ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

CYBER INFRASTRUCTURE PROTECTION - VOL 1 - PART 1 OF 3

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-144
Course Content:	129 pgs
PDH/CE Hours:	8

OFFICIAL COURSE/EXAM

(SEE INSTRUCTIONS ON NEXT PAGE)

WWW.ENGINEERING-PDH.COM
TOLL FREE (US & CA): 1-833-ENGR-PDH (1-833-364-7734)
SUPPORT@ENGINEERING-PDH.COM

ELE-144 EXAM PREVIEW

- TAKE EXAM! -

Instructions:

- At your convenience and own pace, review the course material below. When ready, click "Take Exam!" above to complete the live graded exam. (Note it may take a few seconds for the link to pull up the exam.) You will be able to re-take the exam as many times as needed to pass.
- Upon a satisfactory completion of the course exam, which is a score of 70% or better, you will be provided with your course completion certificate. Be sure to download and print your certificates to keep for your records.

Exam Preview:

1. According to the reference material, the term cyberpower means "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."
    a. True
    b. False
2. According to the reference material, the recent Heartland Payment Systems data breach compromised financial information in over ____ million transactions and involved financial records held by over 200 institutions
    a. 20
    b. 50
    c. 80
    d. 100
3. According to the reference material, in the widely publicized TJX Companies breach that occurred from 2005 to 2007, thieves stole over __ million credit card numbers.
    a. 25
    b. 35
    c. 45
    d. 55
4. One of the rules of thumb that characterizes cyberspace is Gilder's Law, which states that the total bandwidth of communication systems triples every __ months
    a. 12
    b. 18
    c. 24
    d. 36

5. According to the reference material, in Afghanistan, USAID invested $14.2 million to develop the 365 node ____-based district communications net-work (DCN) to extend voice and Internet access to the district level for use by local government officials and the local population.
    a. TDMA
    b. BGAN
    c. VSAT
    d. GATR
6. According to the reference material, from the middle of April 2009 to the present, the United States has been in a pre-pandemic event suggested by the World Health Organization (WHO) as stage 5.
    a. True
    b. False
7. Which of the following types of malwares is NOT mentioned in the reference material when it states that malware attacks cost the global economy billions of dollars in lost productivity?
    a. Trojans
    b. Spam
    c. Worms
    d. Viruses
8. One of the rules of thumb that characterizes cyberspace is Moore's Law, which states the number of transistors on a chip approximately doubles every ___ months
    a. 12
    b. 18
    c. 24
    d. 36
9. Figure 2.1 A Framework for Categorizing the Cyber Problem shows a visual representation of the 4 key area of the cyber domain. Which key area is comprised of factors such as legal, governance, and organization?
    a. Cyberpower
    b. Cyberstrategy
    c. Cyberspace
    d. Institutional factors
10. In the Service Provider Collaboration for the Collective good, it was suggested that during a pandemic or a national emergency, each organization should "voluntarily" reduce their Internet traffic by 25 percent below peak levels.
    a. True
    b. False

CONTENTS

PREFACE

The Internet, as well as other telecommunication networks and information systems, have become an integrated part of our daily lives, and our dependency upon their underlying infrastructure is ever-increasing. Unfortunately, as our dependency has grown, so have hostile attacks on the cyber infrastructure by network predators. The lack of security as a core element in the initial design of these information systems has made common desktop software, infrastructure services, and information networks increasingly vulnerable to continuous and innovative breakers of security. Worms, viruses, and spam are examples of attacks that cost the global economy billions of dollars in lost productivity. Sophisticated distributed denial of service (DDoS) attacks that use thousands of web robots (bots) on the Internet and telecommunications networks are on the rise. The ramifications of these attacks are clear: the potential for a devastating large-scale network failure, service interruption, or the total unavailability of service.

Yet many security programs are based solely on reactive measures, such as the patching of software or the detection of attacks that have already occurred, instead of proactive measures that prevent attacks in the first place. Most of the network security configurations are performed manually and require experts to monitor, tune security devices, and recover from attacks. On the other hand, attacks are getting more sophisticated and highly automated, which gives the attackers an advantage in this technology race.

A key contribution of this book is that it provides an integrated view and a comprehensive framework

of the various issues relating to cyber infrastructure protection. It covers not only strategy and policy issues, but it also covers social, legal, and technical aspects of cyber security as well.

We strongly recommend this book for policymakers and researchers so that they may stay abreast of the latest research and develop a greater understanding of cyber security issues.

CHAPTER 1

INTRODUCTION

This book is intended to address important issues in the security and protection of information systems and network infrastructure. This includes the strategic implications of the potential failure of our critical network and information systems infrastructure; identifying critical infrastructure networks and services; analysis and risk assessment of current network and information systems infrastructure; classification of network infrastructure attacks; automating the management of infrastructure security; and building defense systems to proactively detect network attacks as soon as possible once they have been initiated.

The chapters in this book are the result of invited presentations in a 2-day conference on cyber infrastructure protection held at the City University of New York, City College, on June 4-5, 2009.[1]

The book is divided into three main parts. Part I deals with strategy and policy issues related to cyber security and provides discussions covering the theory of cyberpower, Internet survivability, large scale data breaches, and the role of cyberpower in humanitarian assistance. Part 2 covers social and legal aspects of cyber infrastructure protection and discusses the attack dynamics of political and religiously motivated hackers. Part 3 discusses the technical aspects of cyber infrastructure protection including the resilience of data centers, intrusion detection, and a strong emphasis on Internet protocol (IP) networks.

STRATEGY AND POLICY ASPECTS

The four chapters in Part I provide a good framework for the various issues dealing with strategy and policy of cyber security. In Chapter 2, Stuart H. Starr presents a preliminary theory of cyberpower**.** The chapter, attempts to achieve five objectives. First, it will establish a framework that will categorize the various elements of the cyber domain. Second, it will define the key terms of interest. Third, it will begin to make clear the various benchmarks and principles that explain the various cyber categories. Fourth, it will characterize the degree to which the various categories of the cyber domain are connected. Finally, it will anticipate key changes in the cyber domain and provide a basis for analyzing them.

However, it must be emphasized that this evolving theory is in its preliminary stages. Thus, it is to be anticipated that it will not be complete. In addition, given the long gestation period for theories of "hard science" (e.g., physics, chemistry, and biology), it is likely that some of the elements are likely to be wrong.

In Chapter 3, Mike Chumer addresses the survivability of the Internet. The use of the "commodity" Internet, referred to simply as the Internet, is the cornerstone of private and public sector communication, application use, information sharing, and a host of taken-for-granted usages. During a recent planning symposium in 2007, hosted by SunGard and the New Jersey Business Force, the key discussion question was, "Will the Internet Be There When You Really Need It?" The planning symposium focused on how the internet will be effected if a pandemic based upon H5N1 (the bird flu) was to break out in the United

States. In this chapter, Mr. Chumer addresses the following issues that resulted from this symposium:

- Foreseeable short- and long-term impacts if the Internet either "crashes," "goes down," or "stops working";
- Whether existing protocols for providing collaboration and coordination between U.S. service providers (cable, telephone, and "last mile" providers) are sufficient enough to preserve Internet access and limit overload;
- Points of Internet failure that planners must consider when modifying or developing business practices;
- The effects on computer applications and/or protocols if the Internet slows down rather than halting during a pandemic, as well as mitigation strategies;
- In the face of heavy demand on the Internet, which features or services should contingency planners expect to shut down or redirect to conserve or preserve bandwidth;
- Whether contingency planners should expect attacks from hackers during a state when the Internet is weakened;
- Whether we as a nation are becoming too dependent on the Internet and underestimating its risks for the sake of cost, convenience, and efficiency;
- Will the Internet be resilient enough to hold up under the onslaught of school, business, home enterprise, emergency management, and recreational users during a pandemic?

Mr. Chumer concludes the chapter with a set of recommendations drawing upon those presented during the symposium.

Chapter 4 by, Douglas Salane, posits that despite heightened awareness, large scale data breaches continue to occur and pose significant risks to both individuals and organizations. The recent Heartland Payment Systems data breach compromised financial information in over 100 million transactions and involved financial records held by over 200 institutions. An examination of recent data breaches shows that fraudsters are increasingly targeting institutions that hold large collections of credit card and social security numbers. Particularly at risk are bank and credit card payment processors, as well as large retailers who do not properly secure their systems. Frequently, breached data winds up in the hands of overseas organized crime rings that make financial data available to the underground Internet economy, which provides a ready market for the purchase and sale of large volumes of personal financial data. Credit industry studies based on link analysis techniques confirm that breached identities often are used to perpetrate credit fraud soon after a breach occurs. These studies also show that breached identities may be used intermittently for several years. We conclude that strong data breach notification legislation is essential for consumer protection, and that the direct and indirect costs of breach notification provide significant economic incentives to protect data. Our analysis also concludes that deployment of privacy enhancing technologies, enterprise level methods for quickly patching and updating information systems, and enhanced privacy standards are needed to mitigate the risks of data breaches.

Chapter 5, "The Role of Cyberpower in Humanitarian Assistance/Disaster Relief (HA/DR) and Stability and Reconstruction Operations," by Larry Wentz, ex-

plores the role and challenges of cyberpower (information and communication technologies [ICT]) in humanitarian assistance/disaster relief (HA/DR) and stability and reconstruction operations. It examines whether a strategic use of cyber assets in U.S. Government (USG) engagement and intervention activities such as HA/DR and stability and reconstruction operations could lead to more successful results. Certainly, the information revolution has been a dynamic and positive factor in business, government, and social arenas in the Western world. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities of all types.

Complicating the challenges of HA/DR and stability and reconstruction operations related to failed-state interventions are the exacerbating difficulties that typically consist of: spoilers interfering with the intervening forces; refugees and internally displaced persons requiring humanitarian assistance; buildings requiring reconstruction; roads, power, water, telecommunications, healthcare, and education systems that are disrupted or dysfunctional; absence of a functioning government and laws, lack of regulations, and enforcement mechanisms; widespread unemployment and poverty; and a shortage of leaders, managers, administrators, and technical personnel with 21st century technical and management skills. Additionally, the operations lack a U.S. whole of government approach; a lack of trust among stakeholders; a lack of policy, procedures, business practices, and people; and organizational culture differences. It is not a technology challenge per se, generally, technology is an enabler if properly employed.

The chapter concludes that civil-military collaboration and information sharing activities and the smart use of information and ICT can have decisive impacts if they are treated as a core part of the nation's overall strategy and not just as "nice to have" adjuncts to HA/DR initiatives, or to the kinetic phases of warfare and stability and reconstruction operations. It is further suggested that utilizing the elements of the information revolution and the whole of government in a strategic approach to HA/DR and stability and reconstruction operations can have positive results and sets forth the strategic and operational parameters of such an effort. Finally, enhancing the influence of USG responses to HA/DR and interventions in stability and reconstruction operations will require a multifaceted strategy that differentiates the circumstances of the messages, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers.

LEGAL AND SOCIAL ASPECTS

Cybercrime and attack dynamics are explored in Part II of this book. The first chapter is presented by Michael M. Losavio, J. Eagle Shutt, and Deborah Wilson Keeling. The chapter examines how public policy may evolve to adequately address cybercrime. Historically, legal protections against criminal activity have been developed in a world wherein any criminal violation was coupled with physical proximity. Global information networks have created criminal opportunities in which criminal violation and physical proximity are decoupled.

In Chapter 6, the authors argue that cyberspace public policy has not adequately incentivized and sup-

ported protective behaviors in the cyber community. They examine the roles that user-level/consumer-level conduct, social engagement, and administrative policy play in protecting information infrastructure. They suggest proactive work with laws and administrative/citizen-level engagement to reform the cyberspace community. To that end, they examine applicable legal and transnational regimes that impact such a strategy and the options for expanding administrative and citizen engagement in the cyber security enterprise.

Chapter 7, by Thomas J. Holt, is titled, "The Attack Dynamics of Political and Religiously Motivated Hackers." There is a significant body of research focused on mitigating attacks through technical solutions. Though these studies are critical for decreasing the impact of various vulnerabilities and hacks, researchers still pay generally little attention to the affect that motivations play in the frequency, type, and severity of hacker activity. Economic gain and social status have been identified as critical drivers of computer hacker behavior in the past, but few have considered how nationalism and religious beliefs influence the activities of some hacker communities. Such attacks are, however, gaining prominence and pose a risk to critical infrastructure and web-based resources. For example, a number of Turkish hackers engaged in high profile web defacements against Danish websites that featured a cartoon of the prophet Muhammad in 2007. To expand our understanding of religious and nationalist cyber attack, this chapter explores the active and emerging hacker community in the Muslim-majority nation of Turkey. Using multiple qualitative data sets, including interviews with active hackers and posts from multiple web forums, the findings ex-

plore the nature of attacks, target selection, the role of peers in facilitating attacks, and justifications through the lens of religious and national pride. The results can benefit information security professionals, law enforcement, and the intelligence community by providing unique insights on the social dynamics driving hacker activity.

TECHNICAL ASPECTS

The five chapters in Part III characterize the technical and architectural issues of cyber security.

Chapter 8, by Yehia Khalil and Adel Elmaghraby, deals with the topic of the resilience of data centers. Data centers are the core of all legacy information in a cyber society. With the incredible growth of critical data volumes in financial institutions, government organizations, and global companies, data centers are becoming larger and more distributed, posing more challenges for operational continuity in the presence of experienced cyber attackers and the occasional natural disasters. The need for resilience assessment emerged due to the gap in existing reliability, availability, and serviceability (RAS) measures. Resilience as an evaluation metric leads to better system design and management; this chapter illustrates why resilience evaluation is needed and it surveys the continuing research.

Chapter 9, by Edward Wagner and Anup K. Ghosh, covers the development of high fidelity sensors for intrusion activity on enterprise networks. Future success in cyber will require flexible security, which can respond to the dynamic nature of current and future threats. Much of our current defenses are based upon fixed defenses that attempt to protect in-

ternal assets against external threats. Appliances like firewalls and proxies positioned at network segment perimeters similar to the Maginot Line attempt to shield us from outsiders attempting to break in. There are other mechanisms such as public key infrastructure and antivirus software within the network perimeter. This added layer is referred to as "Defense in Depth" methodology. However, in each component of security architecture, vulnerabilities are revealed over time. These defenses lack any agility; their defenses must become agile and responsive. They propose high fidelity sensors in the form of virtualized applications on each user's machine to complement network-based sensors. In addition, they equip each user such that even as they are reporting intrusions, their machine and data are protected from the intrusions they are reporting. Their approach is able to protect users from broad classes of malicious code attacks, while being able to detect and report both known and unknown attack code.

IP networks are no longer optional throughout the business and government sectors. This fact, along with the emergence of international regulations on security, reliability, and quality of service (QoS), means that IP network assessment is also no longer an option. With IP networks representing the core of our cyber infrastructure, the lack of deep understanding of such networking infrastructure may lead to drastic strategic implications and may limit our ability to provide a solid cyber infrastructure. The remaining chapters in Part III focus exclusively on IP networks.

In Chapter 10, Angelos Keromytis, indicates that voice over IP (VoIP) and similar technologies are increasingly accepted and used by enterprises, consumers, and governments**.** They are attractive to all these

entities due to their increased flexibility, lower costs, and new capabilities. However, these benefits come at the cost of increased complexity, reliance on untested software, and a heightened risk of fraud. In this chapter, the author provides an overview of VoIP technologies, outlines the risks and threats against them, and highlights some vulnerabilities that have been discovered to date. The chapter closes with a discussion of possible directions for addressing some of these issues, including the work in the ANR VAMPIRE project, which seeks to understand the parameters of the problem space and the extent of VoIP-related malicious activity.

Chapter 11, by Rajesh Talpade, discusses foolproof IP network configuration assessment. IP networks have come of age. They are increasingly replacing leased-line data infrastructure and traditional phone service, and are expected to offer Public Switched Telephone Network (PSTN)-quality service at a much lower cost. As a result, there is an urgent need for assuring IP network security, reliability, and QoS. In fact, regulators are now requiring compliance with IP-related mandates. This chapter discusses the complex nature of IP networks, and how that complexity makes them particularly vulnerable to faults and intrusions. It describes regulatory efforts to mandate IP network assessment, explains why many current approaches to assessment fall short, and describes the requirements for an effective solution to satisfy business, government, and regulatory requirements.

In Chapter 12, Nirwan Ansari and Amey Shevtekar provide an overview on the new breed of denial of service (DoS) attacks on the Internet. Denial of service attacks impose serious threats to the Internet. Many attackers are professionals who are motivated by finan-

cial gain. They bring a higher level of sophistication along with inventive attack techniques that can evade detection. For example a shrew attack is a new type of threat to the Internet; it was first reported in 2003, and several of these types of attacks have emerged since. These attacks are lethal because of the inability of traditional detection systems to detect them. They possess several traits, such as low average rate and the use of transmission control protocol (TCP) as attack traffic, that empower them to evade detection. Little progress has been made in mitigating these attacks. This chapter presents an overview of this new breed of DoS attacks along with proposed detection systems for mitigating them. The chapter will lead to a better understanding of these attacks, and will stimulate further development of effective algorithms to detect these attacks and to identify new vulnerabilities which have yet to be discovered.

ENDNOTES – CHAPTER 1

1 . Available from *www.ccny.cuny.edu/cip09*.

PART I

STRATEGY AND POLICY ASPECTS

CHAPTER 2

DEVELOPING A THEORY OF CYBERPOWER*

Stuart H. Starr

INTRODUCTION

The goal of this chapter is to develop a preliminary theory of cyberpower. A theory of cyberpower will try to achieve five objectives.[1] First, it will establish a framework that will categorize the various elements of the cyber domain. Second, it will define the key terms of interest. Third, it will begin to make clear the various benchmarks and principles that explain the various cyber categories. Fourth, it will characterize the degree to which the various categories of the cyber domain are connected. Finally, it will anticipate key changes in the cyber domain and provide a basis for analyzing them.

However, it must be emphasized that this evolving theory is in its preliminary stages. Thus, it is to be anticipated that it will not be complete. In addition, given the long gestation period for theories of "hard science" (e.g., physics, chemistry, and biology), it is likely that some of the elements are likely to be wrong.

---

* The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. All information and sources for this chapter were drawn from unclassified materials.

ELEMENTS OF A THEORY

Categorize.

In analyzing the cyber domain, four key areas emerge (see Figure 2.1). These include the cyber-infrastructure ("cyberspace"), the levers of national power (i.e., diplomacy, information, military, economic [DIME], or "cyberpower"), the degree to which key entities are empowered by changes in cyberspace ("cyberstrategy"), and the institutional factors that affect the cyber domain (e.g., legal, governance, and organization). For the purposes of this chapter, this framework will be employed to decompose the problem.

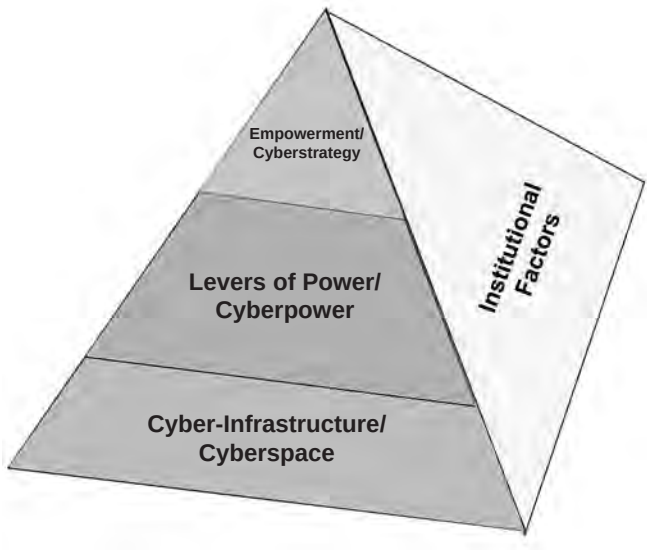

Figure 2.1. A Framework for Categorizing the Cyber Problem.

Define.

Although the definitions of many of these terms are still contentious, this chapter will use the following definitions of key terms. First is the formal definition of cyberspace that the Deputy Secretary of Defense formulated: ". . . the interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries."[2] This definition does not explicitly deal with the information and cognitive dimensions of the problem. To deal with those aspects explicitly, we have introduced two complementary terms, "cyberpower" and "cyberstrategy," which were defined by Professor Dan Kuehl, National Defense University (NDU).

The term cyberpower means "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."[3] In this context, the instruments of power include the elements of the DIME paradigm. For the purposes of this evolving theory, primary emphasis will be placed on the military and informational levers of power.

Similarly, the term cyberstrategy is defined as "the development and employment of capabilities to operate in cyberspace, integrated and coordinated with the other operational domains, to achieve or support the achievement of objectives across the elements of national power."[4] Thus, one of the key issues associated with cyberstrategy deals with the challenge of devising "tailored deterrence" to affect the behavior of the key entities empowered by developments in cyberspace.

Explain.

Cyberspace. Over the last 15 years, a set of rules of thumb have emerged to characterize cyberspace. Some of the more notable of these rules of thumb include the following:

- Moore's Law (i.e., the number of transistors on a chip approximately doubles every 18 months);[5]
- Gilder's Law ("total bandwidth of communication systems triples every 12 months");[6]
- Proliferation of IP addresses in transitioning from IPv4 to IPv6 (e.g., IPv6 will provide 2^{128} addresses; this would provide $5x10^{28}$ addresses for each of the 6.5 billion people alive today).

In addition, recent analyses have suggested the following straw man principles for cyberspace. First, the offensive has the advantage. This is due to the challenges of attribution of an attack and the fact that an adversary faces a "target rich" environment. Consequently, if cyberspace is to be more resistant to attack, it may require a new architecture that has "designed in" security.

Cyberpower. Robert Metcalfe formulated one of the oft-quoted laws of cyberpower.[7] He characterized the value of a network as "N^2," where N describes the number of people who are part of the network. However, more recently, it has been demonstrated that the value of a network tends to vary as N*log (N). Note that this equation suggests that the "value" of a network is substantially less than "Metcalfe's Law."[8]

In addition, there have been many studies about the contribution that net-centricity can have to mission effectiveness. For example, studies of air-to-

air combat suggest that the value of a digital link (e.g., Link 16) can enhance air-to-air loss exchange ratios by approximately 2.5.[9] This is due to the enhanced situation awareness, improved engagement geometry and the efficiency of the engagement. However, the complexity of modern conflict is such that it is difficult to assess the affect of net-centricity on complex missions. Thus, for example, studies of air-land operations are much more complex and very scenario-dependent. In addition, preliminary studies of humanitarian assistance/disaster relief and stability operations are currently underway. Chapter 5 in this book will provide preliminary results for those operations.

Cyberstrategy. Recent studies have suggested that the "low end" users (e.g., individuals, "hacktivists," terrorists, and transnational criminals) have considerably enhanced their power through recent cyberspace trends.[10] This is due, in part, to the low cost of entry into cyberspace (e.g., the low cost for a sophisticated computer or cell phone; the extensive investment that the commercial world has made in cyberspace (e.g., applications such as Google Earth); and the major investments in cyberspace that have been made by governments (e.g., the Global Positioning System).

Similarly, potential near-peer adversaries are aggressively exploring options to exploit attributes of cyberspace (e.g., exfiltration of data; distributed denial of service attacks, and implementation of innovative cyber stratagems). These activities have been well-documented in recent news accounts.[11]

From a U.S. perspective, new concepts and initiatives are emerging from the Comprehensive National Cyber Initiative (CNCI). At a minimum, it has been recommended that the United States must incorporate a creative and aggressive cyber "opposing force" to stress the system in future experiments and exercises.

Institutional Factors. Over the last several years, a number of studies have been conducted to address the issues of cyberspace governance, the legal dimension of cyberspace and cyberpower, the tension between civil liberties and national security, and the sharing of information between the public and private sectors. In the area of cyberspace governance, there is a growing appreciation that one should seek *influence* over cyberspace vice *governance.* In the near term, there are a number of policy governance issues that remain to be addressed (e.g., the extension of the contract of the Internet Corporation for Assigned Names and Numbers [ICANN]; and the role of the International Telecommunications Union [ITU] in cyber governance).

The legal dimension of cyberspace has barely addressed the key issues that must be resolved during the next decade. For example, the issues of concern include: what is an act of cyber war; what is a proportionate reaction to an act of cyber war; how should one treat intellectual property in cyberspace; how should one resolve differences in sovereign laws and international treaties.

It is broadly recognized that there is a need for a framework and enhanced dialogue to harmonize the efforts of civil liberties and proponents of enhanced national security**.** This issue is being pursed as a component of the CNCI initiative.

Finally, many studies have cited the need to address the issue of sharing of cyber information between the U.S. Government and industry. However, there is still a need to provide guidance and procedures to clarify this issue.

Connect.

It is well understood that the various categories of the cyber domain are strongly interconnected. To address this problem, there is a need for a family of Measures of Merit (MoM) to provide that linkage (see Figure 2.2).

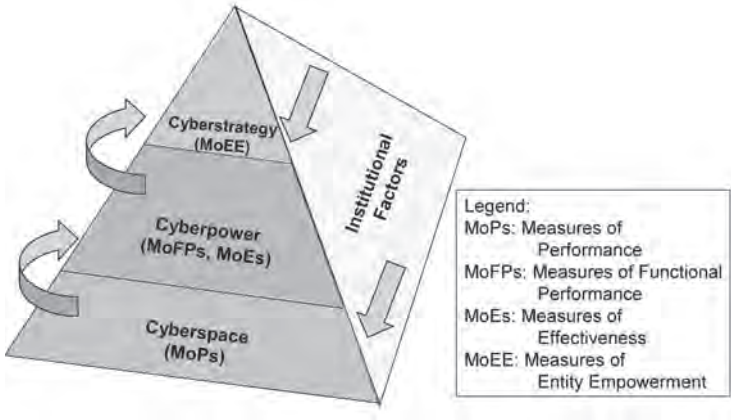

Figure 2.2. Representative Measures of Merit.

For example, cyberspace can be characterized by a set of Measures of Performance (MoPs). These might include performance in cyberspace (e.g., connectivity, bandwidth, and latency) and resistance to adversary countermeasures (e.g., resistance to distributed denial of service attacks, resistance to exfiltration attempts, and resistance to corruption of data).

In the areas of cyberpower, it is useful to think about Measures of Functional Performance (MoFP) and Measures of Effectiveness (MoE). For example, in the case of air-to-air combat, appropriate MoFP

might be the range at which air combatants are able to detect, identify, and characterize unknown aircraft. Similarly, loss exchange ratios may be suitable MoE.

In the area of cyberstrategy, one might use political, military, economic, social, information, and infrastructure (PMESII) measures to characterize Measures of Entity Empowerment (MoEE). Thus, for example, one could characterize the extent to which changes in cyberspace might effect changes in politics (e.g., the number of people who vote in an election), military status (e.g., the enhancement in the security of the population), economic factors (e.g., the change in unemployment statistics), social (e.g., ability of diverse social groups to live in harmony), information (e.g., the extent to which social networks support political activity), and infrastructure (e.g., the extent to which improvements in supervisory control and data acquisition [SCADA] systems enhance the availability of electricity and clean water). The actual MoEE will have to be tailored to the entity that is being empowered by changes in cyberspace. Thus, a terrorist, who seeks to, *inter alia,* proselytize, raise money, educate, and train, would have a different set of MoEE.

Finally, one needs to formulate MoMs that are appropriate for issues of governance; legal issues, civil liberties, critical infrastructure protection, and cyber reorganization. Work is currently ongoing in those fields.

Anticipate.

From the perspective of a senior decisionmaker, the key challenge is anticipating the key issues of interest and performing the analyses needed to make knowledgeable decisions.

In the area of cyberspace, it is important to perform technology projections to identify potential key breakthroughs (e.g., cloud computing); explore options to enhance attribution in cyberspace; develop techniques to protect essential data from exfiltration or corruption; and formulate an objective network architecture that is more secure and identify options to transition to it.

In the area of cyberpower, it is important to extend existing analyses to assess the impact of changes in cyberspace on the other elements of power (e.g., diplomatic and economic) and to perform risk assessments to guide future policy decisions.

In the area of cyberstrategy, additional research is needed to guide the development of "tailored deterrence" (particularly against nonstate actors) and to explore options to thwart the efforts of key entities to perform cyber espionage.

In the area of institutional factors, the major challenges are to address the legal issues associated with the cyber domain and to harmonize civil liberties and national security.

Overall, there is a need to develop assessment methods, tools, data, services (e.g., verification, validation, and accreditation [VV&A]), and intellectual capital to assess cyber issues. Figure 2.3 suggests the relative maturity of key tools in the areas of cyberspace, cyberpower, cyberstrategy, and institutional factors.

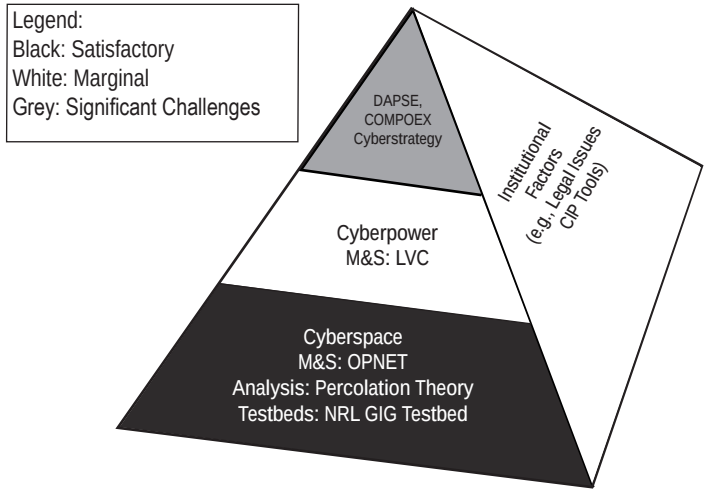

Figure 2.3. State-of-the-Practice in Assessing Cyber Issues.

In the area of cyberspace, there are several tools that the community is employing to address computer science and communications issues. Perhaps the best known is the operations network (OPNET) simulation that is widely employed to address network architectural issues.[12] From an analytic perspective, techniques such as percolation theory enable one to evaluate the robustness of a network.[13] Looking to the future, the National Research Laboratory (NRL) has developed a Global Information Grid (GIG) Testbed to explore the myriad issues associated with linking new systems and networks.

In the area of cyberpower, the community has had some success in employing live, virtual, and constructive simulations. For example, in assessments of air-to-air combat, insights have been derived from the

live Air Intercept Missile Evaluation/Air Combat Evaluation (AIMVAL-ACEVAL) experiments, virtual experiments in the former McDonnell Air Combat Simulator (MACS), and constructive experiments using tools such as TAC BRAWLER. However, the community still requires better tools to assess the impact of advances in cyberspace on broader military and informational effectiveness (e.g., land combat in complex terrain).

In the area of cyberstrategy, a number of promising initiatives are underway. In response to a recent tasking by Strategic Command (STRATCOM), a new methodology and associated tools are emerging (i.e., Deterrence Analysis & Planning Support Environment [DAPSE]).[14] However, these results have not yet been applied to major cyberstrategy issues. In addition, promising tools are emerging from academia (e.g., Senturion; GMU's Pythia) and Defense Advanced Research Projects Agency (DARPA) (e.g., Conflict Modeling, Planning & Outcomes Experimentation [COMPOEX]). However, these are still in early stages of development and application.

Finally, as noted above, there are only primitive tools available to address issues of governance, legal issues, and civil liberties. Some tools are being developed to explore the cascading effects among critical infrastructures (e.g., National Infrastructure Simulation and Analysis Center [NISAC] system dynamics models); however, they have not yet undergone rigorous validation.[15]

KEY CHALLENGES

Theories for the "hard" sciences have taken hundreds of years to evolve. However, this preliminary "theory of cyberpower" is approximately only 1-year

old! As a consequence, there is a great deal of work that remains to be done in each of the areas of interest.

In the area of Categorize, it is understood that the preliminary framework is just one way of decomposing the problem. It is necessary to formulate alternative frameworks to support further decomposition of the cyber domain.

In the area of Define, there has been a great deal of contention over the most basic terms (e.g., cyberspace and domain). Steps must be taken in the near term to develop a taxonomy that will formulate and define the key terms of interest.

In the area of Explain, it is understood that we are just beginning to deal with a very complex and time-variable problem set. It is vital to conduct studies to create benchmarks and to gain a deeper understanding of key cyber issues.

In the area of Connect, the selection of MoMs is in its infancy. We must consider all of the entities that are being empowered by changes in cyberspace and develop appropriate MoMs for them.

Finally, in the area of Anticipate, we understand the challenge in trying to predict the evolution of cyberspace. At a minimum, we need to generate a research agenda to address unresolved cyber issues. This should include the development of methods, tools, data, services (e.g., VV&A), and intellectual capital to attack many of these problems.

ENDNOTES - CHAPTER 2

1. Dr. Harold R. Winton, "An Imperfect Jewel," presented at INSS workshop on the Theory of Warfare at the National Defense University, Washington, DC, September 2006.

2. Deputy Secretary of Defense Memorandum, "The Definition of Cyberspace," Washington, DC: Department of Defense May 12, 2008.

3. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem." in Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz, Eds., *Cyberpower and National Security,* Washington, DC: Center for Technology and National Security Policy, National Defense University, Potomac Books, Inc., 2009, p .48.

4. *Ibid.,* p. 40.

5. Sally Adee, "37 Years of Moore's Law," *IEEE Spectrum*, May 2008.

6. Rich Kalgaard, "Ten Laws of the Modern World," April 19, 2005, available from *Forbes.com*.

7. George Gilder, "Metcalfe's Law and Legacy," *Forbes ASAP*, September 13, 1993.

8. Bob Briscoe, Andrew Odlyzko, and Benjamin Tilly, "Metcalfe's Law is Wrong," *IEEE Spectrum*, July 2006.

9. Dan Gonzales *et al.*, "Network-Centric Operations Case Study: Air-to-Air Combat With and Without Link 16," Santa Monica, CA: RAND Corporation, National Defense Research Institute, 2005.

10. Irving Lachow, "Cyber Terrorism: Menace or Myth?" Chap. 19, *Cyberpower and National Security*, Bethesda, MD: Potomac Press, 2009.

11. John Markoff, "Vast Spy System Loots Computers in 103 Countries," *New York Times*, March 29, 2009.

12. Emad Aboelela, "Network Simulation Experiments Manual," Amsterdam: Morgan Kaufmann Publishers, 3rd Ed., June 2003.

13. Ira Kohlberg, "Percolation Theory of Coupled Infrastructures," 2007 Homeland Security Symposium entitled "Cascading

Infrastructure Failures: Avoidance and Response," Washington, DC: National Academies of Sciences, May 2007.

14. "Deterrence in the 21st Century: An Effects-Based Approach in An Interconnected World, Vol. I," Nancy Chesser, ed., *Strategic Multi-Layer Analysis Team*, USSTRATCOM Global Innovation and Strategy Center, October 1, 2007.

15. Colonel William Wimbish and Major Jeffrey Sterling, "A National Infrastructure Simulation and Analysis Center (NISAC): Strategic Leader Education and Formulation of Critical Infrastructure Policies," Carlisle, PA: Center for Strategic Leadership, U.S. Army War College, August 2003.

CHAPTER 3

SURVIVABILITY OF THE INTERNET

Michael J. Chumer

INTRODUCTION

In 2007, a symposium was sponsored by the New Jersey Business Force (NJBF) and SunGard. During the symposium, a panel of experts posed a series of questions that were then addressed in detail by work-groups drawn from the symposium participants. This chapter presents the key issues identified by those issues that affect the resilience and survivability of the Internet during a pandemic declaration.

The use of the "commodity" Internet, referred to simply as the Internet, is the cornerstone of private and public sector communication, application access and use, information sharing, and a host of taken-for-granted usages. During the SunGard[1] and NJBF[2] symposium in 2007, the key question posed and addressed was, "Will the Internet Be There When You Really Need It?"[3] The planning symposium focused on the effects on the Internet if a pandemic based upon H5N1 (the bird flu) was to break out in the United States. In addition, the symposium addressed reciprocal effects on businesses given a marginally functioning Internet.

From the middle of April 2009 to the present, the United States has been in a pre-pandemic event suggested by the World Health Organization (WHO) as stage 5.[4] This in turn has caused many private sector organizations to review their pandemic plans and take the necessary steps to revise and adjust them in anticipation of a pandemic declaration. The virus

strain is called H1N1 (swine flu) instead of the H5N1, but that does not alter the business planning process or the steps that make sense for organizations to take in preparation of such a declaration.

As the symposium suggested, a pandemic plan should consider the availability of the Internet for business continuity, given that social distancing will be required. Social distancing will affect all employees, to include "key" personnel. As personnel work from home, the traffic on the Internet will change in a way where certain Internet Service Providers (ISP) may encounter Internet traffic loads that were not anticipated.

SYMPOSIUM DATA COLLECTION

The symposium was conducted as a modified table top exercise (TTX). In the morning, presentations were given that addressed the H5N1 virus along with predictions on how it might spread in the United States; who would be at risk; the role of the public sector, personal protection and the responsibility of the individual; and some initial thoughts about the role and concerns of business and business continuity planning in general. Initial presentations by 10 experts were followed by a facilitated panel discussion designed to surface issues that would later be discussed in detail by the symposium participants.

Subsequent to the panel discussion, the 110 participants were divided into workgroups which engaged in a TTX that addressed in more detail the major questions that surfaced during the panel discussion.

Data that resulted from the panel discussion and from the individual workgroup TTXs were captured and analyzed by a team of researchers. The key items

in the panel and TTX data were identified, resulting in a white paper jointly authored by the NJBF and SunGard.[5] Most of the material contained in the white paper has been incorporated and reassessed in this chapter.[6]

In the white paper, a series of topical area issues posed as questions were developed:

- **Business continuity effects due to Internet reduced availability**. What are the foreseeable short-term and long-term impacts if the Internet either "crashes," "goes down," or "stops working"?
- **Service provider collaboration for the collective good**. Explain whether existing protocols for providing collaboration and coordination between U.S. service providers (cable, telephone, and "last mile" providers) are sufficient enough to preserve Internet access and limit overload.
- **Points of Internet failure**. What must planners consider when modifying or developing business practices?
- **The effects on computer applications and/or protocols**. What are the effects on applications and/or protocols if the Internet slows down rather than halting during a pandemic, as well as mitigation strategies for such an event?
- **Increased Internet demand**. In the face of heavy demand on the Internet, which features or services should contingency planners expect to shut down or redirect to conserve or preserve bandwidth?
- **Hacker Attacks**. Should contingency planners expect attacks from hackers during a state when the Internet is weakened?

- **Growing Internet Reliability**. Whether we as a nation are depending too much on the Internet and underestimating its risks for the sake of cost, convenience, and efficiency?
- **Internet Resilience**. Will the Internet be resilient enough to hold up under the onslaught of school, business, home enterprise, emergency management, and recreational users during a pandemic?

CURRENT ESCALATING SITUATION

On June 11, 2009, the WHO raised the pandemic alert level from phase 5 to phase 6, which indicates the start of a full-fledged worldwide pandemic. This declaration, in turn, suggests that certain actions or behaviors should be "triggered" within organizations (the public and/or private sector). The general discussion that follows in the next section reveals answers to questions about the effects of a pandemic declaration on the Internet. Many business organizations, in turn, are reviewing their current continuity of operations plans (COOPS), and public sector organizations also are reviewing their continuity of government plans (COOGS). The next section also provides guidance to organizations about what issues they need to address to ensure that business can continue to function and continue to survive during a pandemic.

That section also indicates that the "commodity" Internet plays a significant and vital role in the ability of business to do business. The Internet is a critical component within the supply-and-value chain of each organization, linking businesses as the producers of products and/or the providers of services to the customers that benefit from those products and services.

The reliance on the Internet has grown over the past 16 years (the backbone of the Internet was contracted in 1993 or outsourced by the National Science Foundation to the private sector). This growth has been exponential and, along with it, a growing dependency and interdependency has occurred, with the tacit belief that the Internet will always be there. Businesses have developed processes and procedures where the Internet is a critical component. If the Internet slows down significantly, which may occur during a pandemic, or even cease to function in certain parts of the country due to unexpected traffic patterns, coupled with denial of service attacks, business and governments need to be prepared. This will not be an easy task.

GENERAL DISCUSSION

The sections that follow discuss in detail the answers to the questions that were posed to symposium attendees through the panel discussion and the subsequent TTX. Each section provides planning guidance to both organizational planners and organizational emergency management/security functions.

Business Continuity Effects Due to Internet Reduced Availability with Examples of Healthcare and Education.

The symposium data suggested that healthcare and education would be greatly impacted over the long term during periods of reduced availability. In 2006, healthcare approached one-sixth of the gross domestic product (GDP), inferring that the economic impact during periods of reduced Internet availability would be significant. The amount of communication

being passed over the Internet due to patient electronic records, clinical data being shared geographically, and the bandwidth of clinical data, especially those requiring visualization, would all suffer time lags and delays with the ultimate potential of affecting patient diagnostics and treatment protocols.

A significant percentage of education from K-12 is still done face-to-face (F2F), suggesting that during periods of social distancing, essential delivery of education material would not occur. When education delivery is viewed at the community college or college level, we do see a movement toward both distance learning and hybrid (blended learning) course delivery. However, the majority of distance learning courses are delivered over home-to-school Internet connections, suggesting that some delays in the delivery of course content would occur during periods of reduced Internet availability.

In addition, over the short term, e-mails—which in 2006 averaged 84 billion per day—voice over Internet protocol (VOIP), and instant messaging would be affected. This will leave those people whose social networks are tied to a virtual space to seek out different forms of social networking. It might be very difficult during periods of social distancing for those individuals and collectives that rely on virtual communication to adapt to both physical and virtual isolation.

Service Provider Collaboration for the Collective Good.

The symposium discussed whether existing protocols for providing collaboration and coordination between U.S. service providers (cable, telephone, and "last mile" providers) are sufficient enough to pre-

serve Internet access and limit overload. Discussion for this topic was robust. It is clear that the ownership of the Internet resides with the private sector and, in that vein, there is some but not a lot of coordination between Internet "backbone" providers to ensure that infrastructure "build-outs" keep up with capacity demands. However, during a pandemic or any emergency situation which may require a reduction of Internet traffic, existing protocols are either insufficient or do not exist. Furthermore, the symposium data suggested,

> To date the private sector has established no definitive industry standards governing Internet user priorities and preferences in the event of a catastrophic event or an 'incident of national significance.'[7]

This gets into the entire notion of establishing priorities during periods of reduced Internet availability. Recommendations emerging from the symposium include the following:

- In emergency situations; forming an advisory group comprising Internet Service Providers and Government representatives to address key issues;
- Expanding the role of existing ISP groups (FISPA) to include formulating policies.

As the discussion moved forward, a further suggestion was that, during a pandemic or a national emergency, each organization should "voluntarily" reduce their Internet traffic by 10 percent below peak levels. Additional symposium recommendations in this area were:

- limiting video streaming and VoIP;
- adopting off-hour business solutions;

- prioritizing business applications;
- blocking noncritical Internet traffic.[8]

This is certainly an area open to more debate, such as addressing the role government should play in Internet traffic regulation during emergency situations and/or periods of reduced Internet availability. The consensus was that the government should be a partner with the private sector with limited intervention.

Points of Internet Failure.

The symposium data indicated that planners must consider access infrastructure and bandwidth as they develop business practices that focus on their continuity of operations. Access infrastructure must be planned from business locations to the first ISP and also from a "critical" employee location to that employee's primary ISP. Businesses for the most part do a good job in monitoring their network traffic to include their Internet access points. There are often "first" and "last mile" issues which suggest that redundancy of access becomes a critical part of the plan. However, what is often overlooked is the access that critical employees should have from their home location. This becomes an important planning consideration during social distancing when the tacit expectation is that an employee can access organizational applications from their home location as they would from their work location. For employees, the issue of "first" and "last mile" redundancy becomes salient as well. This suggests that organizational planners should possess an inventory of critical employee home access capabilities which might suggest redundant Internet access from a home location.

Bandwidth is the second item that planners must consider. Again, this is important at business locations, but becomes more important when employees work at home. We are in an era where audio, video, and graphics are transmitted over Internet infrastructures. Many organizational applications are developed for a thin client architecture where most of the processing is performed on organizational servers. This architecture suggests that significant bandwidth capacity may be required to access web-based organizational applications.

The symposium data indicated that the following are the least likely points of failure: "Among the least likely points of failure are Domain Name Servers (DNS), corporate high-capacity bandwidth, local exchange carrier, and redundant corporate routing."[9]

The Effects on Computer Applications and/or Protocols.

What are the effects on applications and/or protocols if the Internet slows down rather than halting during a pandemic, as well as mitigation strategies? Symposium data suggested that this question is tightly coupled to the role that the Internet plays within organizational supply and value chains.[10] Much of organizational supply and value chains are outsourced to different organizations (vendors or partners) requiring "tight coupling"[11] from a communication perspective. This suggests that access and bandwidth considerations that were previously addressed take on a significant level of importance.

In conjunction with supply and value chain considerations unique to the specific organization, there is the entire issue of supply/value chain interdependen-

cies and critical application access.[12] Business environments where a "just in time" mentality has developed suggests a business continuity focus on stabilizing the supply chain during a pandemic or incident of national significance. The symposium indicated that the supply/value chain issue should be stabilized first before employee essential needs of "food, water, and healthcare" should be addressed.[13]

Increased Internet Demand.

In the face of heavy demand on the Internet, which features or services should contingency planners expect to shut down or redirect to conserve or preserve bandwidth? The Internet has become less of an "amenity" and more of an "expectation."[14] Witness that what began as a service that hotels would offer to gain a competitive advantage has now become a common expectation of business travelers. Since the expectation for robust and ubiquitous Internet services has been set, restricting usage would be met by a general resistance from the public writ large. This resistance could be somewhat overcome by requesting the public to engage in behavior directed toward voluntary restrictions on their Internet use. However, the symposium indicated that "Voluntary restrictions would have to be imposed for limited periods, applied equitably, and based on established priorities."[15] It was recommended that the public sector, especially the individual states, develop a list of priority users and suggested the following:

- "Urgent (utilities, public service networks, government),
- Priority (commodity transportation, food, medicine, relief supplies),
- Normal (those not listed above)."[16]

What was not mentioned at the symposium but has relevance here is the development of a priority switching scheme for critical Internet services. At present there is "Internet 2"[17] and "The National Lambda Rail."[18] Both are services that possess fiber backbones which are separate from the basic backbone infrastructure of the commodity Internet. Once developed, urgent and priority services could benefit by being switched during an emergency to one of these high bandwidth, high capacity services.

Hacker Attacks.

Should contingency planners expect attacks from hackers during a state when the Internet is weakened? The symposium data indicated that the cyber infrastructure used by organizations is always at risk from hackers and from a variety of sources initiating unwanted intrusions. During a pandemic, it was agreed that the weakened state of the commodity Internet has the potential of putting organizations at a higher level of risk. The greatest vulnerabilities will be in the areas of online banking and the movement of critical operations to the commodity Internet.

It is expected that during periods of social distancing, online banking activity will increase significantly which would open up opportunities for hacking. Additionally, as more organizationally "critical" application functions move to the Internet due to employees performing telework, this will become a target for hacking activity as well. Hackers are not averse to taking advantage of other vulnerabilities. It was agreed that identify theft activities would increase significantly, especially targeting people who died as a re-

sult of the pandemic. Finally, the weakened state of the Internet could spawn denial of service activity. The white paper suggested the following as potential remedies:

> Businesses should consider adding varying degrees of redundancy and security during their preparations. They can improve the security of online, networked operations during the mass migration of critical functions and services, including telecommuting, to the Internet. Specifically, companies can step up enforcement of standard security controls and policies (e.g., firewalls).
>
> They also can install encryption software, limit employee access and privileges to e-mail, and control access to major non-mission-critical business processes. They can increase the frequency of mandatory password resets, require two-factor authentication, set tighter controls over extra-net partners, implement more aggressive patch management, and increase monitoring of the cyber or virtual environment.[19]

Growing Internet Reliability.

Are we as a nation becoming too dependent on the Internet and underestimating its risks for the sake of cost, convenience, and efficiency? Internet dependency has been growing since the National Science Foundation allowed the commercialization of the Internet backbone in 1993. E-mail communication has increased significantly each year, and services like "Facebook"[20] and "Twitter"[21] are beginning to redefine technology based "social networking." Blogging activity is increasing, as well as online shopping. So we as a nation and as a society have become very dependent upon the Internet and have incorporated its

use into everyday life. The Internet has become extremely convenient.

The convenience of the Internet needs to be balanced against potential risks. An understanding of this balance and the steps that should be taken by people in general, and organizational employees specifically, suggest focus and constant reinforcement on education. This education should address and develop an understanding of the risks of the Internet and its counterbalance—the rewards of Internet use.

A list of planning guidelines that organizations should follow for both educating themselves as well as educating their employees is included in the appendix. During the symposium, the value of developing a risk–reward education program was stressed in order to further develop an understanding of the risks and vulnerabilities of Internet use and access.

Internet Resilience.

Will the Internet and ISPs be resilient enough to hold up under the onslaught of school, business, home enterprise, emergency management, and recreational users during a pandemic?[22] The ability for ISPs to engineer their capacity in such a way where they are able to accommodate this surge becomes important. It is expected that the Internet will not "break" during a pandemic, but it will certainly "bend" under the surge in expected use.

The white paper suggested areas that need to be addressed to begin to ensure that the Internet is as resilient as possible. These are:

> The goal would be to avoid or eliminate single points of failure; establish reliability standards; have multiple geographically isolated Post Office Protocal (POP)

servers; and ensure redundancy using non-terrestrial communications to geographically diverse ground stations. In addition, Tier 1 and 2 providers could manage bandwidth for Tier 3 and 4 providers, allowing maximum efficiency in meeting the expected surge in demand for Internet bandwidth.[23]

CONCLUSION

In general, it was concluded that the backbone of the Internet is fairly "robust" and should be capable of withstanding the surge that would be expected during the initial stages of a pandemic declaration. However, the points of backbone access and the ability to address local surge issues may cause the Internet to bend to levels that may be unacceptable to local users. The white paper that followed the symposium concluded with the following recommendation, included here in its entirety:

> In the U.S., the Internet is analogous to private and commercial cars and trucks, i.e., it is indispensable. Continuity of Operations (COOP) planners must take threats to Internet availability as seriously as they would take threats to the availability of gasoline.
>
> The direct and indirect threats a pandemic would pose to the Internet are genuine.
>
> The potential for hostile human interference—for example, terrorist attacks or other disruptive behavior—during a pandemic should be factored into continuity plans. The U.S. economy remains a high-value target, and America's enemies probably would attempt to exploit a pandemic through asymmetrical warfare (e.g., cyber attacks) to further weaken the economy and therefore the country.

Degradation or loss of Internet service during a pandemic may reduce businesses to a state Herbert Spencer described as 'survival of the fittest.' In this environment, organizations that were well prepared beforehand will have the best chance of prevailing. To improve their chances, companies can:

- Engineer systems for peak usage by expanding capacity or reserving additional bandwidth,
- Eliminate or reduce vulnerabilities, and
- Educate employees to take care of themselves.

Internet Service Providers (ISPs) and government representatives should form a joint task force to develop an Internet assurance strategy and voluntary guidelines for implementation during a pandemic. However, while the private sector probably would accept voluntary controls over Internet use during a pandemic, as long as limitations and restrictions are justifiable and equitably applied, government-directed mandates could be opposed as Marshall Law.

Identify potential problems now by conducting comprehensive exercises that would stress IT systems. Companies could conduct tests locally at first, adopting a process of continuous review that would integrate technology issues into overall planning efforts, incorporate the legal and human resources functions into the planning process, ensure that critical employees have primary and secondary means of communication, develop policies and standard operating procedures for mission critical functions, and establish a worst-case scenario as a baseline for testing. Companies could then coordinate regional exercises with government and other businesses.

The supply chain is a national center of gravity, and the Internet is an integral component of America's economic engine. These are a foundation of business and workforce survival; therefore, protecting them is essential for Continuity of Community and economic

recovery. Because the 'social fabric' may unravel in the event of a supply chain meltdown, companies should organize mitigation measures around supply chain failures and the reduced availability of critical workers. These Page measures are an essential underpinning for successful voluntary home isolation policies.

There are non-intrusive steps the private sector can take to prevent Internet overload and preserve capacity. These include voluntary conservation guidelines, in-house measures and protocols to limit consumption of bandwidth, and employee understanding and compliance.

Companies and government should prepare the general public for Internet disruptions. This preparation can include promoting civic responsibility to gain cooperation for Internet emergency measures, explaining Internet prioritization schemes, and trying to take the mystique out of information technology (i.e., persuade people that IT is a utility or resource, not much different from electricity or transportation).

Companies, government, and the general public should strive to understand a pandemic's physiological and technological challenges, and then adopt multi-faceted approaches to physical, cyber, and personnel protection.[24]

These recommendations frame the type of "preparedness" thinking that should go into the development of plans due to a pandemic declaration (we are now in WHO, phase 6). The appendix provides important and specific guidance to planners given the uncertainty of H1N1.

ENDNOTES - CHAPTER 3

1. SunGard, available from www.*sungard.com/*.

2. New Jersey Business Force, *www.njbusinessforce.org/*.

3. New Jersey Business Force/SunGard White Paper, "Will the Internet Be There When You Really Need It?" Pandemic Symposium sponsored by the New Jersey Business Force and SunGard, 2007.

4. World Health Organization, *www.who.int/en/*.

5. New Jersey Business Force/SunGard White Paper.

6. *Ibid.*

7. *Ibid*., p. 4.

8. *Ibid*.

9. *Ibid*., p. 4.

10. M. E. Porter, "How Competitive Forces Shape Strategy," *Harvard business Review*, March/ April 1979; M. E. Porter, *Competitive Strategy*, New York: Free Press, 1980; M. E. Porter, *Competitive Advantage*, New York: Free Press, 1985.

11. M. J. Chumer and M. Turoff, "Command and Control (C2): Adapting the Distributed Military Model for Emergency Response and Emergency Management," 11th ICCRTS, 2006, available from *www.dodccrp.org/events/11th_ICCRTS/html/papers/005.pdf*.

12. Porter, "How Competitive Forces Shape Strategy"; Porter, *Competitive Strategy*; Porter, *Competitive Advantage*.

13. New Jersey Business Force/SunGard White Paper, p. 5.

14. *Ibid*., p. 7.

15. *Ibid*., p. 7.

16. *Ibid*., p. 7.

17. Internet 2, available from *www.internet2.edu/*.

18. National Lambda Rail, available from *www.nlr.net/*.

19. New Jersey Business Force/SunGard White Paper, p. 8.

20. Facebook, available from *www.facebook.com/*.

21. Twitter, available from *twitter.com/*.

22. Robert Stephan, Statement for the Record, 2008, available from *homeland.house.gov/SiteDoments/20080514143442-12325*.doc.

23. New Jersey Business Force/SunGard White Paper, p. 10.

24. *Ibid*., pp. 11-12.

APPENDIX

The 10 items listed in this appendix are drawn directly from the white paper and are offered here as guidance for all organizations to follow in developing a resilient COOP that focuses upon Internet vulnerabilities.[1]

Planning Guidelines.

1. System and staff redundancy, enhancing redundancy by purchasing diverse equipment and systems.

2. Survivability based on the Continuity of Community concept.
   a. Plans, policies & procedures to ensure the resiliency of:
      i. Economy
      ii. Government
      iii. Society
      iv. Family
      v. Nuclear and Extended
      vi. The Individual
   b. Information technologies take on increasing importance when employing emergency measures to contain pandemic outbreaks,
   c. Quarantines,
   d. Social distancing.

3. Preparation combined with prevention,
   a. Ensuring multiple means of Internet access, and,
   b. Assessing existing bandwidth against potential surge requirements.

4. Identification of essential systems and people.

5. Education, training, exercising, and testing of IT systems in concert with continuity plans.
   a. Preparing employees to telecommute, including encouraging them to embrace mobile (i.e., handheld) and personal computing platforms,
   b. Educating, training, and testing employees on recovery responsibilities,
   c. Examining security issues.

6. Staffs that are important to the continuity effort, including Human Resources, Legal, and Information Technology.

7. Cascading impacts.
   a. Looking at service provider plans and the capacities and capabilities they possess,
   b. Determining whether first- and last-mile connections are potential points of failure.

8. Systems security in all facets of operations.
   a. Checking personnel, firewalls, passwords, etc.,
   b. Maintaining security's priority over urgency,
   c. Enforcing rules/procedures across all organizational levels,
   d. Remaining vigilant against cyber threats.

9. The balance between mitigation measures and demand for IT and Internet services.
   a. Reducing non-essential usage to prevent overloading,

b. Addressing problems at the source to lower unrealistic expectations,
c. Making concerted public relations and customer relations effort.

10. Realistic expectations.
    a. Planning and reinforcing what you can control,
    b. Accepting and trying to influence what you cannot,
    c. Proceeding without waiting for government or anyone else to tell you what to do.

ENDNOTES - APPENDIX

1. New Jersey Business Force/Surguard White Pages, pp. 9-10.

REFERENCES

Chumer, M. J., and M. Turoff, *Command and Control (C2): Adapting the Distributed Military Model for Emergency Response and Emergency Management, 11th ICCRTS,* 2006, available from *www.dodccrp.org/events/11th_ICCRTS/html/papers/005.pdf.*

Facebook, available from *www.facebook.com/.*

Internet 2, available from *www.internet2.edu/.*

National Lambda Rail, available from *www.nlr.net/.*

New Jersey Business Force, available from *www.njbusiness-force.org/.*

New Jersey Business Force/SunGard White Paper, "Will the Internet Be There When You Really Need It?" Pandemic Symposium Sponsored by the New Jersey Business Force and SunGard, 2007.

Porter, M. E., "How Competitive Forces Shape Strategy," *Harvard Business Review*, March/April, 1979.

_____, *Competitive Strategy*, New York: Free Press, 1980.

_____, *Competitive Advantage*, New York: Free Press, 1985.

Stephan, Robert, Statement for the Record, 2008, available from *homeland.house.gov/SiteDocuments/20080514143442-12325.doc.*

SunGard, available from *www.sungard.com/.*

Twitter, available from *twitter.com/.*

World Health Organization (WHO), available from *www.who.int/en/.*

CHAPTER 4

ARE LARGE-SCALE DATA BREACHES INEVITABLE?

Douglas E. Salane

INTRODUCTION

Despite heightened awareness, large-scale data breaches continue to occur and pose significant risks to both individuals and organizations. An examination of recent data breaches shows that fraudsters increasingly are targeting institutions that hold large collections of credit card and social security numbers. Particularly at risk are card payment processors and retailers who do not properly secure their systems. Frequently, breached data winds up in the hands of overseas organized crime rings that make financial data available to the underground Internet economy, which provides a ready market for the purchase and sale of large volumes of personal financial data. This chapter concludes that strong data breach notification legislation is essential for consumer protection, and that the direct and indirect costs of breach notification provide significant economic incentives to protect data. Also needed are standards for end-to-end encryption, enterprise level methods for quickly patching and updating information systems, and enhanced privacy standards to protect sensitive financial information.

A data breach occurs when an organization loses control over who has access to restricted information. The Privacy Rights Clearing House, a nonprofit privacy advocacy organization, maintains a partial list

of the breaches reported since 2005.[1] Losses of tens of thousands of records now occur almost on a weekly basis. Large-scale breaches at data aggregators, credit card payment processors, and national retail chains have compromised the sensitive personal and financial data of millions individuals. Currently, 44 states have data breach notification laws that require organizations to notify the individuals affected by a breach. For organizations holding data on individuals, breaches are no longer an internal matter and can be quite costly, both in terms of breach notification costs and the loss of confidence of customers and business partners.

Data breaches exposing information that can be used to commit fraud are of particular concern. Such breaches typically involve sensitive financial information such as credit card and bank account numbers. Often causing even greater harm, however, is the loss of personally identifiable information (PII) such as driver license or social security numbers. Unlike compromised credit card and account numbers, it is difficult to know how thieves will use a social security number or other PII to commit fraud. A growing demand for the stolen PII now provides a ready market for both types of information, and data thieves have ample incentive to steal both.

The scale and scope of data breaches during this decade has been alarming. From 2003 to 2005, each of the three leading data aggregation companies, Acxiom,[2] LexisNexis,[3] and ChoicePoint,[4] suffered serious data breaches by failing to control business partners who had access to their databases.[5] In 2005, ChoicePoint inadvertently released the financial records of 163,000 persons by making the data available to identity thieves who posed as legitimate clients. In 2003

and 2004, in two separate incidents, Acxiom subcontractors stole information in the company's databases. In one case, the subcontractor stole over one billion records. From 2003 to 2005, LexisNexis found that unauthorized persons used identification of legitimate users to obtain social security numbers, driver's license numbers, and the names and addresses of over 310,000 individuals in its databases. In a May 2009 announcement, the company notified over 40,000 individuals that credit card data that it held may have been compromised in 2007.

During the past 4 years, several major retailers and card payment processing companies have had extremely large data breaches. In June 2005, Master Card disclosed that a card processor, CardSystems Solutions, suffered a data breach that compromised the credit card information of over 40 million card holders.[6] In the widely publicized TJX Companies breach that occurred from 2005 to 2007, thieves stole over 45 million credit card numbers.[7] According to the Massachusetts Bankers Association, the breach affected the credit records of over 20 percent of New Englanders. In March 2008, Hannaford Brothers Co. disclosed that malicious software in its payment systems compromised at least 4.2 million credit and debit card accounts.[8] In December 2008, payment processor RBS Wordplay said a breach of its payment systems affected more than 1.5 million people.[9] Security and law enforcement experts are still trying to determine the extent of the Heartland Payment System Breach discovered in December 2008. Heartland processes over 100 million credit/debit transactions per month and is one of the top 10 payment processors. For over 18 months, malicious software on a Heartland server intercepted unencrypted Track 2 (information on the

magnetic strip of a credit or debit card). The company became aware of the breach when Visa reported excessive fraudulent activity in credit card transactions processed by Heartland.[10]

Although large-scale breaches attract the most attention, smaller targeted breaches can result in significant losses since they often provide thieves with the information needed to commit fraud. Recently thieves installed skimmers on automatic teller machines (ATMs) in New York City and positioned concealed cameras near the machines to record Personal Identification Numbers (PINs). After fabricating credit cards with the stolen information, the thieves were able to steal over $500,000 from about 200 victims.[11] Thieves then attempted to withdraw the maximum allowable amount from each account for as many days as possible. Skimmers for capturing the card's Track 2 data and devices for fabricating cards are available on the Internet. This type of crime no longer requires exceptional technical skills, and ATM frauds that use this equipment are becoming increasingly common.

Due to the potential impact of breaches on consumers, organizations, and commerce, data breach research is an active area. Two organizations that provide breach information are the Open Security Foundation, through its DataLossDB Project, and the previously mentioned Privacy Rights Clearing House.[12] The DataLossDB Project maintains a downloadable database of incidents and provides aggregate statistics on breaches since 2005. The primary sources of information on data breaches are breach notification letters sent to state attorneys general, which typically are required under state breach notification laws. Copies of breach notification letters are then sent to individuals whose information has been compromised. Press re-

ports, SEC filings, and company statements are other important sources. Despite California's landmark breach notification legislation in 2003 and the adoption of breach notification legislation in 44 states, detailed information on a data breach is seldom made public or shared with the larger security community at the time of a breach.

Data breaches, particularly large-scale breaches involving PII, raise many questions. Unfortunately, the secrecy that typically surrounds a data breach makes answers hard to find. Detailed information, which may be essential for threat detection throughout a particular industry, is seldom made available at the time a breach occurs. In fact, the details surrounding a breach may not be available for years since large-scale breaches usually result in various legal actions. The parties involved typically have no interest in releasing any more information than the law requires. Ironically, detailed breach information often becomes available in the course of a legal action when it becomes part of the public record. Thus the exact means by which a breach occurred often is not known until long afterward, if ever. Moreover, information about perpetrators and what exactly they do with the information is difficult to obtain. Such information may only come to light years later, if at all, in the course of criminal prosecutions. In addition, it is often not clear how to quantify the harm that may be caused by a breach—if 40 million records are compromised, how many of those records will likely to be used to commit fraud? What information should be made available to affected individuals, and how should they be instructed to protect themselves? Who bears the costs? In industries where multiple parties process data, who should be held responsible for a breach?

The remainder of this chapter examines notable large-scale breaches in the data aggregation, card payment processing, and retail industries. It explores remedies and practices that have been suggested to mitigate breaches, particularly in the card payment industry. The chapter also discusses the costs of notable large breaches, both to individuals and the companies involved. It describes the research and developments needed to improve data breach detection, deterrence, and response.

NOTABLE BREACHES: INSTITUTIONS, CAUSES, AND COSTS

By 2005, largely through acquisitions of smaller data management companies, Acxiom, ChoicePoint, and LexisNexis had grown to be the world's three largest aggregators and providers of individual, data, each with revenues of over $1 billion annually. These organizations leveraged their significant analysis and processing capabilities, gleaned over many years of managing data for large corporate clients, to provide detailed information on, and profiles of, individuals to insurers, collection agencies, direct marketers, employment screeners and government agencies, including state and local law enforcement agencies. The website of Accurint, the information subsidiary of LexisNexis, indicates the detailed information held and made available.[13] For example, one product provided by the company, "People at Work," holds information on 132 million individuals including addresses, phone numbers, and possible dates of employment. The site advertises the ability to find people, their relatives, associates, and assets. Large-scale breaches at each of these data aggregators earlier in this decade raised a

great deal of attention among privacy advocates and prompted calls for regulation of the activities of the data aggregation industry.[14]

During 2002 and 2003, Acxiom suffered two separate serious data breaches that involved Acxiom business partners who had legitimate password access to the company's databases.[15] The first involved the system administrator of a small company who provided services to Acxiom and who routinely downloaded files from an Acxiom FTP server. The administrator exceeded his authority on the server and was able to download and decrypt a file containing passwords. He obtained a master password that allowed him to then download files belonging to other companies. The administrator sealed his fate when he told a hacker friend in a chat room that he had been able to obtain access to a local telephone company database. A subsequent investigation of the hacker friend led to the administrator. As part of the same investigation, Acxiom technicians came upon a second more serious breach that involved theft by a subcontractor to an Acxiom contractor. From January 2001 to June 2003, the subcontractor, who owned a firm that provided e-mail advertising services, accessed over one billion records in Acxiom's databases by extending his authorized access. The individual was later arrested and convicted on various federal charges that included 120 counts of unauthorized access of a protected computer.[16] Prosecutors claim he used the data in his own e-mail advertising business and eventually planned to sell his company and its newly expanded database to a credit rating company.

The ChoicePoint breach occurred in the fall of 2004 and involved the theft of 145,000 consumer records—the number was later revised upward to 163,000 re-

cords.[17] Under California's breach notification law, ChoicePoint had to disclose the breach to California residents. Shortly afterward, attorneys general in 38 states demanded that ChoicePoint disclose the breach to victims in all states.[18] The breach led to numerous calls for an investigation of how information held by aggregators might be used to harm individuals.[19] The breach cost ChoicePoint $2 million just in notification fees and over $10 million in legal fees. In February 2005, the Company said about 750 individuals had been victims of identity theft. The company stated at the time that the breach did not involve a compromise of its networks or hacking, but was carried out by a few individuals who posed as legitimate business customers and were given access to the data, which included personal financial information. The company stated that financial fraud conducted by seemingly legitimate businesses is a pervasive problem. The Federal Trade Commission (FTC) later determined that ChoicePoint was in violation of the Fair Credit Reporting Act. The company settled with the FTC by paying $10 million in fines and $5 million for consumer redress. One of the perpetrators, a Nigerian national living in California, was later arrested and tried under California law on charges of identity theft and fraud. He was sentenced to 10 years in prison and ordered to make restitution of $6 million. The incident led to dramatic changes in the way ChoicePoint safeguards sensitive personal information and how it screens potential business customers.

In 2005, LexisNexis, another leading data aggregator, announced a major breach that exposed the personal information of 310,000 individuals.[20] LexisNexis found after analyzing data over a 2-year period that unauthorized people used identification and pass-

words of legitimate customers to obtain consumer social security numbers, driver's license numbers, names, and addresses. The company stated that the breach involved 59 incidents of improper access to data. The company added that various techniques were used to gain access to the data, including, collecting identification and passwords from machines infected with viruses, using computer programs to generate passwords and identification that matched those of legitimate customers, and unauthorized access by former employees of companies with legitimate access to LexisNexis data. The incident appeared to be not one breach, but a series of breaches that occurred over a multi-year period and involved several different groups.

In May 2009, LexisNexis disclosed a breach that exposed the personal information of 40,000 individuals and compromised names, birthdates, and social security numbers.[21] The breach appears to have taken place from June 2004 to October 2007. The company breach letter said the thieves, who were once legitimate LexisNexis customers, used mailboxes at commercial mail services and PII taken from LexisNexis to set up about 300 fraudulent credit cards. The breach letter indicated that LexisNexis learned of the breach from the U.S. Postal Inspection Service, which was investigating the fraudulent credit cards.[22]

In congressional testimony in 2005, Acxiom's chief privacy officer discussed the company's data breaches.[23] She claimed that most information obtained was of a nonsensitive nature, and none of it was used to commit identity fraud. She noted that the company would henceforth require stronger passwords and keep data on servers only for the period for which it is needed. She mentioned that Acxiom had decided to appoint a

chief information security officer, a position now common in most large organizations. From her testimony, it was obvious that this breach was an embarrassment for a company that obtains over 80 percent of its revenues from managing data for large corporations and large public agencies. She indicated that Acxiom was in the process of participating in dozens of audits by clients, whose trust in the company had certainly been diminished. The privacy officer reflecting the words of the then FTC commissioner said there is no such thing as perfect security and that breaches will happen even when all precautions are taken. The privacy officer's testimony underscored the importance of removing data when it was no longer needed and effectively monitoring contractors and vendors with access to company data. At a recent presentation at John Jay College, the chief security officer of Time Inc. indicated that vendor management now was one of his major responsibilities.[24]

The retail and card payment processing industries have suffered a number of large-scale breaches during the past 5 years. Unlike the data aggregation industry, breaches in these industries appear to have involved malware on servers that collected data and transmitted it outside the company. These breaches, however, also involved individuals with detailed insider knowledge of the systems that were compromised. Although the credit card industry and retail industries have not reported significant rises in the rates of credit card fraud, the scope of recent payment card breaches, the rapidity with which stolen credit information was used, and the geographical scope of the fraud, raise concerns that data thieves are now taking advantage of the capabilities afforded by worldwide crime organizations to monetize vast collections of breached financial information.[25]

One of largest breaches of a payment processor occurred at CardSystems Solutions, a company that processed both credit and debit credit card transactions. According to the FTC,[26] in 2005 the company handled over 210 million card purchases worth $15 billion for more than 119,000 small and mid-size merchants. The company's CEO admitted in congressional testimony that the data thieves captured Track 2 information belonging to 263,000 individuals.[27] Security experts later determined that credit and debit information of over 40 million customers may have been compromised. Despite the incredible volume of transactions processed by the company, at the time, the company had only 115 employees. The breach was not discovered by CardSystems, but by MasterCard security while tracking fraudulent card activity.[28]

The FTC charged CardSystems Solution with violation of Section 5 of the FTC Act, which prohibits unfair or deceptive business practices.[29] The FTC claimed that the company violated the Act by failing to adopt widely accepted, easily deployed security standards that would have prevented the exposure of the sensitive financial data of tens of millions of individuals. The FTC further charged that the company neglected industry security polices with respect to the type of data it collected and the amount of time it held the data.

A forensic investigation of the breach found numerous security lapses both in the company's systems and procedures. The company violated it own industry security polices by storing data in unencrypted format on a server accessible from a public network. Data thieves were able to execute a Structured Query Language (SQL) injection attack that allowed an unauthorized script to be placed on a WebFacing server.

The script exported data to an external FTP site every 4 days. In addition, data was retained for purposes other than payment processing, another violation of industry policy. Furthermore, the company did not adequately assess its system vulnerabilities to commonly known attacks, did not use strong passwords, and did not implement simple, widely used defenses to thwart SQL attacks. The CEO also added in congressional testimony that the company stored Track 2 data for later analysis, another violation of industry security standards.[30]

The breach raised new levels of security awareness within the card payment processing industry and provided significant impetus for compliance with the industry's newly developed Payment Card Industry Data Security Standard (PCI DSS or simply PCI).[31] Today, loss of PCI certification can put a payment processor out of business, because it means that the company failed to comply with information security standards, which undermines the confidence of customers and partners. Shortly after the CardSystems breach, Visa and American Express stopped processing with the company. After revising security policies, upgrading systems, and implementing end-to-end encryption on its backend systems and networks, the company eventually gained PCI certification. PayByTouch, another payment processor, then purchased the company at a steep discount.[32] The largest breach of a retailer's payment processing systems occurred at TJX Companies from 2005 to 2007.[33] Intruders had access to the systems for over 18 months. In filings with the SEC, the company said 45.6 million card numbers may have been taken. Card issuing banks later raised the total to 94 million. In addition, thieves captured personal information such as driver's license numbers, which

was used to track merchandise returns.[34] According to industry estimates, a card replacement can cost between $5 and $15 dollars, and a breach notification may cost up to $35 per notification. Shortly after the compromise, thieves used the card numbers to make purchases in Georgia, Florida, and Louisiana in the United States, as well as in Hong Kong and Sweden. By September 2007, the breach had cost the company over $150 million, and the company still faced numerous class action law suits.

TJX believes a flaw in its wireless networks may have allowed malware to be placed on one of its Retail Transaction Switch Servers (RTS) that processes and stores information on customer purchases and charge backs for its stores throughout North America. At the time TJX was in the process of upgrading its wireless security from the weaker Wired Equivalent Privacy (WEP) standard to the stronger WiFi Protected Access (WPA) standard.[35] TJX admits that intruders had accessed the system at times from July 2005 to January 2007.

A report by the Office of the Privacy Commissioner of Canada[36] provides a summary of the security lapses of TJX Companies that led to the breach. The privacy commission found that the TJX intruders gained access to the names, addresses, driver's license numbers, and provincial identification numbers of over 330 persons with addresses in Canada. According to Canadian privacy law, TJX should not have collected this information in card transactions. Citing analyses of the incident, the commission found that the company did not have in place adequate logging procedures to do a proper forensic analysis of the incident. The data thieves actually deleted information so it was difficult to tell what information was compromised.

The commission also faulted the company for not being fully compliant with industry standards and practices such as PCI. The commission noted that as far back as 2003, the Institute of Electrical and Electronics Engineers (IEEE) standards committees had recommended migration from the WEP security standard to the stronger WPA standard, yet the company had at the time of the breach failed to complete the migration. Even though the commission found that TJX had an adequate organizational security structure in place, it faulted the company for collecting too much data, holding it too long, using a weak security protocol, and not having adequate monitoring in place to detect a breach in progress or to determine the extent of the breach after the fact.

Another payment processor, RBS World Pay of Scotland, suffered a serious breach in December 2008 that involved over 1.5 million financial records.[37] According to the Federal Bureau of Investigation (FBI), thieves stole Track 2 data from debit cards that were used to pay employees. They also may have accessed the social security numbers of one million customers. The FBI said the thieves worked with cashiers in 49 cities, including Atlanta, Chicago, New York, Montreal, Moscow, and Hong Kong, to withdraw over $9 million from accounts. The cashiers locally fabricated cards and made withdrawals from local ATMs. Timing is critical in these frauds. If good fraud monitoring is deployed, the information has to be monetized quickly before cards are cancelled.

In January 2009, Heartland Payment Systems Inc. announced the largest data breach to date of a payment processor, over 100 million cards compromised. Heartland is among the top 10 card payment processors and handles over 100 million credit and debit

card transactions per month. The breach was detected not by Heartland, but by VISA's security organization, which noticed an increase in fraudulent activity on cards processed by Heartland. The source of the breach was malware on a Heartland system, which intercepted payment information sent to Heartland from thousands of retail merchants. At the time of the breach announcement, Heartland claimed no social security numbers, unencrypted PIN numbers, addresses, or telephone numbers were revealed.[38] Thieves, however, were able to intercept the Track 2 information, which is sufficient to fabricate a duplicate credit card. At the time, the company said it did not know how long the malware was in place, how it got there, or how many accounts were compromised. A security analyst at Gartner Inc. noted that the company was probably not doing file integrity monitoring to detect unauthorized changes in files and directories.[39]

The losses in this breach are significant. Thus far, the breach has cost the company $12 million, including a $7 million fine imposed by MasterCard. Given the number of compromised cards, banks would be unlikely to cancel and reissue all of them since the costs could be between $600 million to $1 billion, which is bigger than any anticipated fraud. Heartland, however, faces a class action lawsuit filed on behalf of financial institutions that have reissued credit and debit cards and now are attempting to recover these and other expenses associated with the breach. The loss of confidence on the part of customers and partners is also a major issue the company is attempting to address.[40]

Thus far, this report has focused on breaches by companies in the data aggregation and payment processing industries. Large-scale breaches, of course,

can occur in any organization that maintains large data repositories or does high volume transaction processing. The Open Security Foundation DataLossDB website shows a dramatic increase in the number of breach incidents since 2000, which is most likely due to the widespread adoption by states of breach notification laws beginning in 2005.[41] Statistics available on that the DataLossDB site show that educational institutions and government agencies account for 42 percent of reported incidents, while nonmedical businesses account for about 46 percent. Rather than malicious attempts to steal data, many breaches, about 29 percent of those reported, are simply the result of lost or stolen storage media (tapes, jump drives, and laptops). The site also shows that breaches involving third parties, common in the payment processing industry, often result in a greater numbers of records lost than those that do not involve third parties.

MONETIZING THE CRIME

What makes large-scale data breaches so dangerous is that modern organized crime has developed efficient mechanisms for the sale and widespread distribution of large collections of identities and personal financial information.[42] So-called carding forum websites provide repositories for credit information for cyber thieves around the world. These sites often make available both Track 1 and 2 data from a card. In addition, there are sites that include full information about a victim, so-called "fulls," which include name; address; telephone, social security, credit, or debit card numbers; PINs; and a possible a credit history report. This information is, of course, more costly

than just credit card or account numbers. Thieves know that there is a ready market for the proceeds of a large-scale breach of financial information or PII that can be used to commit fraud.

Carders (those who run carding sites) typically buy information from hackers who are responsible for the breach. Carders can break the data into smaller packages and distribute it to lower level carders who may assume the more risky task of making the card's information available to end users. End users, sometimes known as cashers, ultimately monetize the stolen information, which involves the most risk and difficulty (fabricating a card, changing an address, etc.). In some card account heists, a worldwide network of cashers fabricates cards and makes withdrawals at ATMs around the world shortly after the breach. The Shadow Crew site, for example, which was dismantled by the U.S. Secret Service in 2004, had over 4,000 members throughout the world, trafficked in at least 1.7 million credit cards, and caused losses estimated at $4.3 million.[43] Many considered the Shadow Crew to be a loose configuration of cyber criminals, not a highly organized crime group.

A ready market for a large collection of account information creates serious response issues for financial institutions. In a small-scale breach that involves 200 accounts, banks can simply reissue cards with new account numbers. The cost to reissue 45 million compromised cards, however, is probably going to be more than any credit fraud so banks will not reissue cards in such a large breach. Thus compromised cards may stay active and available at carding sites long after the breach. Losses to individuals, merchants, and banks may continue for some time. ID Analytics, a firm that investigates credit fraud, found in one breach they studied that breached information was used sparingly

at first, probably to avoid fraud detection.[44] Soon after the breach was discovered, however, there was an immediate increase in activity in the use of breached identities, followed by a sharp drop off in use after the breach was publicly announced.

Recently, a site known as Dark Market was closed down by its alleged operator. Besides credit card information, the site offered ATM skimmers and other hardware needed for fraud operations. The site's operator said he was closing it because too many law enforcement agents and reporters had gained access to the site, and it was proving difficult to be sure that their accounts had been eliminated. Dark Market even provided review mechanisms that allowed users to evaluate merchandise and weed out so-called "rippers," or those who rip off other fraudsters. In recent congressional testimony, Rita Glavin, Acting Assistant Attorney General, expressed concern that international carding forums provided a ready market for large-scale data breach contraband.[45] She noted that at its height, Dark Market had 2,500 members worldwide. Late in 2008, in connection with the Dark Market site, the FBI announced the arrests of 60 people from six different countries including the United States, Estonia, and the People's Republic of China. Investigators found more than 40 million credit cards, including some from the TJX breach. An FBI undercover agent who penetrated the site provided further details of the Dark Market operation at the April RSA security conference.[46]

CHALLENGES AND REMEDIES

Each industry presents its own data security challenges. Notable large-scale breaches in the data aggre-

gation industry indicate the need to prevent insiders from exceeding authorized access, this is a challenge in an industry where revenue comes from making data available to partners and clients. In the card payment processing industry, the complexity of the data flow and systems in use make securing data a vexing task. In this section, we focus primarily on remedies proposed and existing challenges in the payment processing industry, which has experienced the largest breaches of sensitive financial information.

In 2006, the payment processing industry adopted the Payment Card Industry Data Security Standard.[47] The standard addresses the following areas: network security, protection of card holder data, management of vulnerabilities in system and application software, access control measures, monitoring and testing of network resources, and organizational information security policies. The goal is that all organizations involved in the processing of payment transactions, i.e., card issuing banks, merchants, acquiring banks, and card brand associations, will eventually comply with the PCI standard. An industry supported council oversees continued development of the standard, certifies organizations as compliant, and certifies PCI auditors who monitor compliance.

Recent congressional testimony on PCI standards by representatives of the card associations, a major retailer, and the National Retailers Association indicate the difficulty of establishing, implementing, and monitoring compliance of security standards in an industry as complex as the payment processing industry.[48] For example, the head of fraud control at Visa pointed out that the company serves as the connection point between 1.6 billion payment cards, 16,600 financial institutions, and 29 million merchants in 170 countries.

He could have also added that this system includes hundreds of payment processors such as Heartland and RBS who provide the electronic delivery path that connects merchants, card organizations like Visa and MasterCard, and the financial institutions who provide the funds. In addition, these payment processors also handle ATM card and debit transactions for financial institutions. In these transactions, they hand data over to organizations such as NYCE, which acts as a clearing house for ATM transactions.[49] The card payment system includes larger retailers such as Wal-Mart, with adequate budgets for data security, as well as small corner stores that have very limited resources. It is not surprising that rates of PCI compliance vary considerably throughout the industry.[50]

One frequent criticism of the PCI standard is the requirement for data to be encrypted only on public networks, or if stored on devices accessible from public networks. Data on private networks does not need to be encrypted. In fact, typically Track 2 data delivered by retailers to payment processors is not encrypted. In recent congressional testimony, the head of the National Retailers Association and the CEO of a major retail chain both stated that their organizations would prefer to deliver data in encrypted format. Currently, this is not feasible since there is no industry-wide encryption standard. After the CardSystems breach and the more recent Heartland breach, both organizations proposed either encryption in back end systems or end-to-end encryption as solutions. The Accredited Standards Committee X9 (ASC X9) of the American National Standards Institute (ANSI) is currently working with payment processing industry to develop the end-to-end standard.[51] The cost would be considerable since merchants would have to upgrade

all point of sale equipment to comply with the standard. Some large retailers, however, believe that the cost of large-scale breaches makes the case that there is a potentially significant return on investment as a result of acquiring the required equipment upgrades.[52]

Retailers criticize the card payment system because it requires them to retain too much data on their systems. Charge-backs present a difficult challenge for the industry since retailers must retain PII in addition to credit card data to uniquely identify transactions and prevent charge-back fraud. Frequently, retailers retain a card number and an address, which might provide credentials for a purchase. Rather than maintain data to track the transaction, retailers would like the payment processor and the card association to have systems that can provide them with records of the transaction so they only have to store a signature and a number that identifies the transaction. The Canadian Privacy Commission examination of the TJX Companies breach faulted the company for storing driver's license numbers and provincial identification numbers, which were taken from about 300 people in Alberta, Canada, during the breach and used to commit fraud.[53]

To prevent and respond to data breaches on an industry-wide level, the security community in an industry must have detailed knowledge of incidents and vulnerabilities as soon as possible. For most commercial and open source software, information sharing and collaboration regarding software vulnerabilities and available patches have been the norm for some time.[54] In the payment processing industry, where a vulnerable software component could be in use throughout the industry, such information sharing and response capabilities are only beginning to

be considered. In March 2009, The Financial Services Information Sharing and Analysis Center (FS-ISAC) formed the Payments Processing Information Sharing Council (PPISC), a forum for sharing information about fraud, threats, vulnerabilities, and risk mitigation practices.[55] At the council's first meeting in May 2009, the CEO of Heartland handed out USBs with the malware found on Heartland's systems so other payment processors could try to determine if it was on their systems.[56] Effective deterrence and response require that knowledge of software vulnerabilities and malware be made available, at least to the security community, as soon as it is available.

Card companies increasingly are promoting optional passwords to use with cards.[57] Only a few participating merchants now accept password protected cards, but the number of merchants is increasing. Password protected cards may be particularly attractive to merchants who accept online purchases and international transactions. Unlike card present transactions where fraud rates have dropped during the past 10 years, credit card fraud associated with online and international purchases is a continuing problem for the industry.

The card associations MasterCard and Visa have long used fraud detection systems based on usage patterns to detect anomalous transactions. Their systems store examples of valid transactions and constantly update cardholder data to create a current usage profile. Each new transaction is evaluated against the individual's transaction history. For example, card present purchases of certain types of items outside of an individual's geographic region trigger an alert. These anomalous detection systems have to be consistently updated as thieves consistently find ways to circum-

vent them. A recent trend is the use of a botnet computer to make an online purchase from an IP address that is within the card holder's geographical region.[58]

Breach prevention, detection, and response present challenges to law enforcement agencies, the IT industry, and those charged with formulating information security policy. Based on the breaches examined here, the following is a brief summary of the challenges:

Law Enforcement: (1) Immediate notification in the event of a breach. (2) Enhanced knowledge of carding sites and the role that organized criminal activity plays in monetizing large-scale breaches. (3) Cooperation among law enforcement agencies and governments throughout the world to facilitate breach investigations.

IT Industry: (1) Tracking data in large complex systems. (2) Capabilities for rapid system wide updating and patching. (3) Automated fraud detection tools. (4) Maintaining the integrity of software and systems. (5) Standards for end-to-end encryption in complex distributed systems. (6) Industry-wide clearing houses to share breach information and coordinate an industry wide response to a breach.

Information Security Polices: (1) Limiting data collection and retention versus maintaining data for marketing and other activities. (2) Protecting data when there is commingling of proprietary systems and networks with those attached to the Internet. (3) Authorization and auditing polices that address the ease with which large data repositories can be copied.

National breach notification legislation is now before Congress.[59] In addition to notification, the bill would force companies holding PII to follow data privacy policies established by the Federal Trade Commission. Proponents claim several advantages of the

proposed law: (1) It simplifies breach notification requirements for organizations; (2) It establishes standards for protecting data; and (3) It provides uniform standards by which individuals could check data held for accuracy. Previous attempts at national breach notification legislation raised concerns among privacy advocates because the proposed federal legislation had a lower threshold for breach notification than most state laws, which the bill would have preempted.

The Federal Stimulus bill passed in February 2009[60] requires notification of health care data breaches. The bill requires all medical providers, health plan administrators, and medical clearing houses covered by HIPPA, and even organizations not covered by HIPPA, e.g., the online health record services proposed both by Google and Microsoft, to provide information on breached medical data. Moreover, the law requires the Department of Health and Human Services to issue guidelines for protection of sensitive medical data. Given the rash of large-scale data breaches during the past decade, it is not surprising that recent national breach notification legislation includes provisions for increased government oversight of the use of PII.

CONCLUDING REMARKS

Data breaches must be understood within the industries and organizations within which they occur. Notable breaches in the data aggregation industry involved insiders such as contractors who extended their authorized access. Breaches in the payment processing industry made use of malware that relayed sensitive personal financial information to data thieves. Regardless of the industry, however, basic privacy policies that; (1) limit the amount of data col-

lected, (2) limit where data is stored and the time for which it is stored, and (3) restrict the use of data to the task for which it was collected, play a critical role in preventing breaches. Large-scale breaches are expensive, especially if the lost information involves sensitive personal financial data. Breaches in the payment industry can exact extremely high costs, particularly to organizations such as card processors whose businesses depend on the trust of partners and customers. Breach notification laws, which keep both consumers and business partners aware of what is happening with their data, are changing the way all industries and organizations view information security.

ENDNOTES - CHAPTER 4

1. Privacy Rights Clearing House, available from *www.privacyrights.org/*.

2. About Acxiom, available from *www.acxiom.com/about_us/Pages/AboutAcxiom.aspx*.

3. LexisNexis – About Us, available from *www.lexisnexis.com/about-us/*.

4. ChoicePoint, available from *www.choicepoint.com/*.

5. Reed Elsevier, the parent company of LexisNexis, purchased ChoicePoint in 2008.

6. T. Zeller, "MasterCard Says Security Breach Affects Over 40 Million Cards," *The New York Times*, June 5, 2005.

7. J. Vijayan, "TJX data breach: At 45.6 million card numbers, it's the biggest ever," *Computerworld*, March 29, 2007.

8. J. Vijayan, "Hannaford says malware planted on its store servers stole card data," *Computerworld*, March 28, 2008.

9. B. Krebs, "Data Breach Led to Multimillion Dollar ATM Heists," Security Fix, *The Washington Post*, February 5, 2009.

10. B. Krebs, "Payment Processor Breach May be Largest Ever," Security Fix, *The Washington Post*, January 20, 2009.

11. A. Gendar, "ATMs on Staten Island rigged for identity theft; bandits steal $500G," *The Daily News*, May 11, 2009.

12. Open Security Foundation, DataLossDB Project, available from *datalossdb.org/*.

13. Accurint, available from *www.accurint.com/*.

14. D. Solove and C. J. Hoofnagle, "A Model Regime of Privacy Protection," *University of Illinois Law Review*, February 2006, pp. 375-404.

15. K. Poulsen, "Chats led to Acxiom hacker bust," *SecurityFocus*, December 19, 2003, available from *www.securityfocus.com/news/7697*; B. J. Gillette, "Data thief exposes flimsy security, nets 8 years," *Email Battles*, February 24, 2006, available from *www.emailbattles.com/*.

16. United States Code, Section 1030 (a) (2) (c), available from *www.law.cornell.edu/uscode/18/1030.html*.

17. L. Rosencarnce, "ChoicePoint says data theft cost is $6 Million," *Computerworld*, July 21, 2005.

18. T. R. Weiss, "State officials push choice point on ID theft notifications," *Computerworld*, February 18, 2005.

19. G. Gross, "Lawmakers call for ChoicePoint investigation," *Computerworld*, March 3, 2005.

20. J. Krim, "LexisNexis data breach bigger than estimated," *The Washington Post*, April 13, 2005.

21. A. Westfeldt, "LexisNexis warns 32,000 people about data breach," *SanFrancisco Chronicle*, May 1, 2009.

22. LexisNexis Breach Notification Letter, available from *privacy.wi.gov/databreaches/pdf/LexisNexisLetter050509.pdf*.

23. J. Barret, Acxiom Corporation, Testimony before House Committee on Energy and Commerce, Subcommittee on Commerce, Trade and Consumer Protection, May 11, 2005, available from *archives.energycommerce.house.gov*.

24. R. Duran and F. Garcia, "Information Security and Privacy: Challenges in a Bad Economy and Difficult Legislative Environment," presentation at the Center for Cybercrime Studies, John Jay College of Criminal Justice, March 10, 2009.

25. CyberSource Corporation, "Online Fraud Report: Online Payment Fraud Trends, Merchant Practices and Benchmarks," available from *www.cybersource.com*.

26. Federal Trade Commision, "CardSystems Solutions Settles FTC Charges," February 23, 2006, available from *www.ftc.gov/opa/2006/02/cardsystems_r.shtm*.

27. J. Perry, CardSystems Solutions, Testimony before House Subcommittee on Oversight and Investigations of the Committee on Financial Services, July 21, 2005, available from *www.house.gov*.

28.T. Krazit, "MasterCard Blamed a Third Party Processing Firm," *Computerworld*, June 17, 2005.

29. Federal Trade Commission, "Enforcing Privacy Promises: Section 5 of the FTC Act," available from *www.ftc.gov/privacy/privacyinitiatives/promises.html*.

30. Perry.

31. PCI Security Standards Council, "About the PCI Data Security Standard (PCI DSS)," available from *https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml*.

32. M. Mimoso, "Cleaning up after a data attack," *Information Security*, April 14, 2006.

33. Vijayan, "TJX Data Breach at 45.6M card numbers."

34. J. Vijayan, "Breach at TJX puts card info at risk," *Computerworld*, January 22, 2007.

35. Sans Institute, "The Evolution of Wireless Security Standard in 802.11 Networks: WEP, WPA, and 802.11 Standards," 2003, available from *www.sans.org*.

36. Office of the Privacy Commissioner of Canada, "Report of an Investigation into the Security, Collection, and Retention of Personal Information: TJX Companies," September 25, 2007, available from *www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm*.

37. Vijayan, "Hannaford Says Malware..."

38. E. Mills, "Payment Processor Heartland Reports Breach," CNET News, January 20, 2009, available from *news.cnet.com/8301-1009_3-10146275-83.html*.

39. J. Vijayan, "Heartland Data Breach Sparks Security Concerns in Payment Industry," *Computerworld*, January 22, 2009.

40. Heartland Payment Systems, "Heartland Payment Systems Returns to Visa's list of PCI-DSS Validated Service Providers," May 1, 2009, available from *www.iteotlandpaymentsystems.com*.

41. Open Security Foundation DataLossDB Project, Data Loss Statistics, available from *datalossdb.org/statistics*.

42. K. Perreti, "Data Breaches: What the Underground World of Carding Reveals," *Santa Clara Computer and High Tech Law Journal*, Vol. 25, No. 2, 2009, pp. 375-413.

43. D. Gage, "Head of Shadowcrew Identity Theft Ring Gets Prison Time," *Security Baseline*, June 30, 2006, available from *www.baselinemag.com*.

44. ID Analytics, Inc., available from *www.idanalytics.com/*.

45. U.S. House of Representatives, "Do Payment Card Industry Data Standards Reduce Cybercrime?" Hearing of the Committee on Homeland Security, Subcommittee on Emerging Threats, Cybersecurity, Science and Technology, March 31, 2009, available from *www.usdoj.gov*.

46. S. Nicholas, "FBI Agent discusses big cybercrime bust," *iTnews*, April 23, 2009, available from *www.itnews.com.au*.

47. PCI Security Standards Council.

48. Nicholas.

49. NYCE Payments Network, LLC, available from *www.nyce.net/about.jsp*.

50. A.Conry-Murray, "PCI and The Circle of Blame," *Information Week*, February 25, 2008, pp. 31-36.

51. Heartland Payment Systems, "Accredited Standards Committee X9 Developing New Merchant Data Security Technology Standards," April 29, 2009, available from *www.heartlandpaymentsystems.com*.

52. L. McGlasson, "Heartland Databreack: Is End-to-End Encryption the Answer?," *BankInfo Security*, May 11, 2009, available from *www.bankinfosecurity.com/articles.php?art_id=1455&pg=1*.

53. Office of the Privacy Commissioner of Canada, "Report of an Investigation into the Security, Collection and Retention of Personal Information: TJX Companies, Inc.," September 25, 2007, available from *www.priv.gc.ca/cf-dc/2007/TJX_rep_070925_e.cfm*.

54. Financial Services Information Sharing and Analysis Center, "Payments Processing Information Sharing Council Forms to Foster Information Sharing among Payment Processors," available from *www.ppisc.com/InTheNews.asp*.

55. U.S. CERT, "Technical Cybersecurity Alerts," available from *www.us-cert.gov/cas/techalerts/index.html*.

56. R. Vamosi, "Heartland Comes out swinging after databreach," *Computerworld*, May 12, 2009.

57. A. Mahtab and M. Bokhari, "Information Security Policy Architecture," International Conference on Computational Intelligence and Multimedia Applications, Vol. 4, December 13-15, 2007, pp. 120-122.

58. Brett Stone-Gross *et al*., "Your Botnet is My Botnet: Analysis of a Botnet Takeover," Technical Report, Santa Barbara, University of California, Department of Computer Science, available from *www.cs.ucsb.edu/~seclab/projects/torpig/torpig.pdf*.

59. Data Accountability and Trust Act, H.R.2221, 111th Congress, 2009.

60. B. Bain, "Law Requires Health Data Breach Notifications," Federal Computer Week, February 27, 2009, available from *www.fcw.com/Articles/2009/02/27/Health-Data-Breach-Notification.aspx*.

CHAPTER 5

THE ROLE OF CYBERPOWER IN HUMANITARIAN ASSISTANCE/DISASTER RELIEF (HA/DR) AND STABILITY AND RECONSTRUCTION OPERATIONS*

Larry Wentz

INTRODUCTION

Cyber in the context of this chapter is used in its broadest definition. It includes aspects of both information and information communications technology where information and communications technology (ICT) is defined as the convergence of telecommunications and information technology. Aspects of the ICT encompass the range of technologies for gathering, storing, retrieving, processing, analyzing, and transmitting information that are essential to prospering in a globalized economy and establishing a knowledge culture. Additionally, ICT includes policies, processes, infrastructure, systems, services, education, and people and, most importantly, discussions of ICT need to consider the associated information and messaging activities and their impact on the society and its functions.

This chapter explores the role and challenges of cyberpower (information and ICT) in humanitarian

*The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the Department of Defense or the U.S. Government. All information and sources for this chapter were drawn from unclassified materials.

assistance/disaster relief (HA/DR) and stability and reconstruction operations. It examines whether a strategic use of cyber in U.S. Government (USG) engagement and intervention activities such as HA/DR and stability and reconstruction operations could lead to more successful results. Certainly, the information revolution has been a dynamic and positive factor in business, government, and social arenas in the Western world. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities of all types.

Complicating the challenges of HA/DR and stability and reconstruction operations related to failed-state interventions is the local situation that typically consists of: spoilers interfering with the intervening forces; refugees and internally displaced persons requiring humanitarian assistance; buildings requiring reconstruction; roads, power, water, telecommunications, healthcare, and education systems disrupted or dysfunctional; absence of a functioning government and laws, lack of regulations and enforcement mechanisms; widespread unemployment and poverty; and a shortage of leaders, managers, administrators, and technical personnel with 21st century technical and management skills. Additionally, there is a lack of a USG whole of government approach, a lack of trust among stakeholders, and policy, procedures, business practices, and people and organization culture differences. It is not a technology challenge per se. Generally, technology is an enabler if used properly.

This chapter concludes that civil-military collaboration and information sharing activities and smart use of information and ICT can have decisive impacts if they are treated as a core part of the nation's overall strategy and not just as "nice to have" adjuncts to re-

sponses to HA/DR or to the kinetic phases of warfare and stability and reconstruction operations. It is further suggested that utilizing the elements of the information revolution and the whole of government in a strategic approach to HA/DR and stability and reconstruction operations can have positive results and sets forth the strategic and operational parameters of such an effort. Finally, enhancing the influence of USG responses to HA/DR and interventions in stability and reconstruction operations will require a multifaceted strategy that differentiates the circumstances of the messages, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers.[1]

ROLE OF CYBER AND CHALLENGES

Lack of effective communication, coordination, collaboration, and information sharing among military, civilian government elements, international organizations (IO), intergovernmental organizations (IGO), nongovernmental organizations (NGO), private sector, and affected/host nation elements that form the network of partners and stakeholders involved in complex operations such as humanitarian assistance, disaster relief, security, stability, and reconstruction are consistent factors impacting the ability to conduct more successful operations. There are a number of reasons for this, the most common ones being the lack of a whole of government approach, a lack of trust among stakeholders, differences in policies, procedures, and business practices, and people and organization culture differences. It is not a technology challenge per se. Generally, technology is an enabler if used properly.[2]

A recent workshop co-hosted by the Asia Pacific Center for Security Studies, the Center of Excellence in Disaster Management and Humanitarian Assistance, and the Pacific Disaster Center focused on information sharing for crisis resilience—beyond response and recovery. The workshop out brief identified the following information sharing gaps:

- Lack of a tradition of sharing info within organizations/nation/internationally
- No incentive for organizations/nations to share information/cooperate
- Knowledge: governments do not know where to get info/funding, baseline information/education/training
- Lack of overarching coordinating body
- National realization that info sharing is a priority and commitment to follow-up
- Resiliency/redundancy of systems
- Political will and leadership
- No agreed upon standard set of collaboration tools
- Lack of confidence building measures
- Lack of forums for face to face networking/dialogue
- Lack of understanding between sectors
- Insufficient human resource capacity
- Lack of taking into account local conditions/cultures
- Lack of liaisons
- Information overload (condense and concise): double edged sword
- Lack of standard lexicon/terminology
- Understanding different cultures (military, government, civilian)
- Technology gaps: sending alert but a delay in response from supporting agencies

- Insufficient funds for risk reduction and resiliency
- Assessment of current condition (need to agree on where we are and where we want to be)
- Ability of government to disseminate information internally and to receive from outside
- Lack of standards and data compatibility (not geospatial referenced)
  - No central repository
  - Need better knowledge management
  - Example of a solution: Aid Management Platform and AiDA (accessible database of activities and programs)
  - Development Gateway
  - Reliability and validity
- Too much data (yellow pages on data about data) and information saturation of users
- Gaps in ability for decision makers to focus on the appropriate information
- Ability to identify and communicate with highly vulnerable groups
- Models are insufficient for leaders to make decisions before, during and after a disaster
- Language gaps
- Understanding culture and policy effects on disaster preparedness
- Ownership of information
- Building relationships between private and public sectors
- Gaps in how society responds to the information given
  - Trust in government/sector
  - Education
  - Cultural reasons

The gaps noted above should not come as a surprise and illustrate that much work still needs to be done to create and deploy collaborative information environments to achieve "unity of effort" across the civil-military boundaries. The underlying issues are intellectual, cultural, and social, not technical. Information-rich, easily accessed networks have become a critical commodity—essential service. Today the responder community increasingly demands that all stakeholders in complex operations be able to share situational awareness, reach back in time and distance for unforeseen data requirements, create and exchange data, and collaborate virtually across domains and boundaries.

Prior to a crisis, ICT and related networks need to be self-organizing, flat, robust, and open in order to maintain awareness, develop proactive responses, provide ground truth, and amplify social networks. During a crisis, these same networks need to be deployable in an ad hoc fashion, hastily pushed out or set up in areas that may have been ravaged by war or natural disaster. Networks with nontraditional partners need to be set up and function in the most adverse conditions, using come with what you have ICT or assets indigenous to the crisis area. The information content will no longer be determined by a small handful of experts but by the users themselves. The complexity will drive the practitioners to settle for networks that will simply help them make sense of the situation—sense making—rather than seeking to gain information dominance and clarity. The new information age means ICT is no longer just good to have but essential. The emerging architecture is one of participation, strong social and knowledge networking, and agility to use all available means to communicate—

connectivity increases effectiveness, free revealing makes sense, the community generates content, and the lead user drives the market.

Experience from recent real world operations suggests there is an urgent need to review and revise existing policies, doctrine, procedures, and business practices, and to explore more effective use of information and ICT as an enabler. ICT can be used to overcome current short falls in order to improve the ability of stakeholders to more efficiently and effectively respond, to build trust among diverse groups, to promote unity of effort across civil-military boundaries, and to develop and leverage ICT tools and systems. ICT as an enabler can facilitate seamless information flow to support shared situational awareness, collaboration, coordination, and information sharing as needed.

There are a number of Department of Defense (DoD), Department of State (DoS), U.S. Agency for International Development (USAID), and policy, doctrine, and guidance documents from other organizations that need to be considered in the process of institutionalizing change in how the U.S. military and civilian elements view and integrate ICT into warfighting operations and support of HA/DR and stability and reconstruction operations. Figure 5.1 is an attempt to identify and map the relationship of the existing policy, doctrine, and guidance documents that form the basis for guiding the planning for, and execution of, HA/DR and stability and reconstruction operations. It should be noted, the documents identified do not specifically refer to ICT as an "essential service," although some, such as DoD Directive (DoDD) 3000.05, "Military Support of Stability Operations"; DoD Instruction (DoDI) 8220.02, "ICT Support

to Stability Operations"; and *Field Manual (FM) 3-07, Stability Operations*, certainly imply its importance. None address ICT as a "smart power" tool and as an enabler for HA/DR and stability and reconstruction operations. The National Security Strategy Directive (NSPD)-44, "Management of Interagency Stability Operations"; DoDD 3000.05; DoDI 8220.02; and FM 3-07 are significant steps forward and give ICT much needed attention, but much remains to be done to provide the necessary policy and doctrine guidance required to use ICT operationally as a "smart power" enabler of stability and reconstruction operations. ICT also is a critical enabler of other "smart power" missions such as HA/DR and building partnership capacity (BPC) overseas and defense support to civil authorities (DSCA) at home.

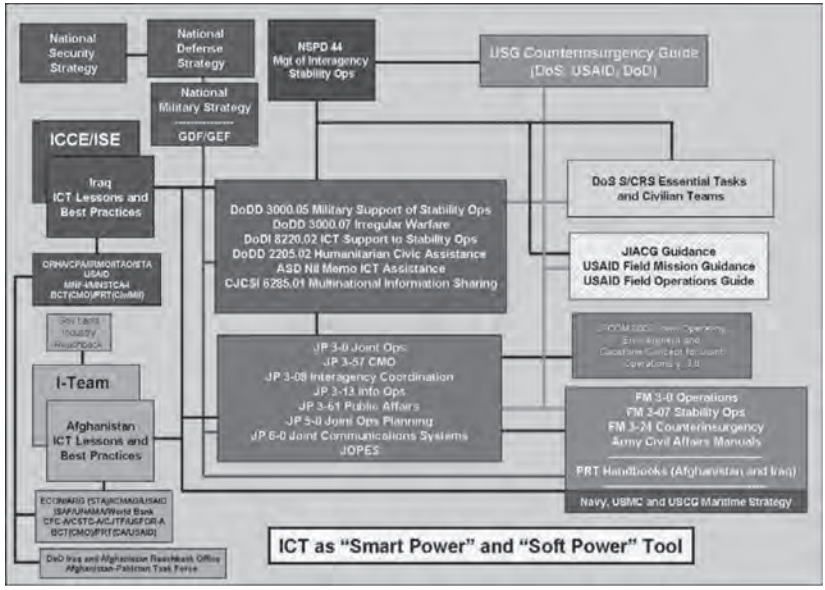

Figure 5.1. Mapping of Policy and Doctrine Documents and Ad Hoc Solutions.

The net effect of shortfalls in policy and doctrine guidance has been the need to use ad hoc approaches tailored to fill real world operational gaps. Examples include creation of various USG ad hoc reconstruction-oriented organizations (a combination of DoS and DoD personnel) in both Iraq (e.g., Iraq Reconstruction Management Office) and Afghanistan (e.g., Afghan Reconstruction Group) and the DoS's employment of senior telecom advisors (STA) at the embassies as a temporary measure to provide senior leadership in the use of commercial ICT, to provide advice to in-country USG civilian and military elements, and to deal with affected nation counterparts— there is a need to have senior civilian professionals dealing with professionals. In the absence of a coordinated USG approach, DoD implemented special arrangements, such as the Multi-National Force-Iraq (MNF-I) Communications and Information Systems (OIS) Iraq Communications Coordination Element (ICCE), created to facilitate coordination and information sharing among civilian-military ICT stakeholders, to provide ICT advice and planning focus for the use of ICT including the U.S. military use of Iraqi ICT, and to work with the Iraqi ICT counterparts. In Afghanistan, the first STA at the Kabul Embassy established an Integration-Team (I-Team) that was used to facilitate coordination and information sharing among civilian and military ICT stakeholders. He also created two reachback arrangements, one USG-focused and the other U.S. ICT industry-focused. DoD also created an Iraq and Afghanistan Reachback Office in the Pentagon to provide reconstruction assistance to all sectors. Some of the various ad hoc arrangements used in Iraq and Afghanistan are illustrated in Figure 5.1 (shown in shades of gray). Experience suggests that all of these ad hoc efforts had

varying degrees of success, and their best practices need to be captured, documented, assessed, and then applied as appropriate in future operations.

A related important task at hand that is being actively worked is to incorporate ICT as an "essential service" and as "critical infrastructure" in the appropriate policy and doctrine guidance. Additionally, efforts have been initiated to capture the best practices and key lessons from experiences in Iraq and Afghanistan and to codify and insert those lessons into appropriate policy, doctrine, planning, and operational guidance documents. While this would drive immediate effects in both of these areas of responsibility (AORs), the more important effect is to embody this policy and doctrine at the departmental level and more specifically, the Services and the combatant commands. We need to change the way we do business in the future.

Over the past 30 years, the information revolution had an important impact on the conduct of military operations. In the United States, it produced what is often called "netcentric warfare" or "netcentric operations"—the combination of shared communications, key data, analytic capabilities, and people schooled in using those capacities—that has enabled enhanced joint activities, integrated distributed capabilities, supported greater speed, and more effective maneuver. The result has been that the United States and its allies have been able to conduct very effective combat operations under a range of conditions, including quick insertion (Panama), maneuver warfare (major combat operations in Iraq), an all-air campaign (Kosovo), and a Special Forces–led effort (Afghanistan).

At the same time that major combat operations have proceeded so successfully, the United States and its allies have undertaken a variety of humanitarian assistance, disaster relief, stability, and reconstruction

operations in Somalia, Haiti, Bosnia, Kosovo, East Timor, several African countries, Afghanistan, and Iraq. These operations generally have included both economic and governance reconstruction and have spanned the full security gamut from nonviolent humanitarian assistance and peacekeeping to full-blown counterinsurgency. Not one of these operations has approached the success achieved in combat operations undertaken during the same period.

U.S. military doctrine recognizes the importance of building broad coalitions of stakeholders in complex contingencies. But, in practice, the focus of military communicators usually is on the needs of the joint or coalition force rather than on external links with civilian participants in the operation. Such external links demand that unclassified information be shared in both directions. Thus, the challenge is twofold: (1) How to encourage the military to engage more with civilians, and (2) how to encourage civilians to link better to the military or local stakeholders? However, there are other factors that need to be considered. In humanitarian operations, there are the guiding principles of impartiality, neutrality, humanity, and independence from political considerations and associated sensitivities to military involvement and intent that need to be carefully considered and managed. Caution needs to be exercised in circumstances where there is a risk that military actions may be perceived as reflecting political rather than humanitarian considerations.

Civilian organizations, including the U.S. DoS and USAID elements, believe rather strongly that the military should not be the first choice option for intervention when civilian relief activities are already there or are being put in place. International organizations

such as the United Nations (UN) and NGOs also question whether under the Oslo guidelines, the military should be involved at all in disaster relief activities.[3] Most view the use of the military as complementing civilian relief activities and should be requested only where there is no comparable civilian alternative. They argue that it is capabilities versus needed capabilities, and in the latter case, civilian assets may be adequate to get the job done. There are also concerns about mixing the use of the terms stability and humanitarian operations and in turn doing things under the banner of stability operations that are humanitarian assistance, creating misperceptions and unnecessary confusion about the purpose or the use of military assets.

There is a strong view within the civilian community that the military needs to be better informed of civilian roles, responsibilities, and capabilities, and that ambassadors need to be better informed about when it is appropriate to request military assistance. Use of the military is a more costly option. Catastrophic disasters obviously require military assistance since they are the only responder element that has the means. There is also a need to educate the civilian community about military roles, responsibilities, capabilities, and business processes. A lack of shared understanding about the civil-military stakeholder roles, responsibilities, capabilities, and limitations is a key factor that needs to be addressed through improved education and training programs and exercises that involve both military and civilian element participation—this will build a more informed and shared understanding of each other and create trust relationships before they will have to work together in a real disaster response.

Historically, ICT has proven to be a basic enabler of informal social and economic discourse, leading to

a strengthening of civil society and the promotion of security, internal stability, job creation, and economic solidity in affected nations. It is a demonstrated enabler of national transformations. There is little doubt that ICT is an engine for economic growth, a means to shape the information environment, and a means to improve social wellbeing. Advances have progressively reduced the costs of managing information, enabling individuals and organizations to undertake information-related tasks much more efficiently and have introduced innovations in products, processes, and organizational structures. ICT enables the generation of new ways of working, market development, and livelihood practices. Additional arguments as to why ICT, and host nation ICT in particular, is important in stability and reconstruction operations include but are not limited to:

- ICT can be used to help create a knowledgeable intervention, organize complex activities, and integrate stability and reconstruction operations with the affected nation.
- Affected nation ICT provides an alternative source of ICT capabilities for use by U.S. Government and coalition partners.
- ICT provides opportunities to shape the environment for stability and reconstruction operations.
- ICT is essential for prospering in a globalized economy and for establishing a knowledge culture.
- ICT can significantly change key parts of affected nation society, particularly providing young people access to global knowledge that changes sectarian attitudes and behaviors.
- ICT provides affected nation transparency to

help reduce corruption and enhance government legitimacy.

- ICT provides the best way to help every sector at once through realistic and modern e-Gov methods (security, governance, distance learning, telemedicine, geographic information system (GIS)-based agriculture, finance, power and water management, and e-commerce).
- ICT allows the U.S. Government to positively influence attitudes of the leadership and the general population of the affected nation.
- ICT is demonstrated to be one of the best generators of jobs and revenues for the affected nation.
- ICT gives situational awareness of the affected nation's forces, capabilities, and threats, which can save lives.

Numerous studies of the HA/DR and stability and reconstruction operations suggest that the strategic use of information and related technology can significantly increase the likelihood of success in affected nation cross-sector reconstruction and development. This is possible if information and ICT are engaged at the outset as part of an overall strategy that coordinates the actions of outside interveners and focuses on generating effective results for the affected nation. This has certainly been the case in business, government, and social arenas in the Western world where the information revolution has been a dynamic and positive factor. The combination of technology, information content, and people schooled in the use of each has reshaped enterprises and activities of all types around the world.

An ICT business model like that suggested in Figure 5.2, coupled with the smart use of information and

ICT, could be employed to help create a knowledgeable intervention; facilitate appropriate integration of intervener ICT reconstruction and development initiatives with the affected nation ICT strategy and plans; help organize complex activities; and enable coordination, information sharing, and implementation activities among interveners and with the affected nation, making the latter more effective. Additionally, ICT can be used to link constituent parts of an integrated multinational reconstruction and capacity-building effort, can help multiple sectors simultaneously (e.g., security, governance, education, health, agriculture, finance, and commerce) and can be used to enhance situational awareness of cross-sector reconstruction and development activities.

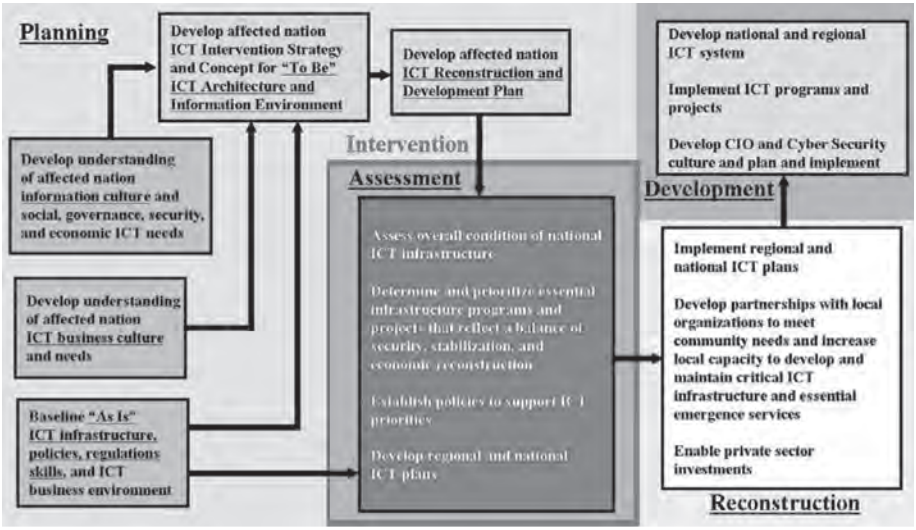

Figure 5.2. ICT Business Model.

Experiences from recent U.S. Government and coalition interventions in the Balkans, Afghanistan, and

Iraq have repeatedly demonstrated that ICT activities supporting stabilization, reconstruction, and development operations in the affected nation can be problematic. These activities suffer from a lack of adequate understanding of the affected nation information culture and related ICT business culture. There is no clear mapping of the organizational roles and responsibilities of the responding stakeholders. Program development, project coordination, information sharing, and ICT implementation are largely uncoordinated and nonstandard. There is no agreed architecture and plan for affected nation ICT reconstruction. A coherent ICT-oriented civil-military strategy and plan for intervening nations and responding IO and NGO organizations is lacking as well, and there are no agreed mechanisms and procedures to enable effective civil-military coordination and information sharing among participants and with the affected nation. Finally, donors and interveners do not consistently view ICT as a high priority need to be addressed early and as an enabler of cross-sector reconstruction and development.

New metrics are needed for measuring progress in complex operations. The U.S. Army Corps of Engineers project, Measuring Progress in Conflict Environments (MPICE), is a good start but needs to more effectively incorporate the ability to measure the impact of information and ICT as an enabler of sector reconstruction. MPICE is based on the methodology and framework proposed in the United States Institute of Peace (USIP) book, *The Quest for Viable Peace*.[4] Other tools are needed for collecting and analyzing information exchange data. For example, modeling and simulation tools to support planning and training (e.g., DARPA's Conflict Modeling, Planning, and Outcomes Experimentation [COMPOEX] program that is

a suite of tools to help military commanders and their civilian counterparts to plan, analyze, and conduct complex operations), improved processes and tools for imagery sharing (products versus raw data), and visualization tools for displaying analysis and shared situational awareness such as GIS, imagery products, and annotation, and mapping tools.

COMMERCIAL ICT CAPABILITY PACKAGES[5]

The efficient and effective deployment of communications assets into austere environments continues to be a key aspect and an important challenge of crisis response. Rapidly deployable ICT capabilities such as very small aperature terminals (VSAT) like the ground-to-air transmit and receive (GATR) and broadband global area network (BGAN) terminals, satellite phones, cell phones, voice-over Internet protocol (VoIP) phones, hand-held radios, and devices that allow disparate communications equipment to interoperate (such as the AC-1000 IP bridge) are readily available to assemble as ICT fly-away kits. However, there is no agreed upon architecture and strategy that can be used to guide responders on how to assemble deployable ICT packages and build hastily formed networks in the crisis area. It is largely an ad hoc plug and play exercise. Hence, there remains the need to help responders determine the right set of items to include in their fly-away ICT package that are simple to use and will interoperate with the ICT that others bring to the crisis.

New collaboration tools are needed that can be employed in disadvantaged information and ICT environments to facilitate collaboration (inexpensive, simple to use, and low bandwidth) and asynchronous

information sharing (need to have tools that do not overload limited bandwidth data links when synchronizing databases). Some of the existing tools include Groove, Sahana, and WebEOC. Other tools are needed that can be used to help breakdown organizational culture, business processes, and technology barriers by creating virtual communities of interest (including language translation) and open collaborative information environments. Web 2.0 tools such as wikis, blogs, Facebook, LinkedIn, Twitter, and YouTube need to be more broadly adopted by civil-military crisis responders. Other off-the-shelf tools to be considered include Toozl (open office on a memory stick) and smart phones (such as the iPhone and the BlackBerrys), and global positioning systems (GPS). Presently, there are numerous Internet websites employed during a crisis response, such as the U.S. Pacific Command (USPACOM) Asia-Pacific Advanced Network (APAN), and UN OCHA websites, such as ReliefWeb and the Virtual On-Site Operations Coordination Center, but there are no agreed guidelines for developing and populating these websites or related database standards. UN OCHA has also created an Emergency Telecoms Cluster to facilitate the deployment of ICT capability packages in disaster areas. Telecom NGOs such as NetHope and Telecoms sans Frontiers have emerged to help provide ICT capabilities in disaster areas for NGO use. All of these ICT capability packages are based on off-the-shelf commercial products and open source products on the Internet.

There is a need to develop a knowledge repository of these capabilities and best practices that can be openly shared with the broader community and is kept current with changing technology. The National Defense University (NDU) Center for Technology and National Security Policy-led project STAR-TIDES has

as part of its research program the development of a knowledge repository for ICT and the plan is to post it on the project website.[6]

ICT STRATEGY FOR STABILITY AND RECONSTRUCTION OPERATIONS-AFGHANISTAN EXAMPLE[7]

The fundamental task of an ICT strategy is to enhance affected nation capacity. That is the critical result for which the complex operation is undertaken. To achieve that result in an effective fashion, the strategy needs to accomplish two tasks, each is familiar to the international community: first, assess the affected nation and, second, establish a goal toward which to build. To put it more in the vernacular, a cure without a diagnosis will be improbable; directions without destination will be random. In short, an effective approach will require an information business plan for the affected nation. Unfortunately, the reality is that there is no agreed international or USG ICT strategy and plan, or information business plan for responding to a crisis or for engagement in a failed state intervention. Furthermore, there is little attention given to the role that information and the consideration of ICT play as essential services, as critical infrastructure, and as enablers of cross-section reconstruction. How to work with and leverage the private sector is also a deficiency in current USG civil-military thinking—it is not part of the current U.S. civilian and military government culture. There is an urgent need for the USG to change the way it does business in the information age. Some changes are starting to happen as a result of policy and doctrine changes, such as DoDD 3000.05 and DODI 8220.02, but changing culture takes time to affect TTPs and mindsets.

The assessment phase of an information and communications business plan should begin before the intervention. It must include analyses of both the information requirements and the available information technology as well as ICT business practices and government regulations and laws. Humanitarian assistance and disaster relief responses may not afford the opportunity to do a detailed assessment in advance, but even so, there is a need to do either some assessment in advance of a possible disaster, which can be used for crisis response planning, or to do a quick assessment that draws upon readily available information. Understanding what ICT capabilities might be available and whether the affected nation is a signature of the Tampere Convention,[8] is important in order to determine if and what type of ICT can legally be brought into the country and used. For more complex response operations, such as a failed-state intervention, there is generally a buildup period so there is time to prepare. An assessment should consider the pre-intervention state of information technology, infrastructure and services (voice, data, and Internet access), and the ICT business culture and information usage in the affected nation. It is important to recognize that baselines will differ in different affected nations and as a result of hostile actions.

Additionally, key elements of an information assessment will include evaluation of the affected nation's telecommunications laws and regulations, telecoms and IT services, and communication infrastructures—land line telephone system, cell phone capacity, Internet availability, cable, microwave and fiber networks, and satellite systems. It should also address usage patterns, language and literacy issues, technical and business training of locals, and financial resources.

Once an assessment has been undertaken, goals will need to be set for operationalizing the information business plan. Generally, it will be useful to time-phase the goals into an initial deployment phase, a middle phase (getting-things-going phase), and a long-term phase (exit-by-interveners). A critical point throughout is that the interveners' information business plan goals need to support the overall goals of the affected nation, and the affected nation will need to generate those goals as promptly as possible—the interveners can certainly help with developing affected nation goals.

The initial deployment phase will require the interveners to consider what deployable capabilities will be useful to help establish an affected-nation recovery. There are both structural information capabilities; such as deployable cell phone capacities, like "cell on wheels"; and the use of transportable satellites, like VSATs; and functional capabilities, like "health care in a box," shelters, renewable power, water purification, sanitization, lighting, and other capabilities that all need to be considered.

The virtue of preplanning is that key interveners can rationalize their capacities in the early, usually chaotic, days of an intervention by considering which capabilities each intervener might focus on. Equally important is to undertake such a discussion remembering that, first, numerous entities will already be in country with some capacities that can be utilized and, second, affected countries will likely have some capacity, and potentially significant capacity. Over the entirety of the intervention, the implementation of the information business plan will likely mean that the lead on different aspects of the plan will change. Broadly, one might expect a a progressive transition

from military interveners to civilian interveners to the affected nation, although the reality is likely to be more complicated and complex because such a progression will not likely be an easily identifiable or set sequence of actions. The transitions will occur over time, so there will be overlaps that need to be carefully managed. If it is understood from the beginning that there will be complex transitions in the way the plan is implemented, it will make for a more realistic and effective approach to be made part of the strategy and plan.

The middle phase of an information business plan for the affected country will focus on five key elements. The first element is to *align the affected country so that it is connected to the collaborative mechanisms used by the interveners in some fashion*. While the key interveners likely can use high-tech means, it may be that the affected country will not be able to do so. An important task of an information business plan will be to allow for low-tech to high-tech connectivity. For example, in Afghanistan, the literacy rate is so low that Internet use is necessarily limited and cell phone connectivity may be much more important. In fact, in Afghanistan, the cell phone is the lifeline communications capability. These points can be more broadly generalized: if the information business plan is to succeed, it must take account of the affected nation's information culture and the related information technology culture and the skill sets of the managers, technical personnel, and the population in general.

The second element is to *help establish working government agencies*. Depending on the overall strategy, these could be a mix of central ministries to start with and then local/district/provincial offices. Information communications technology can be used to

improve ministry effectiveness through facilitating collaboration and information sharing and extending government services from capital to urban areas to provincial and district centers to local officials. ICT and e-governance also allows for an analytic approach through budgeting and transparency of expenditures. These are crucial functions for the establishment of legitimate governance, and information technology can help each.

The creation of a viable telecom and IT business environment is key to setting the initial conditions needed to use ICT as an enabler of cross-sector reconstruction. The affected nation or host nation government needs to take important actions at the outset of the rebuilding process. A competent Minister of Communications with the intellectual and business expertise needs to be appointed to set in motion the nation's vision, strategy, and plans to grow and modernize its telecoms and IT infrastructure and services so as to become a part of the global information society. Telecom and IT laws need to be created and passed early on. A viable regulatory authority needs to be created and empowered and mechanisms need to be put in place to enforce the laws. Public sector telecoms and IT run services may be necessary to jump-start support to governance and civil security and to provide limited services to a broader population—contributing to the establishment of legitimacy, transparency, and to reduce corruption. However, it will also be necessary to consider early on the need to privatize state run enterprises as soon as it makes sense to do so to reduce corruption and provide a level playing field for private investments. Good public-private sector partnerships are important to enable the private sector to invest in growing the infrastructure and of-

fering affordable service with a state of the industry level quality of performance. Two recent real world events illustrate the benefits of initially taking the right steps, and the resulting challenges, from not doing so. For example, Afghanistan ICT is one of the major success stories emerging after years of conflict and open warfare. On the other hand, Iraq has progressed somewhat more slowly due to the continuing security situation, but things are beginning to improve and telecoms reconstruction may emerge as one of Iraq's success stories as well.

A real world example of an ICT business model that worked is Afghanistan. Significant progress has been made in the telecommunications and IT sector in Afghanistan, and it is truly a "success story" emerging out of the recovery of a country left dysfunctional from 23 years of war. Progress towards bridging the digital divide and moving Afghanistan into the 21st century information age has not been accidental but is largely due to having the right people at the right place with the right vision, energy, and expertise to make reasonable decisions and to take action to make things happen. Donor intervention to provide resources to support ICT reconstruction was a key factor as well. Afghanistan ICT success was and continues to be enabled by a number of factors:

- A Government of the Islamic Republic of Aghanistan (GIRoA) understanding of the importance of ICT as an engine of economic development and its role as an enabler of cross-sector reconstruction.
- Early GIRoA establishment of ICT policies, regulations, laws, and a regulatory authority.
- Knowledgeable and experienced Minister of Communication (MoC).

- An agreed MoC vision, strategy, and plan for moving Afghanistan ICT into the 21st century information age supported at the highest level of government, by President Hamid Karzai:
  - Five-year MoC development plan states that GIRoA should:
    a. Use the private sector and appropriate regulations to help jump-start economic recovery through enabling private-sector investments in the rapid expansion of mobile voice services and introduction of Internet service.
    b. Use the government to develop the public ICT for governance and make affordable ICT services accessible to the broader population.
    c. Consideration the early of privatization of government owned telecom and IT.
  - Early International and Regional communications access:
    a. Satellite, fiber optic and digital microwave access.
    b. Private sector international and regional gateways.
  - Robust terrestrial backbone network such as the fiber optic ring and digital microwave.
  - Early emphasis on ICT capacity building, including the establishment of related educational institutions, training facilities, and capabilities.
- Proactive MoC provision of an ICT Strategy for the Afghan National Development Strategy that sets ambitious goals for extension of telecom and IT services to the population in general and to improve governance, national and civil security, drive economic development, and improve quality of life.

- Establishment of a good public-private partnership that enables private ICT investments and rapid growth of their networks.
- International and U.S. Government community support.
  - Placed early emphasis on ICT capacity building, including the establishment of related educational institutions, training facilities, and capabilities.
  - Willingness to invest in and support Afghan MoC creation of a national telecommunications and IT network with early international access.

Differences between Afghanistan and Iraq relate largely to host country government ICT institutions, leadership, strategies, and plans for modernizing the national ICT network. There are also differences in the state of integration of affected nation ICT infrastructure and capabilities. For example, in Afghanistan the MoC is an experienced ICT professional who has a vision, strategy, and a nationally agreed plan for modernizing Afghanistan ICT, and his proactive leadership is making things happen. Additionally, he has been in place since the 2002-03 timeframe and has the support of the Afghan President and other senior government representatives. Telecom and IT laws were enacted by the Afghan parliament early on, and an independent and transparent Afghan telecom regulatory authority was established early as well. Although an MoC state-owned telecom company, Afghan Telecom, was established initially to support government communications at provincial and district levels, and to initially provide local voice and Internet access services (telekiosks) down to district level, it has already been

corporatized and is in the process of being privatized. With the move to privatize Afghan Telcom, the MoC has changed its name to Ministry of Communications and Information Technology (MCIT) and re-refocused its efforts on the use of ICT to improve Government and social services and initiatives including extension to the rural areas so the country can benefit further from ICT by becoming part of the global information society.

The ICT infrastructure of Afghan Telecom and private cellular providers is interconnected and calls can be made between the networks. The MCIT has invested in the construction of a national fiber optic ring around the country linking urban areas and providing regional cross-border and international gateway access. Cable is being implemented in urban areas and digital microwave links are being implemented throughout the country that will also have some access links to regional countries bordering Afghanistan. The private cellular providers are also building digital microwave backbone networks that include access links to regional countries. Satellite access is also used to provide connectivity and international gateway access. Finally, a good public-private partnership was created that enables the private sector to invest while discouraging unnecessary state interference.

In Iraq, the situation seems to be more problematic. The Iraqi MoC has had three different ministers in the last couple of years, and the most recent minister before the current minister was "acting," all of which negatively impacted the early leadership and decisionmaking process. A new minister has been appointed but is not a telecoms and IT experienced business person. There does not appear to be an agreed overall Iraq ICT strategy and plan, but one may emerge

in the near future. On the other hand, the Kurdish region MoC has a strategy and plan, and progress is being made in their area to modernize ICT and improve services including regional and international access. Planning for the initial network included an assumption that demand would be 90 percent voice and 10 percent data, but in reality the demand is just the opposite and the networks have not yet been adapted to meet reality. Furthermore, the networks that have emerged are independent and not interconnected, and roaming is not allowed. Calls from one network to the other must go through an international gateway. The Communications and Media Commission (CMC), the Iraq telecom and IT regulatory authority, has been without strong leadership for some time, and there are concerns about its ability to function and enforce regulations. There are also concerns about its openness and transparency. The telecom law set forth in CPA 65 remains in use since the Iraqis have not yet been able to get their own law enacted by parliament. Privatization of the state own telecom and IT providers, ITPC and SCIS, has been discussed, but no real actions have yet been taken to start the process. It has been suggested that the existence of state-owned enterprises has created perceptions and concerns on the part of the private sector about possible unfair competition. Additionally, the ITPC span of control appears to be limited, with regional elements apparently operating autonomously. In contrast, in Afghanistan, Afghan Telecom has network-wide and regional control of plans, implementation, and operations of the government owned public network.

A good public-private sector partnership does not appear to have yet been created in Iraq, and this makes outside investors nervous as well. It has been

noted by some private sector investors that they are more concerned about the Iraqi government than they are about the insurgents and, as such, this is not a situation that lends itself to promoting outside investment in Iraq. Although corruption is a common thread in both countries, it seems to be more of a concern in the Iraq ICT sector than in Afghanistan. Concerns have also been expressed regarding enough availability of Iraqi ICT trained expertise to support sustaining the operation of U.S. civil and military networks which will be turned over to the Iraqi government. The availability of ICT trained technical and management personnel is a shortfall in both Iraq and Afghanistan. Finally, in Iraq and Afghanistan the stove-piped operational performance and cost of service of the public-private sector ICT networks and services suffer from the lack of roaming among service providers and in Iraq, there is a lack of interconnection and adequate regional and international access and cost-effective service.

Use of embedded subject matter experts (SMEs) in the MCIT/MoC and regulatory authorities are also the common threads, but SMEs seemed to have been less successful in Iraq where they were used for only a short while and none, or few, are apparently being used at this time. The insurgent threat to SME safety has been a concern that is also a contributor to the unwillingness to provide SMEs to Ministries in the red zone. In Afghanistan, the SMEs have been embedded since 2002 in the MoC/MCIT providing trusted advice, continuity of support, and corporate memory. SMEs have also been used with success in other ministries and government organizations such as Afghan Telecom. Physical security threats have not been a major concern in the Afghan capital, but

SMEs are provided with contractor personal security details and they live in guarded safe houses in Kabul. Outside of Kabul it is a different story, and SMEs are not embedded in provincial or district ICT organizations. In both Iraq and Afghanistan, the attacks on ICT infrastructure have occurred, but in many cases seem to be more driven by criminal acts and extortion demands than terrorist actions. There have been incidents where towers have been blown up, switch sites attacked, and maintenance and installation staff kidnapped or even killed. Physical security is something that needs to be planned for and implemented in high threat environments and needs to be part of a national critical infrastructure protection plan. It is not clear if such plans exist in either Afghanistan or Iraq.

The third element for many stability operations will be to *increase connectivity and information flow between the central government and provincial/local governments*. Information communications technology can enhance this connectivity and information flow through, for example, the two-way flow of data and finances. It can also serve to extend government services and establish legitimacy of the government at all levels. Often, the cause of the crisis will have been differences between the central government and a region of the country, and working to bring warring elements together will be important. An information business plan can be an effective part of an overall effort.

In Afghanistan, the World Bank and USAID became engaged in ICT sector reconstruction and granted money to the Afghanistan MCIT to create a national telecommunications system to connect the central government with the country's 34 provinces and create public access centers for Internet and telephone communications at the district level. The World Bank

invested $16.8 million to develop the government communications network (GCN) and another $3.7 million to rehabilitate the International Satellite Gateway in Kabul. The GCN is a 24 node VSAT-based network that provides international voice and Internet access and communications services to support governance to the provincial capital level—governor and key administration elements, including in some cases police chiefs. USAID invested $14.2 million to develop the 365 node VSAT-based district communications network (DCN) to extend voice and Internet access to the district level for use by local government officials and the local population. GCN and DCN serve to enable good governance at the provincial and district levels by helping remote communities and government offices throughout Afghanistan communicate effectively with each other and the world. Subsequently, China, India, and Iran expressed investment interest, but outside of investments by the U.S. Government, the UN, and the World Bank there was little interest from other Western nations or international organizations. A similar government ICT infrastructure arrangement does not exist in Iraq. In this case, commercial cellular and IT services are relied upon as well as ICT networks built especially for Ministries.

Some other common threads between Afghanistan and Iraq include the need for ICT-related capacity building within ministries. This includes the establishment of effective ministry CIOs and government IT business practices including the use of IT and e-Governance capabilities, and the limited ability to effectively exploit the advantages of the ICT sector to enable governance, expand economic opportunities, and improve education and healthcare services though implementation of an effective nationwide backbone

ICT infrastructure and leveraging e-Governance, e-Commerce, e-Education, e-Healthcare, and other e-Solutions. Additionally, there is a need for developing a cyber strategy and plan and for establishing a national cyber organization and capability to protect against and respond to cyber attacks. On the Afghan private sector side, with MCIT/ATRA support GSM providers, such as Roshan, have been more progressive, with funding support from USAID and others, to offer e-Solutions using SMS for financial transactions (the M-PAISA system) and commodities pricing (the TradeNet system) for farmers. Roshan also has a call center in Kabul where, for a fee for service, subscribers can get medical advice, weather reports, and other call-in services.

In both Afghanistan and Iraq, there is no coordinated strategy for implementing Ministry IT architectures, capabilities, training, management, or governance. ICT projects at different Ministries are likely redundant, not integrated, and possibly not compatible. Some Ministries have effective enterprise networks, while others do not. Best practices may already exist, but they are not shared due to lack of visibility and limited to no cross-Ministry coordination. National CIO Councils have been set up in both Afghanistan and Iraq to implement ICT measures supporting the government's agenda for anti-corruption, transparency in governance, and cost-effective investment in ICT capabilities, but they have had only limited success and it has been hard to maintain momentum. In Afghanistan, the National CIO Council is run by the Minister of Communications and IT, and in Iraq it has in the past been run by the Minister of Science and Technology and both report to the Prime Minister's Office.

In Iraq, a shared DoS and DoD initiative to train Iraqi CIOs was initiated. In August 2008, an NDU IRMC CIO training team conducted an intensive 10-day CIO training program in Erbil for Iraqi Ministry CIOs. In early 2009, several Iraqi CIOs were brought to the United States for additional training at NDU and to provide them the opportunity to visit with U.S. CIO counterparts (both government and industry) to gain a firsthand insight into their day-to-day operations. The notion of training Afghan Ministry CIOs has been proposed several times to the Minister of Communications and IT, but no real action has been taken to make this happen. There is some concern that Ministry CIOs may not yet be ready for such training.

The fourth element will often be to *provide certain important greater functionalities in government services to the populace*. While an information business plan may not be able to improve all functionalities significantly, health and education are two arenas of consequence in which such a plan can make an important difference. In the health arena, information technology can be used to build up and interconnect local centers of health care, such as hospitals and rural health care centers; support training of health care workers; and provide valuable functionalities, such as health surveillance systems and reach back to health care subject matter experts and medical library services. In the education arena, information technology can support the development of curriculum and the provision of instruction, as well as the training of teachers. For example, in Afghanistan, ICT is used in some limited instances to connect hospitals with medical schools and with health care centers, universities such as Kabul and Khost have Computer Science programs, universities such as Kabul have partnership programs and

alliances with universities outside of Afghanistan, CISCO academies have been set up to train young girls and boys how to use computers and the Internet, and the MoC set up ICT technician training centers. There are other computer training centers emerging in the private sector as well.

The Afghanistan Ministry of Communications and IT recently initiated a Digital Inclusion Program that will enable the government of Afghanistan to adopt the modern culture of offering services to the public. The re-enabled administrative and governance system will bring transparency, efficiency, and reduce bureaucracy, but this will take some time to implement. The program will install and implement infrastructure, projects, and policies for the introduction of e-government in Afghanistan, which will empower the public to access information, communicate with government, take part in government decisionsmaking, and benefit from the economical opportunities brought by the new culture. The MCIT has also been exploring the use of the DCN as a means to provide voice and data services for health care and educational services in rural areas, as well as general public access to voice services. The wireless local loop contracts have a provision that encourages providers to also make Internet service available to schools in the areas they serve. The MCIT is also looking to use the Afghan Telecom Development Fund (based on a 2.5 percent tax on private sector cell phone calls) to extend access to ICT services to the rural areas. Similar initiatives do not appear to yet exist in Iraq, especially in rural areas. Both Afghanistan and Iraq ICT services for health care and education, and the extension of access to ICT services in rural areas, remain key challenges requiring more active host government attention.

The fifth element is to *provide for the private-sector development of information capabilities*. Two of the most important issues are informed regulatory mechanisms and useful seed financing. An overly constrained regulatory environment will make it difficult for private enterprise to operate at a profit. A properly structured set of incentives can help create an environment in which profit-making companies can contribute importantly to economic reconstruction. Seed money may be very important, especially in the early days of a stability operation, particularly to get local involvement in the development of the information business plan.

The middle phase of the plan often may be the equivalent of the medical "golden hour" for establishing a framework for effective use of ICT for the affected nation. While the information flow may be limited, meeting the expectations of the affected government and its population during this middle phase will be very important for long-term success. This lends itself to the need for a good strategic communications plan to tell the ICT story and help set and manage expectations, both ours and theirs.

The middle phase will naturally flow over into the long-term phase for the affected nation and the exit strategy for the interveners. That part of the information business plan strategy should have at least three key elements. First, as noted above, the private sector should become a key element. Early establishment of a good public-private sector partnership is essential for success. In this regard, creating an environment in which there are commercial opportunities for information communications technology solutions will encourage private sector telecom and IT firms to help seed economic revitalization. Second, the affected na-

tion will need to consider what role it will play in the development of a national information technology infrastructure. Models range from full privatization to early phase ownership to ongoing involvement. If state owned telecom and IT institutions are employed at the outset, it is important to have a clear agreement to privatize and plan for doing this in a timely manner—the earlier the better. Third, as part of their in-country effort, interveners will have to establish IT capabilities to satisfy their needs, but at the same time, these capabilities can also serve to jump-start the affected nation's capabilities and in turn to enable it to start the recovery process. Hence, such facilities and datasets should not be automatically dismantled as the interveners leave. Rather, they should be built with the intent to be used as leave-behinds for local partners, both governmental and nongovernmental, whether commercial or nonprofit. Part of the leave-behind is the need for capacity building plans to ensure that the needed affected-country ICT and management skills are available to sustain operations.

An ICT strategy includes people, content, and technology. In complex operations, the information needs—the content of what must be provided in addition to the connectivity—of the affected nation require consideration. Broadly speaking, those information content needs will fall into the categories of security, humanitarian, economic, governance/rule of law, and social.

In analyzing how such information needs should be fulfilled, an ICT strategy will recognize that the information element will support functional strategies for each of these arenas—all of which will have significant subparts. For example, the establishment of prosecutorial, court, and prison functions will have security

and rule of law/governance aspects. Significant programs will be under way to help create each of these elements as part of a stability operation. Responding to the information needs of those programs has to be an affiliated strategic effort or, to use the terms of the international community, needs to be aligned with the overall aims of the functional programs.

The specific needs may be provided with the use of information from one or more of the interveners. In a variety of ways, information technology can be utilized to provide expert assistance. A simple example is maintaining an online list of experts. More sophisticated efforts can be established, such as a call-in center for the provision of various kinds of information. Research arrangements can be set up online, as can connectivity with key national and international organizations, both governmental and nongovernmental, that are willing and able to provide assistance.

As is true for the technology itself, information needs change over time. In fact, the ability to provide information may become more important as the affected nation develops its own capacities. The capacity to access such information may be developed in two parallel fashions. First, in a traditional approach there could be an office to help facilitate access to expert management. More recently, a distributed approach, such as wikis and blogs, may be able to make a great deal of expert information available without a specific data manager, if the right information tools are provided. Issues of trust and reliability will arise, but the community approach to providing information via the Internet and Web 2.0 tools has been very powerful in other arenas, and its use in complex operations should be encouraged.[9]

The discussion of the management of information needs raises the important question of how to manage the ICT strategy in the course of the stability and reconstruction operation and how to mange the overlaps and transition from military to civilian lead. Adoption of a strategic approach and even operational activities will be greatly facilitated by the establishment of a forward field organization. Ideally, this would be a joint DoS-DoD function with the task of carrying out the information and ICT strategies and plan in country. In complex operations, the organization likely would initially be collocated with the military command activity and at some point transitioned to DoS/Embassy. Ad hoc arrangements such as the Afghan Reconstruction Group and the Iraq Reconstruction Management Office/Iraq Transition Assistance Office, along with their respective senior telecom advisor positions, are models worth reviewing for future operations. Additionally, the role and effectiveness of the I-Team and the reach back support to the Afghanistan ICT and the Iraq ICCE are other models to review. There is certainly a need to institutionalize the USG ICT support process for future operations and to revisit the creation of a senior telecoms advisor position to focus USG support on the affected nation ICT reconstruction and its use as a cross-sector enabler. There is also a need to develop an agreed approach to establishing a civil-military collaborative information environment to support complex operations collaboration and information sharing and shared reconstruction-oriented situation awareness with ICT as a key element to be tracked. Also, there is a need to include a strategic communications program to tell the ICT success stories and to make information available to stakeholders using open source technology such as portals and Web 2.0 and beyond capabilities. [10]

The role of the organization would include carrying out the USG aspects of the ICT strategy and plan. In addition, the organization would collaborate with the organizations with which preplanning took place, including key countries, the UN, the World Bank, and major NGOs. As promptly as possible, the organization would want to begin to work with the affected nation, though precisely what that means will depend on the unique circumstances of the operation. As a forward community of interest is being set up, the organization will want to create mechanisms that add additional entities to the effort that have not been part of the preplanning. The DoD is encouraging the development of an open-source, collaborative arena, tentatively called "the hub," that would use blogging, file-sharing, and Wikipedia-type and Web 2.0 approaches to create an open space for collaborative sharing.[11] This hub type approach may be very valuable, as may more structured relationships. In addition, the organization will want to work with the public affairs office (PAO) to facilitate interaction with the media and, most importantly, information for the public at large. For example, U.S. commanders in Afghanistan recently launched their "social networking strategy" for Afghanistan using the hugely popular website Twitter to release information about some of their operations,[12] a Facebook page,[13] and the popular YouTube video sharing site[14] to post videos about their work and the daily lives of U.S. troops. The decision to use the latest Internet fad was meant to "engage non-traditional audiences directly with news, videos, pictures, and other information from Operation Enduring Freedom," the U.S. military said, and to "preempt extremist propaganda."[15]

OBSERVATIONS

ICT can be important components for success in complex operations. To achieve successful results requires that a purposeful strategy be adopted to use these capabilities to achieve the desired end of facilitating recovery and building up the affected nation and to develop operational activities that effectively implement the strategy. A strategic approach causes coalition participants to undertake five key activities:

1. Conduct pre-event activities with partners,
2. Implement improved collaboration,
3. Ensure improved data usability,
4. Develop an information toolbox, and
5. Create a forward field information office.

Also, creating an overall focus to generate an effective affected nation information business plan consists of four actionable items:

1. Assess the affected nation information capacity and culture and business processes,
2. Build an affected nation information goal,
3. Create immediate, medium, and long-term in formation capacities, and
4. Analyze information needs and develop methods to fulfill those needs.

Civil-Military collaboration and information sharing activities can have decisive impacts in complex operations. To more effectively address shortfalls in responder activities, they need to be treated as a core part of the nation's overall strategy and, as noted earlier, not just as "nice to have" adjuncts to the kinetic phases of warfare. U.S. military and civilian government agencies need to start to "think" information

and ICT. Key points to consider for future operations include:

- "Think" Information and Information Communications Technology (ICT)
  - Collaboration and information sharing
  - Enabler of cross-sector reconstruction
  - Influence operations
  - Enabler of "unity of effort" across the civil-military boundaries;
- Think and do "whole of government"
  - Diplomacy, defense, and development
  - Enable the "affected nation" do not do it for them;
- View ICT as an "essential service" and as "critical infrastructure";
- Engage and leverage the "new media" such as Web 2.0 and beyond;
- Metrics for ICT need to measure "outcomes" not just outputs;
- Employ information and ICT capabilities as a means to inform, influence, and build trust.

Furthering this argument, in complex operations the United States cannot achieve the social, political, and economic goals for which its military forces are committed unless the overall U.S. Government can engage effectively with local governments, businesses, and members of civil society.[16] Additionally, improvements in information sharing will need to proactively address changes that reflect:

- Culture: "The Will to Share";
- Policy: "The Rules for Sharing";
- Governance: "The Environment to Influence Sharing";
- Economics and Resources: "The Value of Sharing";

- Technology and Infrastructure: "The Capability to Enable Sharing.

As noted, Information and ICT can significantly increase the likelihood of success in complex operations—if they are engaged as part of an overall strategy that coordinates the actions of the whole of U.S. Government (interagency) and, as appropriate, outside IO, IGO, NGO, international business, and other civil-military stakeholders. The focus also needs to be on generating effective results for the host or affected nation—enable the host or affected nations to be successful. Properly utilized, ICT can help create effective initiatives and knowledgeable interventions, organize complex activities, and integrate complex operations with the host or affected nation, making the latter more effective.

Key to these results is a U.S. Government strategy that requires that: (1) the U.S. Government must give high priority to such a whole of government approach and ensure that the effort is a joint civilian-military activity; (2) the military and other U.S. Government elements need to "think" information and ICT and treat ICT as an "essential service" and make it a part of policy and doctrine for and the planning and execution of complex operation; (3) preplanning and the establishment of ICT partnerships is undertaken with key regular participants in complex operations, such as NATO, the United Nations (UN), the World Bank and others such as regional nations in affected nation area; (4) the focus of initiatives and complex interventions, including the use of ICT, is on supporting and enabling the host or affected nation governmental, security, societal, and economic development; and (5) key information technology capabilities are harnessed

to support the strategy. Implementing the strategy will include: (1) development of an information business plan for host and affected nations so that ICT is effectively used to support security cooperation, capacity building, and stabilization and reconstruction; (2) agreements among complex operations stakeholders on data-sharing and collaboration, including data-sharing on a differentiated basis; and (3) use of commercial IT tools and data provided on an unclassified basis as appropriate.[17]

Enhancing the influence of U.S. Government responses to HA/DR and interventions into stability and reconstruction operations will require a multifaceted strategic communications strategy that differentiates the circumstances of the messages, key places of delivery, and sophistication with which messages are created and delivered, with particular focus on channels and messengers. To improve in these areas, the U.S. Government must focus on actions that include discerning the nature of the audiences, societies, and cultures into which messages will be delivered; increasing the number of experts in geographic and cultural arenas, particularly in languages; augmenting resources for overall strategic communications and ICT influence efforts; encouraging long-term communications and ICT influence efforts along with short-term responses; and understanding that successful strategic communications and ICT influence operations cannot be achieved by the U.S. Government acting on its own; allies and partners are needed both to shape our messages and to support theirs.[18]

ENDNOTES - CHAPTER 5

1. Frank Kramer, Stuart Starr, and Larry Wentz, *Cyberpower and National Security*, Washington, DC: Center for Technology and National Security Policy, National Defense University (NDU) Press, 2009.

2. Larry Wentz, *An ICT Primer: ICT for Civil-Military Coordination in Disaster Relief and Stabilization and Reconstruction*, Defense and Technology Paper 31, Washington, DC: Center for Technology and National Security Policy, National Defense University, July 2006.

3. See UN OCHA website for details on use the of foreign military assets in disaster relief, available from *ochaonline.un.org/AboutOCHA/Organigramme/EmergencyServicesBranchESB/CivilMilitaryCoordinationSection/PolicyGuidanceandPublications/tabid/1403/language/en-US/Default.aspx*.

4. Jock Covey, Michael Dziedzic, and Leonard Hawley, eds., *The Quest for Viable Peace: International Intervention and Strategies for Conflict Transformation*, Washington, DC: U.S. Institute for Peace Press, May 2005.

5. Wentz.

6. Website address is *www.star-tides.net*.

7. Frank Kramer, Stuart Starr, and Larry Wentz, "I-Power: Using the Information Revolution for Success in Stability Operations," *Defense Horizons*, No. 55, January 2007, pp. 1-8.

8. For nations that have ratified the Tampere Convention, regulatory barriers are waved for telecommunications to be used in disasters, available from *www.itu.int/ITU-D/emergencytelecoms/tampere.html*.

9. Mark Drapeau and Linton Wells II, *Social Software and National Security: An Initial Net Assessment*, Defense and Technology Paper 61, Washington, DC: Center for Technology and National Security Policy National Defense University, April 2009.

10. Kramer, Starr, and Wentz, *Cyberpower and National Security*.

11. Drapeau and Wells, *Social Software and National Security*.

12. Available from *twitter.com/usfora*.

13. Available from *tiny.cc/MJtsf*.

14. Available from *www.youtube.com/usfora*.

15. Paul Tait and Jerry Norton, "U.S. Military Turns to Twitter for Afghan Hard News," Reuters, June 2, 2009, available from *Reuters.com/article/idussp477109.*

16. Hans Binnendijk and Patrick M. Cronin, *Civilian Surge: Key to Complex Operations*, Washington, DC: Center for Technology and National Security Policy, National Defense University, December 2008.

17. Kramer, Starr, and Wentz, *I-Power*.

18. Franklin D. Kramer and Larry Wentz, "Cyber Influence and International Security," *Defense Horizons,* No. 61, January 2008, pp. 1-11.