of survivability threats - attacks, outages, failures, environmental disturbances, and so on. Up to now, there is a considerable debate over the definitions of minimal and essential - as well as recognition of the problems inherent in trying to focus on a single universal MEII. Nevertheless, the concept is valuable as a guiding architectural concept. Based on extensive interviews, detailed studies of the architectures of several pervasive and important systems, and analysis of the literature on vulnerabilities and risks in information systems, a methodology to assist in developing MEII-like characteristics in future information systems has been developed. The methodology consists of (1) identifying the information functions that are essential to the unit's mission; (2) determining the information systems that are essential to accomplish those functions; (3) searching for vulnerabilities within those systems components; (4) applying appropriate protection techniques for vulnerabilities found at varying system levels; and (5) testing the protections against a set of threat scenarios

to check their robustness. Application of this methodology will result in a form of MEII that is a set of systems in nested enclaves of increasing security.

The goal of infrastructure assurance research and development (R&D) is to support the development of technologies that will counter threats and reduce vulnerabilities in those areas having the potential for causing significant national security, economic, and/or social impacts. Physical and information threats are addressed. Specific technologies considered are those that protect infrastructure and thereby reduce vulnerability, detect intrusions and provide warnings, mitigate the effects of disruptions (incidents), assist in the management of incidents, and facilitate recovery. Focal points of the program are to: (1) develop technologies that support rapid recognition of large-scale attacks and (2) develop systems that exhibit inherent survivability properties, i.e., the ability to continue operation in the face of attacks that are partially successful. Particular objectives are to: (a) recognize national-scale attacks and distinguish them from events of only local significance; (b) limit the impact of an attack by ensuring the integrity of data and programs; and (c) impede denial-of-service attacks by limiting the resource consumption that can be attained by the attacker. Finally, we have to realize that many of the critical infrastructures are becoming increasingly more international. This is a logical consequence of the increasing globalization.

Meanwhile, several critical infrastructure protection initiatives are in preparation in Europe (e.g., European Union, Germany, UK). Complementary to national initiatives in Europe, the European Commission is exploring the establishment of a European Dependability Initiative of the Information Society Technologies Program. This work is carried out with the support of the Joint Research Center, Institute for Systems, Informatics, and Safety. The studies initiated by the European Commission introduce and explore the concept of survivability. It highlights the distinction between the traditional dependability perspective and the viewpoint currently explored in the survivability approach.

INFORMATION ASSURANCE AGENDA

Reporting And Analyzing Security Incidents

Reporting and analyzing security incidents will for a long time remain an unsolved problem, if only one attack in 20 is noticed by the victim and only one attack in 20 gets reported. In an unusually broad and stringent study, Howard [6] analyzed trends in Internet security through an investigation of 4,299 security-related incidents on the Internet reported to the CERT Coordination Center (CERT/CC) from 1989 to 1995. Prior to this research, our knowledge of security problems on the Internet was limited and primarily anecdotal. Howard's research accomplished the following: (1) development of a taxonomy for the classification of Internet attacks and incidents, (2) organization, classification, and analysis of incident records available at the CERT/CC, and (3) development of recommendations to improve Internet security, and to gather and distribute information about Internet security.

With the exception of denial-of-service attacks, security incidents were generally found to be decreasing relative to the size of the Internet. Estimates based on this research indicated that a typical Internet domain was involved in no more than around one incident per year, and a typical Internet host in around one incident every 45 years. The taxonomy of computer and network attacks developed for this research was used to present a summary of the relative fre-

quency of various methods of operation and corrective actions. This was followed by an analysis of three subgroups: (1) a case study of one site that reported all incidents, (2) 22 incidents that were identified by various measures as being the most severe in the records, and (3) denial-of-service incidents. Data from all incidents and these three subgroups were used to estimate the total Internet incident activity during the period of the research. This was followed by a critical evaluation of the utility of the taxonomy developed for this research. The analysis concludes with recommendations for Internet users, Internet suppliers, response teams, and the U.S. government. Howard's study presents only a preliminary analysis of the data derived from the incident records during 1989 to 1995. It was recommended that the data set should be made available on-line for use by other researchers. In addition, useful information concerning incident analysis, the related methodical problems, and the use of taxonomies, is given by Cohen [3].

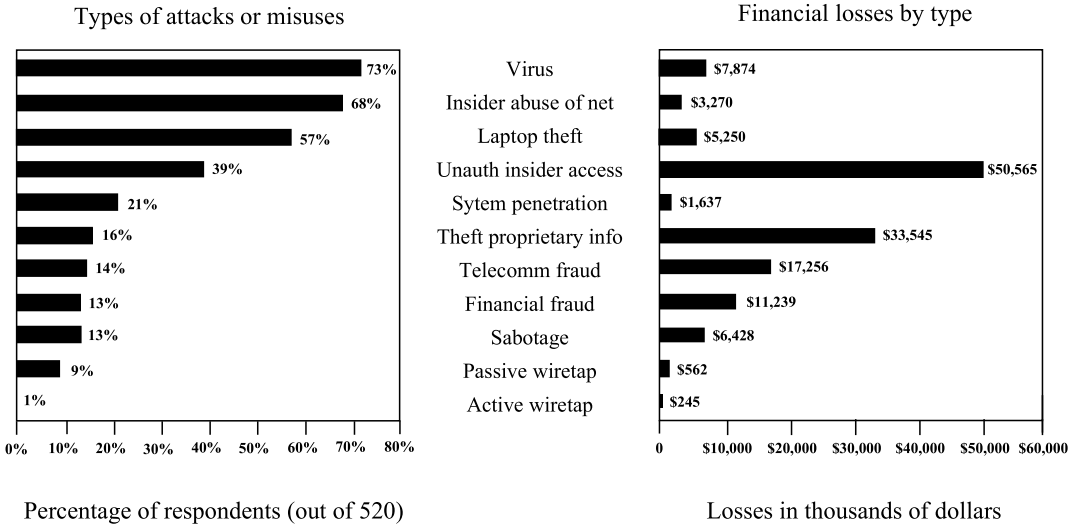

Figure 5: Computer Crime: Type of Attack and Financial Losses [4].

As correlated with increasing security incidents, computer crime and misuse have been on the rise, no doubt owing to the proliferation of computing technologies and growth of the Internet. The left side of figure 5 shows the number of respondents reporting different types of attacks or misuse against their computing and telecommunications resources, ordered from most prevalent to least prevalent type. The right side of figure 5 shows the losses in thousands of dollars for incidents of those types with quantifiable losses. The figures show that whereas computer viruses were encountered by the greatest number of companies, with 73% of respondents saying they detected incidents of that type, they did not account for the largest losses, which were attributed to unauthorized access by insiders and theft of proprietary information. The two least reported threats, active and passive wiretaps, however, also accounted for the smallest losses. The respondents said that likely sources of attack are disgruntled employees (89%), independent hackers (72%), domestic corporations (48%), foreign corporations (29%), and foreign governments (21%).

Assurance Mechanisms

Information assurance includes the totality of security safeguards needed to provide an acceptable protection level for an infrastructure and for data handled by an infrastructure. More recently, the aspect of survivability has been recognized as a critical component. Survivable systems include the properties of: fault tolerance; robust, adaptive response; distribution and variability; and recovery and restoration [23].
The emphasis of this chapter is on technical security measures, but physical and personnel security measures are essential complementary protection. Physical-level security includes controls for physical access to facilities, protection from local capture of information via unintentional electromagnetic radiation, protection from failure of supporting utilities and natural disasters, and many other threats.

A formal security policy model is the core of the concept of trust [23]. It mathematically defines a trusted computing base (TCB) as an abstract model. The model includes the notion of a secure state of the TCB, subjects (users that access the TCB), objects (data sets in the TCB), and actions that the TCB performs. The model describes these fundamental actions and the state transitions of the TCB. The model permits analysis and provides a means of proof that any given TCB architecture implementation always remains in secure states.

The control of access to authentic users is the fundamental security mechanism of single or networked systems. The process of authentication requires the user to verify identity to establish access, and access controls restrict the processes that may be performed by the authenticated user or users attempting to gain authentication. Authentication of a user in a secure manner requires a mechanism that verifies the identity of the requesting user to a stated degree of assurance.

Cryptography provides the mathematical processes for transforming data (by encryption and decryption) between an open format and a secure cipher text format to provide the privacy property. The strength of the encryption algorithm is a measure of the degree to which the cipher text endures attacks. The ultimate strength and generality of cryptographic processes lies in the mathematical formulation of the underlying transform algorithms. The general cryptosystem includes the cryptographic message path that includes the encryption, transmission, and decryption process, and a supporting method of distributing a numerical variable, or key, that controls the encryption transformation. The generation, storage, distribution, and overall protection of keys are critical to the security of all cryptosystems. Compromised keys provide the most direct means of unauthorized access. For this reason, physical, information, and perceptual layers of security must protect the key management functions, including those summarized below. In addition to providing privacy, the encryption process provides a means of authentication of a message by an encrypted data item called a digital signature. The digital signature permits proof of identity of the sender, and proof that an attacker has not modified the message.

Firewalls are trusted systems that integrate authentication, connection control, incident-response, encryption, network structure security, and content security into a single secure unit. Located between two networks, all traffic passing between the networks must pass through the firewall, which restricts passage to only authorized traffic allowed by the security policy. The firewall effectively creates a security “domain” or “enclave” by providing a perimeter de-

fense to a network (the secured domain). The four basic types of firewalls are (1) packet filters, (2) circuit relays, (3) application gateways, and (4) dynamic packet filters.

Systems for intrusion detection and response (IDS) are needed to protect computer systems and networks from internal or external intrusions. Traditional computer security distinguishes auditing from alarm reporting. Security auditing reviews the records of activities to detect security incidents (including changes in operational configuration), to verify compliance with security policy, and to test security controls. Security alarm reporting monitors security-related events that may indicate misuse of security controls or configurations, hostile activities against security controls, or behaviors inconsistent with security policy. Automated detection of incidents and immediate alarm reporting and response is required to respond to structured information warfare attacks on networks. As in all alarm systems, false alarm and detection failure rates measure overall detection performance. Automatic detection and reporting is required for a wide range of threatening actions, e.g., external intrusions, internal security intrusions, system failures, and anomalous behavior.

SCIENCE AND ENGINEERING ISSUES

Citizenry, industry, government, and the military have become vulnerable due to the reliance on technology, particularly information technologies. Even more frightening, but less understood, is that this vulnerability is increased due to reliance on the world economy and coalition arrangements in the military. As the immensity of the information assurance (IA) problem before the information society has been uncovered, growing attention is being given to this topic by the press, industry, and the government. The field of information assurance focuses on designing systems that can enforce security policies even in the presence of malicious code. The challenge is to design, develop, and deploy complex systems with confidence in their ability to satisfy security requirements. A theory of computer security is on the way that offers a formal method for security engineering, so that we can expect to get affordable, verifiable, scalable technologies for a robust and secure defense infrastructure. This theory will have three components: policy, mechanism, and assurance.

Attempts have been made to address the growing information assurance problem. Some of these attempts were typically ‘reactionary’, at a shallow level, and with narrow focus. For instance, firewalls were introduced to protect local area networks from the Internet; however, they were developed at a superficial level to control the known protocols and threats that were plainly evident. Many authors have shown that there are inherent problems in the existing design and assessment processes that create our information systems [3, 11, 17, 18].

According to DARPA [20], these problems can only be addressed by a fundamental change in information assurance philosophy. It is evident that existing methods are inconsistent, inefficient, do not approach problems with a truly “system-level” viewpoint, and have goals and results limited by the currently abstract and immature nature of the discipline. These limitations cannot be overcome with additional evolutionary research in the same core concepts such as vulnerabilities, threats, and countermeasures. According to DARPA [20], a new information assurance paradigm is required – one that enables the designer and analyst to capture and probe the causality, relationships, and objectives of an entire system. A step in the basic science of information assurance should be to develop equivalencies, relationships, laws, logic, postulates, proofs, and methods for calculation so that metrics can be used effectively.

Just as in other disciplines, complexities of systems will often not allow for closed solutions; therefore, modeling of information assurance will be needed. The overall goal of the new DARPA approach is to provide a science-based environment for design and assessment that will yield improved information assurance and allow for faster design and assessment at less cost. This environment will consist of methods and automated tools to provide consistent results and metrics to specify information assurance. This work is being performed because current designers and assessors have no way to consistently measure the many aspects of information assurance. They also work without an integrated environment and automated tool support that could vastly improve their performance and the assurance of their information systems.

Some analyses of methods and tools needed by the information warfare (IW) community have resulted in a set of major findings and recommendations. The assessment of the nature of the problem has led to the appreciation that information warfare methods must be able to cope with complex, dynamic, interactive, adaptive processes; teams of humans, under stress, across cultures; and uncertainty as an inherent property. It is anticipated that a diverse mix of methods and techniques will be needed to attack the problems in the IW areas. These tool-based methods should include, but are not limited to, the following: (1) Expert elicitation (e.g., use of structured means to elicit judgments from experts); (2) Constructive Modeling and Simulation (e.g., simulated people operating simulated systems); (3) Virtual Modeling and Simulation (e.g., real people operating simulated systems); and (4) Live Modeling and Simulation (e.g., real people operating real systems).

EDUCATION

Advancing the professional education in Information Warfare (IW), Information Assurance (IA), and Critical Infrastructure Protection (CIP) is an urgent need, in all civil and military organizations of all countries, since the most important aspect of these three areas is people. To meet these challenges, we must improve both the quality and delivery of assurance-related education. According to [7], the number of skilled practitioners of computer security who are able to address the complexities of modern technology and are familiar with successful approaches to system security is very small.

People want security but are faced with two difficulties. First, they do not know how to achieve it in the context of their enterprises. They may not even know of a way to translate organizational procedures into policies, much less implement a set of mechanisms to enforce those policies. Second, they have no way of knowing whether their chosen mechanisms are effective. Modern educational approaches emphasize information assurance not simply as a separate discipline, but as a multi-disciplinary science which includes elements of operating systems, networking, databases, the theory of computation, programming languages, architecture, and human-computer interaction [7, 11, 12, 13, 14]. The body of knowledge must be incorporated as appropriate into this set of disciplines.

In 1999 the NSA Information Systems Security Organization (NSA/ISSO) has founded a National INFOSEC Education & Training Program (NIETP) with seven subprograms [14]: (1) Seven Centers of Academic Excellence in Information Assurance Education; (2) National Colloquium for Information Systems Security Education; (3) University Outreach Program;

(4) Electronic Develop-A-Curriculum Program; (5) "Blue Box" Initiative; (6) Service Academy Visiting Professorship Program; and (7) Information Assurance Courseware Evaluation Process. The goals of the National Colloquium are to create an environment for exchange and dialog among leaders in government, industry and academia concerning the need for and utility of information security and information assurance education. Given the scope and fluid state of knowledge of information security, the Colloquium will strive to foster the development of academic curricula which recognizes the need expressed by government and industry, and is based on the recognized 'best practices' available in the field. The Colloquium will assist educational institutions by fostering the continued development and sharing of information security education resources.

The information warfare (IW) course of the Naval Postgraduate School (NPS), Monterey [13], is designed to provide students with an opportunity to apply fundamental systems engineering analysis and theory to an IW system problem encountered in an operational environment. Students can model a generic information system, applying systems engineering design theory, and processes to develop a relevant IW system. They could learn to choose sound engineering approaches to both defend the system under study, and conversely to attack the system if one were to assume its possession by an adversary. The class can be coordinated using a step-by-step decision analysis process. For example, nodal and critical path analyses will be reviewed for vulnerability, with emphasis on technology trends in the fields of communications and computers. Organizational decision systems (command & control) and human factors engineering will be studied in order to permit modeling of adversaries military and civil command structure as part of the project. There can be a class project (with two teams competing) devoted to the formulation and presentation of an organized systems approach to solving the operational application of an Information Warfare challenge using the communications equipment selected.

CONCLUSIONS

Twenty years ago, corporate and military information infrastructures were separate and distinct, and the term 'information warfare' did not exist. Today they are on the way to become one and the same, and the resulting networked information systems open many doors for information warfare. The military community depends upon (nearly) the same computer networks and networking equipment to fight wars as industry depends upon to conduct business. In this respect, it is worth noticing that over 95% of US military communication links make use of commercially leased lines and satellites, and during the operation Desert Storm this percentage was even higher [9]. The government has three roles with respect to the nation's information infrastructure: to be forthcoming about the genuine threat, to stimulate adequate regulations, and to foster public confidence. This paper could help to open a dialogue among academia, industry, and government toward assuring information infrastructures and information systems. The security community needs a common vocabulary to discuss threats and countermeasures, and a common methodology to discover weaknesses in systems, to prioritize weaknesses in terms of relative dangers to the system, and to determine cost-effective countermeasures. Indeed, there exists a common problem area in the context of information warfare, with challenges for a new level of cooperation in science, engineering, and education - but many of these problems still have to be uncovered for cooperation. As expressed in figure 1, the areas of Information Warfare (IW), Information Security (INFOSEC), and Critical

Infrastructure Protection (CIP) belong together, and we should work out the interrelationships between their sub-areas.

NOTES

[1] Anderson, R., Feldman, P., et al. (1999): *Securing the U.S. Defense Information Infrastructure: A Proposed Approach (MR-993)*, Santa Monica, CA: RAND. <www.rand.org/publications/>

[2] Cobb, A. C. (1997): *Australia's Vulnerability to Information Attack: Towards a National Information Policy*, Strategic and Defence Studies Centre, Australian National University, Canberra. <coombs.anu.edu.au/~acobb/X0016_Australias_Vulnerabi.html>

[3] Cohen, F. (1999): *Simulating Cyber Attacks, Defenses, and Consequences*, Fred Cohen & Associates (Information Security Services). <all.net>

[4] Denning, D. E. (1999): *Information Warfare and Security*. Reading, MA: Addison-Wesley.

[5] Gray, J. V., Barlow, W. J., Barnett, J. W., Gerrity, J. L., & Turner, R. D. (1997): *Information Operations*, A Research Aid (IDA Document D-2082). Alexandria, VA: Institute for Defense Analysis (IDA).

[6] Howard, J. D. (1997): *An Analysis Of Security Incidents On The Internet 1989-1995*, Pittsburgh, PA: Carnegie-Mellon University. <www.cert.org/research/JHThesis/Start.html>

[7] Irvine, C. E., Chin, S. -K., & Frincke, D. (1998):' Integrating Security into the Curriculum', *IEEE Computer*, Dec. 1998, p. 25-30.

[8] JP3-13 (1998): *Joint Doctrine for Information Operations,* (Joint Publication JP3-13, 9 October 1998). <www.dtic.mil/doctrine/jel/c_pubs2.html>

[9] Luiijf, E. A. M. (1999): 'Information Assurance and the Information Society', In: Gattiker, U., Pederson, R., & Peterson, K. (Eds.): *EICAR Proceedings 1999*. Aalborg, DK: TIM-World ApS (ISBN 87-987271-0-9).

[10] NATO (1998): *NATO Information Operations (Info Ops) Concept,* (NATO MCM-0969-98). Brussels, Belgium: NATO Headquarters.

[11] Neumann, P. G. (1999): *Practical Architectures for Survivable Systems and Networks,* (Report). Computer Science Laboratory, SRI International, Menlo Park, California. <http://www.csl.sri.com/~neumann/arl-one.html>

[12] NPS/CISR (1998): Naval Postgraduate School Center for Information Security Studies and Research. The Naval Postgraduate School, Monterey, CA. <cisr.nps.navy.mil>

[13] NPS/IW (1998): Information Warfare Academic Group. The Naval Postgraduate School, Monterey, CA. <web.nps.navy.mil/~iwag/matrix.html>

[14] NSA/ISSO (1999): National Security Agency (NSA). Information Systems Security Organization (ISSO). <www.nsa.gov:8080/isso/>

[15] OSD (1998): Information Operations Planning Tools. <www.acq.osd.mil/at/iopt.htm>

[16] Pfleeger, C. P. (1997): *Security in Computing,* Englewood Cliffs, NJ: Prentice Hall.

[17] Salter, C., Saydjari, O. S., Schneier, B., & Wallner, J. (1999): *Toward A Secure System Engineering Methodology,* Proceedings, ACM New Security Paradigms Workshop, Sept. 22-25, 1998, Charlottsville, VA. New York: ACM.

[18] Schneider, F. B: (Ed.) (1998): *Trust in Cyberspace,* (NRC Report). Washington, DC: National Academy Press. <www.nap.edu/readingroom/books/trust/>

[19] Schwartau, W. (1998): Bibliography of W. Schwartau (Chez Winn). www.infowar.com/

[20] Skroch, M. (1999): *Development of a Science-Based Approach for Information Assurance,* (White Paper, DARPA/ISO, 10 May 1999). Alexandria, VA: Defense Advanced Research Projects Agency (DARPA). <www.darpa.mil/iso/iaset/iaset.htm>

[21] Theuerkauf, T. (1998): *Erste Ueberlegungen zu den konzeptionellen Ableitungen des Phaenomens Information Operation / Information Warfare*. In: CCG (1998): Information Warfare (Seminar, 30.6.-2.7.1998). Wessling-Oberpfaffenhofen: Carl-Crantz-Gesellschaft (CCG). www.ccg.dlr.de

[22] TNO/FEL (1999): WWW-resources related to Information Security and Information Operations / Information Warfare. Instituut TNO/FEL (Physics and Electronics Laboratory), Den Haag. <www.tno.nl/instit/fel/intern/work.html>

[23] Waltz, E. (1998): *Information Warfare Principles and Operations*, Norwood, MA: Artech House. <www.artech-house.com/links/pdfbooks.html>

[24] Ware, W. H. (1998): *The Cyber-Posture of the National Information Infrastructure,* (MR-976-OSTP). Santa Monica, California: RAND Corporation. <www.rand.org/publications/>

[25] Whitaker, R. (1998): *Information Warfare. Questing Power via Cyberspace*. <www.informatik.umu.se/~rwhit/IW.html>