ENGINEERING-PDH.com
ONLINE CONTINUING EDUCATION

CYBER INFRASTRUCTURE PROTECTION - VOL 2 - PART 3 OF 3

Main Category:	Electrical Engineering
Sub Category:	-
Course #:	ELE-149
Course Content:	52 pgs
PDH/CE Hours:	4

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-149 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 refence material, a significant issue with many anomaly detection-based approaches is their potentially high false-negative rate.
    a. True
    b. False
2. Table 9-2 suggests a potential decomposition of the MoMs associated with the cyber problem. Which of the following measures corresponds to the statement: Time to create, validate, and disseminate influence messages?
    a. Entity Empowerment
    b. Effectiveness
    c. Functional Performance
    d. Performance
3. A set of anomaly detectors analyzes the collected data and generates alerts when anomalies are detected. Which of the following anomaly detectors is NOT mentioned in the reference material?
    a. Frequency Anomaly Detectors
    b. Profile Anomaly Detectors
    c. Source Anomaly Detectors
    d. Volume Anomaly Detectors
4. According to the reference material, it has been estimated that in recent months, approximately 90 percent of the traffic on the Internet is spam.
    a. True
    b. False

5. Which of the following anomaly detectors fits the description: examines the flow-level behavior of individual nodes within the monitored network in conjunction with Blacklist/Whitelist information to identify potentially malicious nodes?
    a. Frequency Anomaly Detectors
    b. Profile Anomaly Detectors
    c. Source Anomaly Detectors
    d. Volume Anomaly Detectors
6. According to the reference material, as the bandwidth increases to the megahertz/sec range, the user is able to access advanced features such as imagery and video products.
    a. True
    b. False
7. According to the reference material, the system is designed to scale to Tier 1 ISP data rates wherein several _____ of flow data could be generated every few minutes.
    a. Kilobytes
    b. Megabytes
    c. Gigabytes
    d. Terabytes
8. According to the reference material, in the area of cyber strategy, there is the need to develop and apply risk assessment tools that enable one to estimate the probability and consequence of a cyber-attack.
    a. True
    b. False
9. Which of the following anomaly detectors fits the description: operates by considering a near-term moving window of flow records when computing traffic volumes to a destination address?
    a. Frequency Anomaly Detectors
    b. Profile Anomaly Detectors
    c. Source Anomaly Detectors
    d. Volume Anomaly Detectors
10. According to the reference material, our primary assessment tools for cyber power deal with the impact of changes in cyberspace on the military and informational levers of national power.
    a. True
    b. False

PART III:

CYBER INFRASTRUCTURE

CHAPTER 8

ISP GRADE THREAT MONITORING

Abhrajit Ghosh

INTRODUCTION

Today's Internet Service Provider (ISP) has to deal with various types of threats that impact not only its operations but also those of its customers. These threats manifest in the form of malicious network traffic that may either overload the network infrastructure (e.g., Distributed Denial of Service [DDoS]) or enable the execution of illegal activities (e.g., spam, identity [ID] theft). ISPs can typically provision excess network capacity to deal with volume-based attacks; however, their end customers may not always be able to do so. Consequently, it is very often the ISPs' responsibility to detect and mitigate attacks that target their customers. Originators of malicious activities that are relatively stealthy in nature cannot easily be monitored from their targets, because of the intermittent nature of the activity observed at each individual target. However, an ISP has access to substantially more data on each node within its administrative domain and is in a better position to detect originators of potentially malicious activities, as well as to mitigate the threat posed by them. According to Arbor Networks, the most significant threat faced by IP network operators today is host- or link-level DDoS.[1] A significant portion of DDoS attacks are known to employ IP Spoofing; a technique that allows an attacker to fake source addresses on attack traffic. The use of IP Spoofing makes it more difficult to trace the attack back to

its source and delays the start of mitigation. Another significant source of concern is botnet activity. Botnets are networks of (typically) illegitimately controlled computers, spread across the public Internet, under the control of one or more so-called bot-herders. While botnets can be employed for the purpose of originating DDoS attacks, they may also be used to run large spam-delivery operations, which may in turn be used to propagate malicious code onto unsuspecting network users' computers. Botnets can also be used to explore compromised hosts and networks for valuable data to exfiltrate into the hands of an adversary.

Many ISPs operate Security Operation Centers (SOCs), wherein dedicated systems and personnel monitor and analyze data feeds to detect the occurrence of malicious activities. The volume of data available at an ISP's SOC can be challenging for most analysis systems. It is essential that the data collection strategy as well as the analysis algorithms be tuned to such data volumes.

MONITORING FOR THREATS

Several approaches have been proposed in the past for detection of volume-based network attacks. Volume analysis approaches make use of flow record export capabilities at network routers such as sFlow[2] and NetFlow[3] in conjunction with flow-collection software such as nfdump[4] and flow-tools.[5] Analysis algorithms look for evidence of anomalous traffic volumes in the exported flow records. The operation of these components appears in Figure 8-1. Traffic enters a network via one of its edge routers and may traverse one or more core routers before exiting. It is possible to enable flow data export capabilities on either core or

edge routers. In many cases, network operators minimize the processing load on routers by mirroring traffic observed at the routers to dedicated flow agents. In the latter case, flow agents act as flow exporters, thus offloading some of the flow data export load from the routers. Exported flow data are directed to one or more flow collectors, which typically save flow information into persistent storage for subsequent analysis. Various flavors of analysis tools are available; for example, nfdump provides tools to compute statistical data on individual flows or on flow aggregates. Tools such as Nfsen provide graphical web-based front ends for flow analysis visualization.[6]

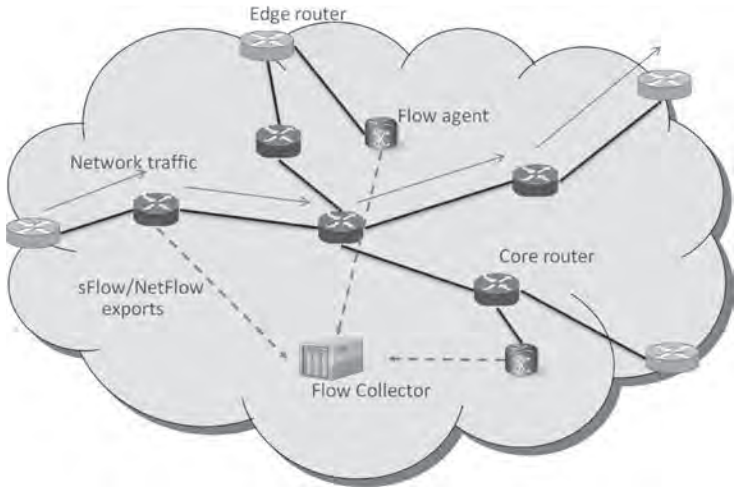

Figure 8-1. Flow Data Collection.

An alternative approach is to use Simple Network Management Protocol (SNMP)-based network monitoring tools to observe standard network monitoring Management Information Bases (MIBs).[7] For example, packets-per-second counters within the

SNMP MIB structure at a router can be used to detect volume anomalies. SNMP-based detection of volume anomalies is inherently coarser grained than the flow analysis-based approaches. On the other hand, SNMP data analysis is a lighter weight process than flow data analysis. Both methods cannot by themselves distinguish between legitimate and illegitimate volume anomalies.

Deep Packet Inspection (DPI)-based approaches provide a means to inspect every byte of every packet passing through the inspection device.[8] This approach allows for the inspection of the application payload the packet carries and can help identify the program or service being used. DPI-based approaches are especially useful for applications that use nonstandard ports such as Skype and other peer-to-peer applications. As such, this is a computationally intensive process, especially at high network data rates, and is typically implemented using custom hardware solutions. The use of custom hardware makes DPI approaches fairly expensive for large-scale deployments. In addition, DPI approaches may not be very useful if the inspected data payloads are encrypted. An approach for using DPI-based solutions is to compare observed application payloads with known attack signatures. However, this requires the maintenance of an attack signature repository and is not very useful when considered in the context of zero-day attacks.

SECURITY MONITORING SYSTEM

Telcordia has spent several years researching various aspects of network security; in particular, the problem of monitoring large-scale networks for malicious activity. The company has developed a system

for large-scale security monitoring that examines data exported by flow agents for anomalies. An illustration of a typical deployment appears in Figure 8-2. The system receives NetFlow and sFlow feeds from multiple flow agents located within the monitored network. It also periodically downloads the following types of data from publicly accessible sources:

- BGP (Border Gateway Protocol) routing information from public BGP Routing Information Bases (RIBs).[9]
- BGP Autonomous System (AS) number registration information from Internet Routing Registries (IRRs).[10]
- Blacklisted IP address lists from Domain Name System Blacklists (DNSBLs)[11] and legitimate IP address lists from Domain Name System Whitelists (DNSWLs).[12]

Flow data are analyzed in conjunction with the above types of data sources for anomalies.

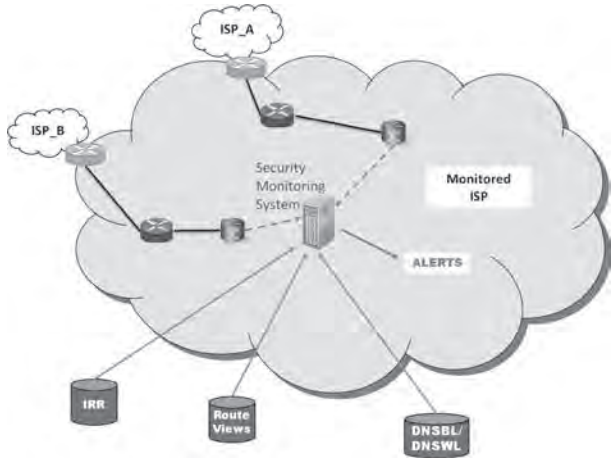

Figure 8-2. Security Monitoring System Deployment.

The goal of the system is to detect various types of network traffic anomalies that could be caused by DDoS, spamming, IP address spoofing, and botnet activities. The system is designed to scale to Tier 1 ISP data rates wherein several gigabytes of flow data could be generated every few minutes.

A high level architecture of the monitoring system appears in Figure 8-3. A set of data collectors acquires flow data from within the monitored network and publicly accessible data from the types of sources listed above that reside outside the monitored network. Collected data are written into persistent storage, which consists of an SQL database and a set of flat files.

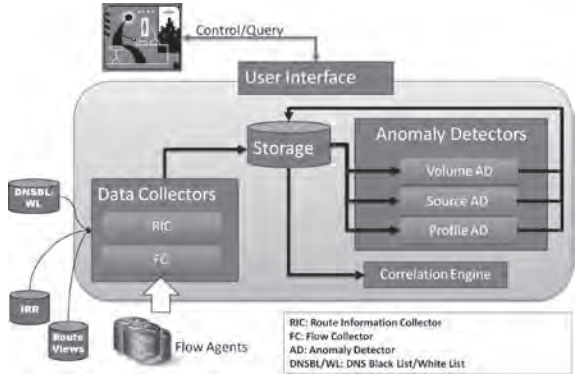

Figure 8-3. Monitoring System Architecture.

A set of anomaly detectors analyzes the collected data and generates alerts when anomalies are detected. Currently three types of anomaly detectors are provided: (a) Volume Anomaly Detectors; (b) Source Anomaly Detectors; and, (c) Profile Anomaly Detectors. The Volume Anomaly Detector analyzes collected data for volume anomalies using a variety of approaches. The Source Anomaly detector incorporates algorithms for

spoofed-source IP address detection and makes use of flow data, BGP routing data, and AS number registration data. The Profile Anomaly detector examines the flow-level behavior of individual nodes within the monitored network in conjunction with Blacklist/Whitelist information to identify potentially malicious nodes. Each Anomaly Detector outputs the result of its analysis into a structured query language (SQL) table.

Results of the outputs of various anomaly detectors can be analyzed in conjunction with each other using the Correlation Engine. The Correlation Engine attempts to determine if detected anomalous activities are contemporaneous. It also attempts to identify if an attack source generating one type of attack is also responsible for other types of attacks. As such, the correlation engine provides a means to reduce the overall false-positive rate of the monitoring system.

SECURE ANOMALY DETECTION

The goal of the source anomaly detectors is to identify instances of source IP address spoofing in observed flows. The basic principle of the operation of source anomaly detectors appears in Figure 8-4. Here, data for the monitored ISP are acquired via NetFlow/sFlow data feeds from three flow agents. Source address profiles are generated for each flow agent using training flow data. Alerts are raised when a source IP address that does not match a flow agent's profile is observed at the agent. For example, during training, source IP addresses from ISP_D are expected at flow agent FA2, while source IP addresses from ISP_A are expected at FA1. An alert will occur if flows with source IP addresses from ISP_D are observed at FA1, since this could be evidence of a possible spoofing attack.

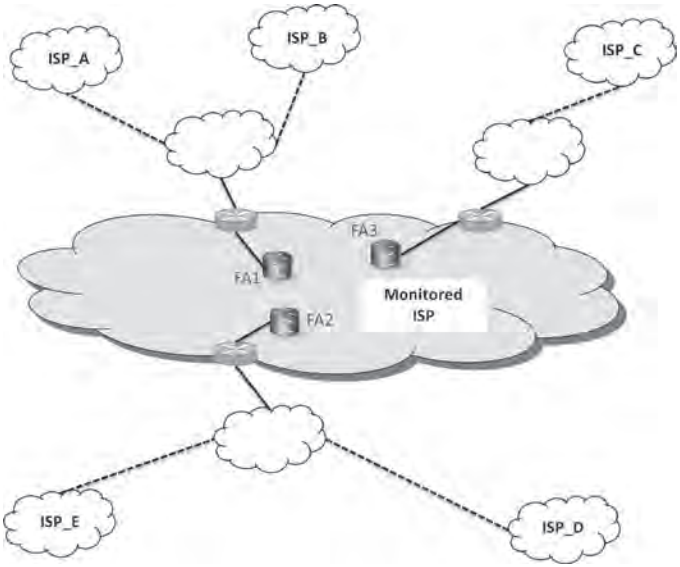

Figure 8-4. Source Anomaly Detection Overview.

While using training data, care must be taken to reduce the possibility of using spoofed traffic to build the source address profiles. While building the profiles, care can be taken by considering only flows for established TCP connections and by ignoring flows to destinations receiving data from bogon sources. It is also possible that training data may not be adequate to cover all potential sources of traffic. One can address this potential issue by considering profiles based on BGP AS numbers, given that a single BGP AS number can map to several IP address prefixes, including those prefixes not observed during training.

PROFILE ANOMALY DETECTION

The profile anomaly detectors detect any behavioral anomalies pertaining to hosts within the monitored network. One profile anomaly detector, that is

currently part of the system, identifies potential spammers using flow data and spammer blacklists. Figure 8-5 illustrates the operation of the spammer detector. This detector operates in a two-step process.

1. Training: During this process, training flows build a communication profile for each suspected spammer node. Nodes with similar communication profiles are grouped into clusters. Subsequently, IP address blacklists and whitelists identify clusters that contain known spammers. The existing clusters are then labeled as spammer clusters or as non-spammer clusters.

2. Judgment: As in the training case, observed flows build communication profiles for suspected spammer nodes. The best matching cluster is identified for each communication profile. A node is identified as a spammer if its profile matches a spammer cluster.

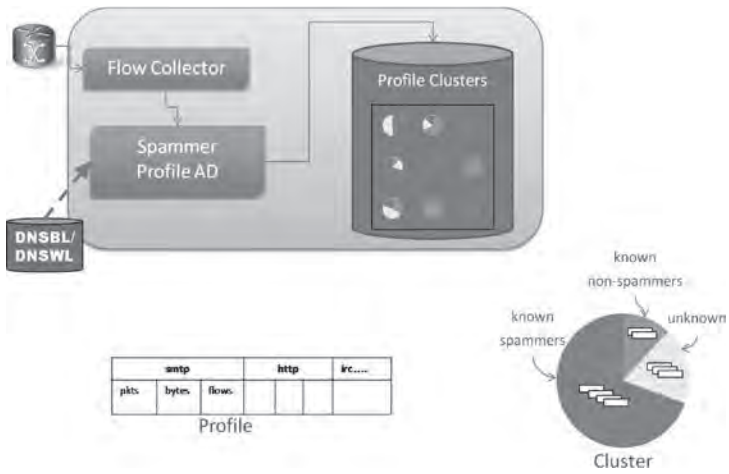

Figure 8-5. Spammer Detection Overview.

VOLUME ANOMALY DETECTION

Our system incorporates an efficient real-time volume anomaly detector that gives early warning of observed volume anomalies. The volume anomaly detector operates by considering a near-term moving window of flow records when computing traffic volumes to a destination address. The operation of the real-time volume anomaly detector appears in Figure 8-6. Flow records from flow agents are stored in memory over a user-defined time window (e.g., 5 minutes). Traffic volumes are computed for destinations observed within a given time window and are compared against operator-specified thresholds to determine the presence of anomalies. This approach eliminates the need to create large archives of flow records for the purpose of volume-based analysis and allows more timely detection of anomalies in the observed data. The approach is also somewhat more accurate than the archive-based approach, since it is not constrained by artificial time boundaries used while archiving files.

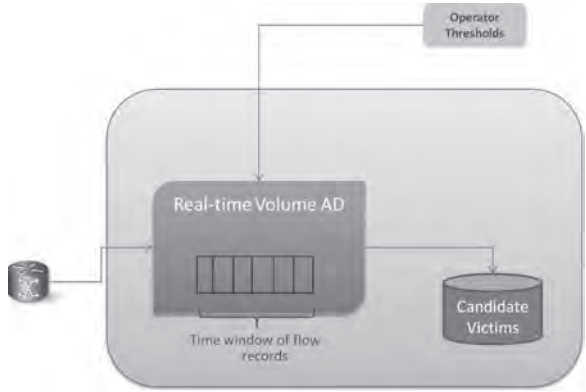

Figure 8-6. Volume Anomaly Detection Overview.

ANOMALY CORRELATION

Our system incorporates a correlation engine that correlates alerts generated by the different types of anomaly detectors. A significant issue with many anomaly detection-based approaches is their potentially high false-positive rate. The correlation engine component reduces the possibility of generating false positives.

Different types of correlations are performed by the system. These may be based on the source IP addresses of observed flows or on their destination IP addresses. For example, source anomaly alerts correlate with volume anomaly alerts to determine whether a volume anomaly targeting a specific destination is happening at the same time as source anomalies are observed. Also, volume anomaly alerts correlate with profile anomaly alerts to determine whether a source of elevated traffic volumes has performed other types of malicious activities such as spamming or participation in a botnet.

CONCLUSION

Our system offers several advantages to an operator who may be interested in monitoring the network for potentially malicious activity. It integrates with standardized data sources, such as NetFlow and sFlow. It has also been evaluated in a Tier 1 ISP environment and has scaled to the high data rates observed therein. There is also no requirement for specialized hardware, as is the case for many current solutions (for example, DPI approaches); the approach is software based and therefore portable.

The use of an alert correlation component is valuable to a network operator who would be very interested in lowering false-positive rates. Given the high data volumes, even a relatively small false-positive rate can lead to a significant number of alerts that may confuse a human operator. This approach uses behavioral anomalies to identify potentially malicious nodes in the target network and is thus in a position to be able to detect zero-day attacks by not depending on the availability of attack signatures. Our system can potentially be used by a network operator to support the delivery of revenue-generating attack detection services to interested customers.

ENDNOTES - CHAPTER 8

1. Arbor Networks, "Worldwide Infrastructure Security Report, Volume V," *www.arbornetworks.com/report*.

2. P. Phaal *et al*., "InMon Corporation's sFlow: A Method for Monitoring Traffic in Switched and Routed Networks," IETF RFC 3176, September 2001.

3. B. Claise, Ed., "Cisco Systems NetFlow Services Export Version 9," IETF RFC 3954, October 2004.

4. See *nfdump.sourceforge.net/*.

5. See *code.google.com/p/flow-tools/*.

6. See *nfsen.sourceforge.net/*.

7. V. Sekar *et al*., "LADS: Large-scale Automated DDoS detection System," USENIX Annual Technical Conference, 2006.

8. T. AbuHmed *et al*., "A Survey on Deep Packet Inspection for Intrusion Detection Systems," *Magazine of Korea Telecommunication Society*, Vol. 24, No. 11, pp. 25-36, November 2007.

9. See *www.routeviews.org/*.

10. See *www.irr.net/*.

11. See *www.uceprotect.net/en/index.php*.

12. See *www.whitelisted.org/*.

CHAPTER 9

THE CHALLEGES ASSOCIATED WITH ASSESSING CYBER ISSUES

Stuart H. Starr

INTRODUCTION

Since the issuance of the 2010 *Quadrennial Defense Review* (QDR), there has been a growing appreciation of the challenges associated with assessing irregular warfare. In particular, there is an understanding that cyber issues are of increased importance in future irregular wars. This manifests in adversary exfiltration of data from sensitive but unclassified databases, cyber attacks on sovereign nations (e.g., Estonia and Georgia), and the fear that critical infrastructures may be the target of a "cyber Pearl Harbor." However, the assessment community is having a difficult time characterizing the current ability to assess cyber issues and prioritizing actions to improve that capability.

The goal of this chapter is to explore the state-of-the-art in the ability to assess cyber issues. To illuminate this problem, the chapter presents a tentative decomposition of the problem into manageable subsets. Using that deconstruction, it identifies candidate cyber policy issues that warrant further analysis and identifies and illustrates candidate Measures of Merit (MoMs). Subsequently, the chapter characterizes some of the more promising existing cyber assessment capabilities that the community is employing, followed by an identification of several cyber assessment capabilities that will be necessary to support future cyber policy assessments. The chapter concludes with a brief

identification of high priority cyber assessment efforts to pursue.

DECOMPOSITION OF THE PROBLEM

To structure the problem, the holistic cyber framework is depicted in Figure 9-1. This framework is patterned after the triangular framework that the military operations research community has employed to decompose the dimensions of traditional warfare. In that framework, the base consists of systems models, upon which rests more complex, higher orders of interactions (e.g., engagements, tactical operations, campaigns). Historically, the outputs from the lower levels provide the feedback to the higher levels of the triangle.

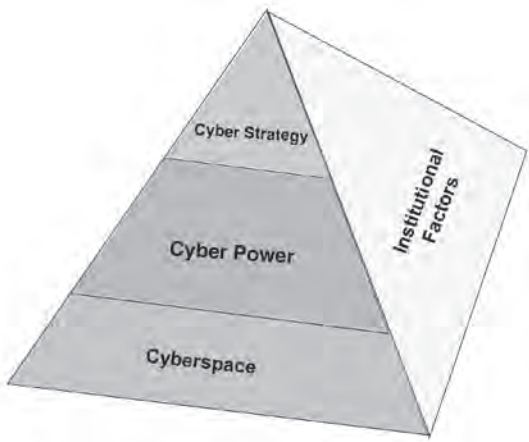

Figure 9-1. Decomposition of the Problem.

By analogy, the bottom of the pyramid consists of "cyberspace," the components, systems, and systems-of-systems that comprise the cyber infrastructure.[1] The

output from this cyber infrastructure enhances "cyber power," the traditional instruments of power: political/diplomatic, informational military, and economic (P/DIME).[2] These instruments of power, in turn, provide the basis for "cyber strategy," the empowerment of the entities at the top of the pyramid.[3] These entities include, *inter alia,* individuals, terrorists, transnational criminals, corporations, nation-states, and international organizations. Note that while nation-states have access to all of these instruments of power, the other entities generally have access to only a subset of them. In addition, initiatives, such as deterrence and treaties, may provide the basis for limiting the empowerment of key entities.

The pyramid suggests that each of these levels is affected by institutional factors. These include governance, legal considerations, regulation, critical infrastructure protection, and consideration of civil liberties.

KEY CYBER POLICY ISSUES

Senior decisionmakers have identified several key policy issues that require further attention (see Table 9.1). Note that this list is representative rather than comprehensive. In Table 9.1, these issues have been aggregated into the categories of cyberspace, cyber power, cyber strategy, and institutional factors. Note that most of these issues are extremely broad and contentious. Consequently, new methods, tools, data, and intellectual capital must address them adequately. In particular, there is a need to cast these issues in the proper context so that one can deal with all of the factors of interest.

Category	Key Issues
Cyberspace	What steps should be taken to enhance the **security** of cyberspace?
	What **resources** are needed to make cyberspace resistant to adversary attacks?
Cyber Power	What **risks** does the military face in implementing Net-Centric Operations?
	How **vulnerable** is the network to computer network attack?
	How should Web 2.0 technologies be exploited to enchance **Influence Operations**?
Cyber Strategy	What **norms** should be used among civilized nations?
	What steps should be taken to enhance **cyber deterrence**?
Institutional Factors	When does a cyber attack rise to the level of an **act of war**?
	What **cascading effects** are faced in attacks against critical infrastructures?
	What steps should be **organized** to mitigate cyber risks?

Table 9-1. Selected Cyber Policy Issues.

MEASURES OF MERIT FOR CYBER ISSUES

Table 9-2 suggests a potential decomposition of the MoMs associated with the cyber problem. It identifies four linked sets of measures: Measures of Performance (MoPs), Measures of Functional Performance (MoFPs), Measures of Effectiveness (MoEs), and Measures of Entity Empowerment (MoEEs). Since this field of endeavor is still in its infancy, the material is meant to be illustrative and not exhaustive.

Measures	Representative Measures
Cyber Strategy— Entity Empowerment	• Political reforms (e.g., participation in democratic elections) • Military efforts to enhance security (e.g., reduction in number, severity of insurgent, terrorist attacks) • Economical reforms (e.g., reconstruction projects completed) • Social reforms (e.g., reconciliation of warring parties) • Information (e.g., gaining trust of host nation population) • Infrastructure (e.g., improvement in delivery of electric power, clean water)
Effectiveness (against targeted groups)	• Informational • Media: Number of positive/negative stories published/aired • Clerics: Tone of mosque sermons • Military: Loss Exchange Ratios
Functional Performance	• Informational • Time to create, validate, and disseminate influence messages • Number of meetings held with surrogate groups
Performance	• System performance (e.g., latency, bandwidth, reliability) • Resistance to adversary attack (e.g., ability to withstand a Denial of Service attack)

Table 9-2. Representative Measures of Merit.

MoPs are needed to characterize the key computer science and electrical engineering dimensions of the problem. A key measure is the amount of bandwidth that is available to representative users of cyberspace. As the bandwidth increases to the megahertz/sec range, the user is able to access advanced features such as imagery and video products. A second key measure is connectivity. For circumstances in which the cyber infrastructure is fixed, a useful measure is the percent of people in a country who have access to

the Internet. However, in many military operations, the cyber infrastructure and the users are mobile. Under these circumstances, a more useful measure is the performance of Mobile, Ad hoc NETwork (MANET) users (e.g., their ability to stay connected). Third, one can introduce measures of the "noise" that characterizes the cyber infrastructure. For example, the extent to which the quality of the Internet is degraded can be characterized by the unwanted email that it carries ("spam"), which can subsume a substantial subset of the network's capacity. As an example, it has been estimated that in recent months, approximately 90 percent of the traffic on the Internet is spam.[4] In addition, the integrity of the information is further compromised by "phishing" exploits in which criminal elements seek to employ the Internet to perpetrate economic scams. Finally, MoPs can be introduced to characterize resistance to adversary actions, including distributed denial of service (DDoS) attacks, propagation of viruses or worms, and illicitly intruding into a system.

It is useful to introduce MoFPs that characterize how successfully selected entities are able to perform key functions, taking advantage of cyberspace. In the case of the U.S. military, the concept of net-centricity is to employ advances in cyberspace to perform essential functions (e.g., use digital links to disseminate a holistic view of the situation to individual weapon systems). Similarly, a basic tenet of net-centricity is to propagate the commander's intent so that the participants in the operation can synchronize their actions.

MoEs must characterize how effective entities can be in their key missions, taking advantage of cyberspace. In the context of major combat operations, MoEs need to characterize the ability to exploit cyberspace

in multiple dimensions. At one extreme, enhancements in cyberspace have the potential to reduce the time to conduct a campaign and the casualties associated with the campaign. At the other extreme, enhancements in cyberspace may substantially enhance blue-loss exchange ratios and the amount of ground gained and controlled.

From the perspective of cyber strategy, there is interest in characterizing the extent to which enhancements in cyberspace can empower key entities. In the case of nation-states, potential MoEEs might include selected political, military, economic, social, informational, and infrastructure (PMESII) variables. As an example, it might address the ability to leverage cyberspace to influence a population (e.g., "win hearts and minds"); shape a nation at strategic crossroads; and deter, persuade, and coerce an adversary.

EXISTING CYBER ASSESSMENT CAPABILITIES

Currently, there are many methods, tools, and data that are being developed to address cyber issues. This section presents a subset of those capabilities in the areas of cyberspace, cyber power, cyber strategy, and institutional factors.

Cyberspace.

In the area of data, we currently have some limited ability to collect real-world cyberspace information. For example, firms such as Gartner, Juniper, Symantec, and IBM extrapolate from samples to estimate the amount of "noise" (e.g., spam) that is infecting the real world. In addition, they provide some limited data characterizing the effectiveness of malware (e.g., DDoS attacks, worms, and viruses).

There are some limited mathematical theories that enable analysts to evaluate the performance of networks. As an illustration, techniques such as percolation theory enable one to evaluate the robustness of a network.[5]

There are also a variety of emerging tools that enable analysts to assess key issues in cyberspace. As a foundation for those tools, operations analysts have historically developed a deep understanding of the nature of the problem by analyzing real operations. In the case of cyber attacks, a representative set of real operations includes the following: Domain Name Server (DNS)-based "pharming attacks" to compromise the DNS server (e.g., redirect the user to a spoofed site or untrusted proxy); email-based "Phishing attacks," in which the phisher might send spam or a targeted email with bait; and deceptive download attacks, in which the adversary piggybacks on other software, posts software on a web site, or corrupts a trusted site.

Similarly, a great deal of useful operational knowledge can derive from key conferences. A representative event is the yearly DEFCON, which bills itself as "the largest underground hacker convention in the world." To suggest its focus, DEFCON has addressed the following issues during 2006 to 2008. In 2006, it focused on "owning" an organization through the BlackBerry and dramatically increasing the "attack surface" through the proliferation of wireless devices (e.g., WiFi) and the transition to IPv6. In 2007, the focus was placed on identity theft. In 2008, the emphasis included exploiting social software, social networks, and hacking opportunities provided by increasing the use of wireless connectivity.[6]

Building on these sources of operational data, there are several modeling and simulation (M&S) tools that the community is employing to address

computer science and communications issues. Perhaps the best known simulation is OPNET, which is widely employed to address network architectural issues.[7] However, OPNET and similar tools contain no description of potential vulnerabilities, such as adversary actions, malicious software, or insider threats. A theoretical prediction of the effects of network degradation can be obtained using OPNET (e.g., by the loss of a particular router or host); however, this is not a simulation of an actual threat.

To provide a more controlled environment for analysis, several test beds are emerging. As one example, the iCollege at National Defense University (NDU) has an Information Assurance (IA) Lab. The IA Lab offers detailed opportunities for non-experts to implant malicious code in software applications and operating systems within closed nets using openly available hacking tools.[8] Similarly, the Department of Energy's Pacific Northwest Laboratory is developing a test bed to explore and evaluate alternative cyber-deception strategies.[9] At the other end of the spectrum, the National Research Laboratory (NRL) has developed a Global Information Grid (GIG) Test bed to explore the myriad system-of-systems issues associated with linking new systems and networks.[10]

Cyber Power.

Our primary assessment tools for cyber power deal with the impact of changes in cyberspace on the military and informational levers of national power. In the military domain, interesting tools are emerging in live-virtual-constructive (LVC) simulations. For example, in assessments of air-to-air combat, insights have been derived from the live AIMVAL-

ACEVAL experiments, virtual experiments in the former McDonnell Air Combat Simulator (MACS), and constructive experiments using tools such as TAC BRAWLER and EASDSIM. These studies[11] have enabled researchers to determine that the advantage of a digital link to an airborne interceptor enhances his or her loss-exchange-ratio by approximately 2.5 percent. However, at present, it is not feasible to generate comparable "rules of thumb" for more complex aspects of contemporary warfare (e.g., air-land battle in complex terrain).

More recently, the Information Operations (IO) Joint Munitions Effectiveness Manual (JMEM) is developing frameworks and tools to address the various pillars of IO. These include computer network operations (subsuming Computer Network Attack [CNA], computer network defense, and computer network exploitation), psychological operations (PSYOP), electronic warfare (EW), operations security, and military deception. As an illustration, JMEM is developing a CNA risk-and-effectiveness analyzer (C-REA). This tool uses the effects and response analysis module (ERAM) as its core with interfaces tailored for planners.

In the area of live simulation, the IO range is emerging, with its hub at Cyber Command (CYBERCOM). This links together a variety of existing ranges (e.g., China Lake and Huntsville) to evaluate the use of CNA or EW techniques. Ultimately, the objective is to expand the IO range to evaluate all of the five pillars of IO. However, it is not clear how the existing IO range will evolve to address these other pillars. In addition, DARPA is in the process of developing a national cyber range.

In the informational domain, techniques are emerging to address media effects. One of the major areas of

interest for the PSYOP community is to evaluate the effects of media on culture and opinion. To illustrate this interest, there are several tools that have been developed and employed. These include the synthetic environments for analysis and simulation (SEAS), an agent-based model that has been developed by Simulex.[12] JFCOM employed SEAS in Afghanistan to support assessments of the extent to which media broadcasts affected the attitudes of the target population. Similarly, Oak Ridge National Laboratory (ORNL) has developed a tool known as Cultural and Media Influences on Opinion (CAMIO).[13] This tool uses an agent-based approach to assess the opinions of a group and how these opinions can be influenced over time. Representative issues of interest include how small groups of acquaintances form from larger populations and change over time. Furthermore, the IO JMEM has developed effectiveness of psychological influence (EPIC) to support the planning of PSYOP groups in developing and delivering messages.[14] However, in each of these examples, there has not been a rigorous verification and validation (V&V) process.

Looking to the future, there is interest in applying massively multiplayer online games (MMOGs) to informational issues. MMOGs offer a self-organizing environment for strategic communication or social networking that can potentially engage very large populations. A representative MMOG is Second Life. Since it offers the possibility of collecting substantial amounts of socio-behavior data, it has the potential to acquire and analyze tacit knowledge and cultural preferences.

Cyber Strategy.

To support cyber strategy assessments, four key initiatives are being pursued. These include exercises, lessons learned from the real world, new assessment methodologies, and societal models.

Over the last 3 years, the Department of Homeland Security (DHS) has conducted three Cyber Storm national cyber exercises. There is general agreement that these exercises have served to raise awareness of the cyber threat posed to critical infrastructures. However, there is concern that no systematic process exists to transform "lessons recorded" into "lessons learned."

As noted above, operations analysts have been successful when they have effectively derived lessons learned from real-world events. In the area of cyber attack, a substantial amount has been learned from the recent cyber attacks on Estonia and Georgia. In the case of Estonia, an extensive DDoS effectively denied citizens access to key Government sites, financial locations, and the media.[15] In response, Estonia has implemented a NATO Cooperative Cyber Defence Centre of Excellence (CCD COE) to support the planning and response to such attacks. More recently, Russia apparently employed a cyber attack as a precursor to their invasion of Georgia. Although details are sketchy, details are beginning to emerge on the dynamics of that attack.[16]

In response to a recent tasking by STRATCOM, a new methodology and associated tools are emerging to address tailored deterrence issues. The Deterrence Analysis and Planning Support Environment (DAPSE) is a process that is also instantiated in a web application. As part of that process, they have developed a typology (consistent with various social science disci-

plines) to characterize the information needed for understanding adversaries and other actors of interest. In addition, they have identified a preliminary set of applicable M&S and developed a decision deterrent calculus (DDC) matrix. The DDC matrix identifies perceived feasible/acceptable options by adversaries, potential U.S. options, and the impact of the result on other actors of interest.[17]

Several organizations are in the process of creating and refining societal simulations. As an example, the Systems Architecture Laboratory at GMU has developed a multi-modeling facility. As an element of this tool kit, it uses colored petri nets to create executable models to assess the effect of alternative DIME options on PMESII effects. They attempt to heuristically determine the course of action that maximizes the achievement of desired effects as a function of time.

Furthermore, DARPA's conflict modeling, planning, and outcomes experimentation (COMPOEX) program is developing decision aids to support leaders in designing and conducting future coalition-oriented, multiagency, intervention campaigns employing unified actions, or a whole of government approach to operations.[18] COMPOEX generates a distribution of "plausible outcomes" rather than precise predictions. COMPOEX's components include:

- Conflict Space Tool: This provides leaders and staff with the ability to explore and map sources of instability, relationships, and centers of power to develop their theory of conflict.
- Campaign Planning Tool: A framework to develop, visualize, and manage a comprehensive campaign plan in a complex environment.
- Family of Models: These are instantiated for the current area of responsibility (AoR), based

largely on systems dynamics models.[19] Additional models are being developed to more accurately represent the operational environment for other AoRs.

- Option Exploration Tool: This enables a staff to explore a multiple series of actions in different environments to see the range of possible outcomes in all environments.

However, there are substantial challenges in performing V&V of these tools and transitioning them to operational users.

Institutional Factors.

In the area of institutional factors, primary emphasis has been placed on the development of legal tools and critical infrastructure protection (CIP) tools. In the legal domain, a major challenge is to characterize rapidly whether a cyber attack is an act of war. Michael N. Schmitt of Durham University has developed a framework to address that issue.[20] The framework systematically considers seven factors which are: severity, immediacy, directness, invasiveness, measurability, presumptive legitimacy, and responsibility. Once one has assessed each of those factors, multi-attribute utility theory can be employed to weigh each of these factors and come to a determination.

To facilitate legal decisions, a dual-decision tree system has been recommended.[21] The first of these trees is a computer-based tree to assemble key data prior to an actual attack (e.g., primary and secondary levels to characterize international law, constitutional law, executive actions [directives], legislative actions [statutes], or judicial rulings [cases]). This tree is complemented by a human-based tree to support

developing a legal brief in near real time, drawing on four levels of abstraction (e.g., citation, precis, excerpt, or full document).[22] Similarly, the system enriches knowledge of legal issues by conducting legal analyses of real-world events (e.g., the NATO CCD COE legal assessment of the Georgian attack).[23]

In the area of CIP, several innovative tools are evolving. The iCollege, NDU, is refining a Supervisory Control and Data Acquisition (SCADA) Laboratory that is designed to explore the vulnerabilities of control systems for electric power generation and other critical infrastructures (e.g., chemical plants or water treatment). Alternatively, under the aegis of DHS, the National Infrastructure Simulation and Analysis Center (NISAC) is developing and applying system dynamics models to assess cascading effects among critical infrastructures. They are taking advantage of the M&S skills resident in Los Alamos National Laboratory and Sandia National Laboratory (LANL/SNL). Furthermore, the U.S. Cyber Consequences Unit (US-CCU) is developing and applying risk assessment tools to critical infrastructure issues. For example, USCCU developed a model of value creation and destruction to evaluate the economic consequences of cyber attacks. In addition, it has published a risk assessment check list for critical infrastructures.[24]

NEEDED CYBER ASSESSMENT CAPABILITIES

This section briefly summarizes some of the major needs for cyber methods, tools, data, and services. In the area of cyberspace, there is a need to institute a more systematic and comprehensive process by which data are collected, organized, and V&V'ed. In addition, there is a need to go beyond OPNET to create

a large-scale, high-fidelity model, which can realistically model a set of malicious activities against a real-world network.

In the area of cyber power, there is the need to develop and apply risk assessment tools that enable one to estimate the probability and consequence of a cyber attack. The results can help one prioritize the allocation of resources to support defense of these resources. Second, there is a need to develop additional functional relationships, linking changes in cyberspace to consequences in cyber power. Senior decisionmakers need access to "rules of thumb" that will enable them to assess the impact of changes in cyberspace (e.g., bandwidth, accessibility) to changes in the instruments of power (e.g., the ability to perform diplomatic, informational, military, and economic activities). At this stage, a few limiting cases exist for relatively simple operations (e.g., limited air-to-air combat). A broad set of studies should be performed that are analogous to the activities that were performed (more narrowly) by the Office of Force Transformation.

In the area of cyber strategy, there is the need to extend and apply recently developed methods. In the area of exercises, it is important to go beyond consciousness raising to the development of a process to mitigate identified cyberspace shortfalls. In addition, the method developed by DAPSE may be useful when considering potential options to deter attacks in cyberspace. Furthermore, a great deal of work is required to develop needed cyber strategy tools. First, at the MORS workshop on deterrence,[25] several variants on game theory were identified and discussed to explore contemporary variants on deterrence. It might be useful to develop game-theoretic tools for analyzing potential cyber attacks. Second, most war games

lack the fidelity and granularity to explore alternative IO attacks. Activities are underway to identify "best of breed" war games and to identify needed capabilities.[26] Third, there is a need for tools that will support integration across kinetic and nonkinetic attacks. Currently several shortfalls limit the ability to accomplish this objective. For example, in the nonkinetic domain, the IO JMEM activity is developing tools to assess the impact of the individual IO pillars on mission effectiveness. However, there is the need for a capstone tool that will enable tradeoffs across the individual pillars. In addition, there is no tool with adequate scope and granularity to support the formulation and assessment of courses of action that subsume a mix of kinetic and nonkinetic actions.

Fourth, human, social, and cultural behavior (HSCB) will have a major impact on individuals and organizations that are subject to cyber attack. As an example, many of the most successful attacks have cleverly employed social engineering features. Thus, there is a need for a HSCB Modeling Test Bed to evaluate V&V candidate social sciences theories and tools to instantiate those tools. Finally, in the area of societal tools, the system is currently in a very primitive stage. Additional work is required to improve the constituent elements of these tools (e.g., underlying models of economic, political, or social behavior) and their interaction. In particular, there is a need for greater transparency in identifying and tracing cause-and-effect relationships. The HSCB Modeling Test Bed might be a useful mechanism to mature these tools and to perform systematic V&V of them.

Many of the creators of cyber tools lack the knowledge to apply them efficiently and effectively. One of the issues is the large number of variables associated with those tools. To begin to address this issue,

two courses of action are necessary. First, flexible, adaptive, and responsive (FAR) exploratory analyses should be performed that develop response surfaces that characterize these tools.[27] Second, innovative experimental designs are required (e.g., exploitation of the insights developed by NPS' SEED Center for Data Farming).[28]

It must be emphasized that virtually none of the tools cited above have undergone rigorous V&V. Even when some of the key V&V tests are performed, they are rarely documented in a clear, transparent fashion that enables senior decisionmakers to make reasoned judgments about the application of these tools to specific issues. The HSCB Modeling Test Bed may prove to be a useful laboratory for conducting these V&V activities.

In the area of institutional factors, there is a need for improved tools to support governance, legal assessments, and CIP issues. Historically, the United States has played a major role in governing cyberspace. However, given the global nature of the Internet, many nations have agitated for a larger role in the governance process. Currently, there is a lack of adequate tools that would enable the formulation and evaluation of key governance issues. As noted above, a proposal has been raised to assemble relevant cyber legal information into dual-decision trees that would enable lawyers to have easy access to key data. An effort is needed to design and instantiate such tools. Finally, as noted above, a number of institutions have been designing and applying a variety of tools to support the assessment of attacks against critical infrastructures (including cascading effects). At this stage, rigorous V&V efforts are required for those tools so that a senior decisionmaker will be able to assign an appropriate level of confidence against those results.

CONCLUSION

This chapter has established a framework for evaluating cyber issues; identified key policy issues that warrant analysis; identified potential MoMs for cyber analysis; characterized the state-of-the-art in performing cyber analyses; and identified key areas that warrant additional attention. As Figure 9-2 suggests, the analysis community's ability to assess cyber issues is uneven. It tends to be strongest in assessing cyberspace issues (in which computer science and electrical engineering issues predominate) and weakest in assessing cyber strategy and institutional factors.

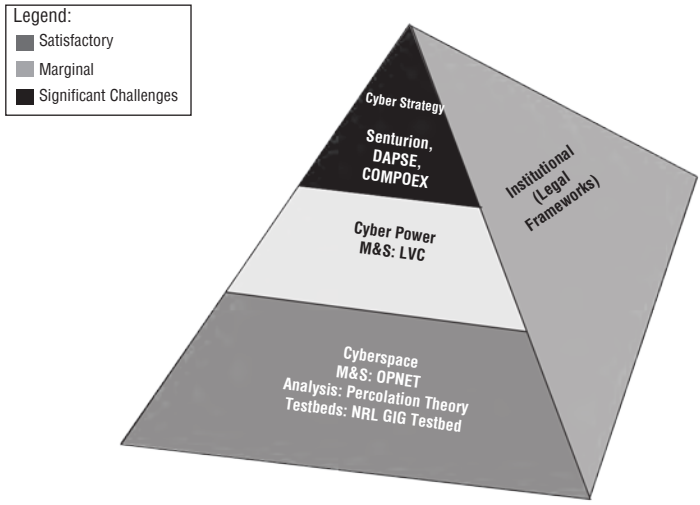

Figure 9-2. Assessment of Existing Cyber Tools.

Overall, there will need to be a substantial infusion of resources to develop the methods, tools, data, and intellectual capital needed to address the concerns of

senior decisionmakers. However, given the limited resources that are available, it is suggested that highest priority be given to the following activities. First, although there are interesting individual tools to support the analyses of cyberspace, there is a need for an integrated suite of analysis tools. At the foundation of these tools, actions must be taken to enhance data collection.

Second, the analysis community requires better tools to assess the impact of advances in cyberspace on broader military and informational effectiveness (e.g., land combat in complex terrain). Similarly, tools are necessary to assess the risks that ensue if an adversary is able to compromise net-centric operations. However, there is extensive uncertainty about many of the key parameters that are introduced in the IO JMEMs frameworks (e.g., many of the parameters that characterize the probability of arrival and the probability of damage). This suggests that exploratory analysis techniques be used with these and comparable frameworks, to deal with the massive uncertainty in key parameters. Furthermore, since human responses to cyber actions are of great importance, there is a need for a HSCB Modeling Test Bed to enhance our ability to enhance HSCB modeling.

Third, there is a need to develop tools that explore the impact of alternative mixes of offensive and defensive actions on deterrence strategies. This is extremely important because of recent proposals that have emerged from the White House.[29] Although emerging societal tools are promising, it is vital that they be subject to rigorous validation, verification, and accreditation (VV&A) activities. Finally, there have been a number of studies of cyber attacks against nation-states (e.g., Estonia and Georgia). However, there is a

need for a more rigorous assessment to develop and implement lessons learned.

Lastly, several efforts are underway to assess the effectiveness and impact of attacking critical infrastructures. However, if these tools are going to be valuable to senior decisionmakers, it is important that they be subject to rigorous VV&A efforts.

ENDNOTES – CHAPTER 9

1. Cyberspace is defined as: "An operational domain whose distinctive and unique character is framed by the use of electronics and the electromagnetic spectrum to create, store, modify, exchange, and exploit information via interconnected and Internet information systems and their associated infrastructures."

2. Cyber power is defined as "the ability to use cyberspace to create advantages and influence events in the other operational environments and across the instruments of power."

3. Cyber strategy 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. John Soat, "IT Confidential: Is There Anything That Can Be Done About E-mail?" *Information Week*, February 17, 2007.

5. Ira Kohlberg, "Percolation Theory of Coupled Infrastructures," 2007 Homeland Security Symposium, "Cascading Infrastructure Failures: Avoidance and Response," National Academies of Sciences, Washington, DC, May 2007.

6. Linton Wells III, "Understanding Cyber Attacks: Lessons from DEFCON, Georgia and IRMC," CTNSP, NDU, September 22, 2008.

7. Emad Aboelela, "Network Simulation Experiments Manual," Burlington, MA: Morgan Kaufmann, 3rd Ed., June 2003.

8. Wells.

9. "Laboratory for Cyber Deception," Pacific Northwest National Laboratory, Phoenix Challenge 2008, Monterey, CA: Naval Postgraduate School, April 2008, available from *www.pnl.gov/*.

10. Stuart Starr *et al*., "Concept for an Enterprise Wide, System Engineering Collaborative Engineering Environment," NDIA Systems Engineering Conference, San Diego, CA, October 2006.

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

12. Synthetic Environments for Analysis and Simulation (SEAS), available from *www.simulexinc.com/products/case-studies/*.

13. Cultural and Media Influences on Opinion (CAMIO), available from *www.ioc.ornl.gov/overviews/shtml*.

14. IO Working Group PSYOP Functional Area Working Group, "Where PSYOP JMEM Fits into the PSYOP Planning and Joint Targeting Processes," FA9200-06-C-0024, July 22, 2008.

15. Joshua Davis, "Hackers Take Down the Most Wired Country in Europe," *Wired Magazine*, Issue 15, No. 09, August 21, 2007.

16. The following vignette suggests the ease with which a cyber attack can be launched: Evegny Morozov, founder of the news aggregator Polymeme, categorized his participation in the Georgian cyber attack. "In less than half an hour, drawing on tools available online and a short program he wrote in a Microsoft document, he developed two options to promote DDoS attacks. He then went to a website named 'StopGeorgia,' which claimed to be 'by and for the 'Russian hack underground'." This site provided target lists of websites, with updates as to whether or not they'd already been taken down, and downloadable code to customize attack options that could be launched with a single click on a button labeled "Start Flood." See Wells.

17. Strategic Multi-Layer Analysis Team, Nancy Chesser, ed., "Deterrence in the 21st Century: An Effects-Based Approach in an

Interconnected World, Volume I," sponsored by USSTRATCOM Global Innovation and Strategy Center, October 1, 2007.

18. Ed Waltz, "Situation Analysis and Collaborative Planning for Complex Operations," 13th International Command and Control Research and Technology Symposium (ICCRTS), Bellevue, WA, June 2008.

19. Corey Lofdahl, "Synthesizing Information for Senior Policy Makers Using Simulations," 13th ICCRTS, Bellevue, WA, June 2008.

20. Michael N. Schmitt, "*Bellum Americanum:* The US View of Twenty-first Century War and its Possible Implications for the Law of Armed Conflict," *Michigan Journal of International Law*, Vol. 19, No. 4, 1998, pp. 1051-1090.

21. See Thomas C. Wingfield *et al.*, "Optimizing Lawful Responses to Cyber Intrusions," Paper No. 290, 10th ICCRTS, McLean, VA, June 2005.

22. *Ibid.*

23. Eneken Tikk *et al.*, "Cyber Attacks Against Georgia: Legal Lessons Identified," NATO Cooperative Cyber Defence of Excellence, Tallinn, Estonia, August 2008.

24. John Bumgarner and Scott Borg, "The US-CCU Cyber-Security Check List," Final Version, 2007.

25. "Analytic Tools for Deterrence & Policy Assessment," JHU/APL, Laurel, MD, February 5-7, 2008, MORS, available from *www.mors.org*.

26. Phoenix Challenge Workshop on Information Operations and Wargames, SPAWAR, Charleston, SC, October 28-30, 2008.

27. Thomas L. Allen *et al.*, "Foundation for an Analysis Modeling and Simulation Business Plan," IDA Paper P-4178, December 2007.

28. SEED Center for Data Farming, available from *harvest.nps.edu*.

29. National Security Presidential Directive (NSPD) 54, "On Computer Network Monitoring and Cyber Security," January 8, 2008.

APPENDIX I

ABBREVIATIONS AND ACRONYMS

Abbreviation/ Acronym	Meaning
AoR	Area of Responsibility
CCDCOE	Cooperative Cyber Defense Centre of Excellence
CAMIO	Cultural and Media Influences on Opinion
CIP	Critical Infrastructure Protection
CNA	Computer Network Attack
COMPOEX	Conflict Modeling, Planning & Outcomes Experimentation
C-REA	CNA Risk and Effectiveness Analyzer
DAPSE	Deterrence Analysis and Planning Support Environment
DARPA	Defense Advance Research Project Agency
DDC	Decision Deterrent Calculus
DDoS	Distributed Denial of Service
DHS	Department of Homeland Security
DIME	Diplomatic, Informational, Military, Economic
DNS	Domain Name Server
EADSIM	Extended Air Defense Simulation
EPIC	Effectiveness of Psychological Influence
ERAM	Effects and Response Analysis Module
EW	Electronic Warfare
FAR	Flexible, Adaptable, Robust
GMU	George Mason University
HSCB	Human, Social, Cultural Behavior
IA	Information Assurance
IO	Information Operations
IPv6	Internet Protocol version 6
IRMC	Information Resource Management College
JFCOM	Joint Forces Command

JMEM	Joint Munitions Effectiveness Manual
LANL	Los Alamos National Laboratory
LVC	Live-Virtual-Constructive
M&S	Modeling and Simulation
MACS	McDonnell Air Combat Simulator
MANET	Mobile, Ad hoc, Network
MMOGs	Massively Multiplayer Online Games
MoEs	Measures of Effectiveness
MoEEs	Measures of Entity Empowerment
MoFPs	Measures of Functional Performance
MoMs	Measures of Merit
MoPs	Measures of Performance
MORS	Military Operations Research Society
MTB	Modeling Test Bed
NDU	National Defense University
NISAC	National Infrastructure Simulation and Analysis Center
NPS	Naval Postgraduate School
NRL	Naval Research Laboratory
ORNL	Oak Ridge National Laboratory
PMESII	Political, Military, Economic, Social, Information, and Infrastructure
PSYOP	Psychological Operations
SCADA	Supervisory Control and Data Administration
SEAS	Synthetic Environment for Analysis and Simulation
SEED	Simulation, Experimentation and Efficient Designs
SNL	Sandia National Laboratory
STRATCOM	Strategic Command
US-CCU	U.S. Cyber Consequences Unit
V&V	Verification and Validation
VV&A	Verification, Validation, and Accreditation

ABOUT THE CONTRIBUTORS

ADAM BOSSLER is an assistant professor of justice studies at Georgia Southern University. His research interests include testing criminological theories that have received little empirical testing, such as control balance theory, examining the application of traditional criminological theories to cybercrime for both the offender and the victim, and evaluating policies and programs aimed at reducing youth violence. Dr. Bossler holds a Ph.D. in criminology and criminal justice from the University of Missouri - St. Louis.

VINCENT BOUDREAU is a professor of political science at the City College of New York and at the CUNY Graduate and University Center. He is currently the director of the Colin Powell Center for Leadership and Service at CCNY. Dr. Boudreau is a specialist in the politics of social movements, particularly in Southeast Asia, and his latest book is *Resisting Dictatorship: Repression and Protest in Southeast Asia* (Cambridge University Press). He also conducts research and writes on repression, government transitions to democracy, and collective violence. At CCNY Dr. Boudreau has served as director of the M.A. Program in International Relations, chair of the Department of Political Science, director of the International Studies Program, and deputy dean of the Division of Social Science. In addition to his academic work, he has undertaken projects with ActionAid Asia, Jubilee South Asia, and The Philippine Rural Reconstruction Movement, and has consulted for Oxfam Asia, Action of Economic Reform (Philippines), and Freedom House. Dr. Boudreau holds a Ph.D. from Cornell University.

GEORGE W. BURRUSS is an assistant professor in the Center for the Study of Crime, Delinquency and Corrections, Southern Illinois University, Carbondale. He received his Ph.D. in criminology and criminal justice from the University of Missouri, St. Louis. He does research on criminal justice organizations, including juvenile courts and the police. He has published articles in *Justice Quarterly*, *Policing*, and *Journal of Criminal Justice.*

MELISSA DARK is a professor in computer technology and associate dean in the College of Technology at Purdue. Ms. Dark specializes in educational measurement and evaluation; her measurement and evaluation expertise has been applied to information security for the development of a hacker aptitude test for the Air Force, evaluation models for software security curriculum exercises, and evaluation theory and practice in security education. She has led faculty development projects in technology education and information security education aimed at increasing the knowledge and skills of secondary and post-secondary educators throughout the United States, and has been active in helping define the information assurance discipline. In addition to focusing on educational interventions in information security, Ms. Dark works in information security policy and economics, investigating the impact of both on the socio-technical interface that is at the core of our challenges in information security.

ABHRAJIT GHOSH is a director at Telcordia Technologies. He has extensive research and development experience in the area of cyber security, including network intrusion detection, policy-based network

security management, network attack traceback, and secure communication architectures. He is currently leading research activities at Telcordia, addressing ISP level network threat monitoring issues.

JOSHUA GRUENSPECHT is the cyber security fellow at the Center for Democracy and Technology, where he specializes in issues at the intersection of law, privacy norms, and technology. He has also worked on cyber security issues at the Senate Homeland Security Government Affairs Committee, where he was the lead analyst on the Comprehensive National Cyber Security Initiative and drafted legislation to protect the national information infrastructure. Mr. Gruenspecht was also an analyst for computer-related crimes at the Department of Justice. Previously, he was an engineer designing computer network exploitation, network security, and device security solutions, first within the federal government and then with BBN Technologies. Mr. Gruenspecht earned a B.S. in computer science and English at Yale University and a J.D. at Harvard Law School.

THOMAS HOLT is an assistant professor in the School of Criminal Justice at Michigan State University specializing in computer crime, cybercrime, and technology. His research focuses on computer hacking, malware, and the role that technology and the Internet play in facilitating all manner of crime and deviance. Dr. Holt has been published in a variety of academic journals, including *Crime and Delinquency*, *Deviant Behavior,* and the *Journal of Criminal Justice*, and has presented his work at various computer security and criminology conferences. He is the project lead for the Spartan Devils Honeynet Project, which is

a joint project of Michigan State University, Arizona State University, and private industry. In addition, he is a member of the editorial board of the International Journal of Cyber Criminology.

LOUIS H. JORDAN, JR., is the Deputy Director of the Strategic Studies Institute, U.S. Army War College, Carlisle Barracks, PA. His assignments include Flight Operations Officer, Company Executive Officer, Asst S3 Air, Asst S3 and Brigade Adjutant in the 42d Infantry (RAINBOW) Division New York Army National Guard. He served as Battalion S3 for 3-140 Aviation (CH-47D), 66th Aviation Brigade, I Corps in Stockton, California. Colonel Jordan has served at the National Guard Bureau as Deputy Division Chief for the Aviation and Safety Division. After serving at the national level, Colonel Jordan commanded the Aviation Support Battalion, Western Army National Guard Aviation Training Site in Marana, Arizona. In 2005, he was selected to be the Brigade Commander for the Western ARNG Aviation Training Site. In 2008, he was selected to command Joint Task Force Raven, the aviation task force for Operation Jump Start along the southwest border in Arizona. Colonel Jordan holds a B.A. in sociology from Fordham University, a master's in strategic studies from the U.S. Army War College, and certification in Strategic Planning from the American Management Association.

DEBORAH WILSON KEELING is currently Chair of the Department of Justice Administration, University of Louisville, KY, and is responsible for academic programs as well as the Southern Police Institute and National Crime Prevention Institute. She has conducted numerous applied research projects for local, state,

and federal criminal justice agencies. Dr. Keeling has organized police training programs in the People's Republic of China, Hungary, Romania, and the Republic of Slovakia. She holds a Ph.D. in sociology from Purdue University.

MAX KILGER is a behavioral profiler for the Honeynet Project and contributes additional efforts in the areas of statistical and data analysis. He has written and co-authored research articles and book chapters on the areas of influence in decisionmaking, the interaction of people with technology, the motivations of malicious online actors, and understanding the changing social structure of the computer hacking community. He was the lead author for the Profiling chapter of the Honeynet Project's book, *Know Your Enemy* (2nd Ed.), which serves as a reference guide for information security professionals in government, military, and private sector organizations. Dr. Kilger also co-authored a chapter examining the vulnerabilities and risks of a cyber attack on the U.S. national electrical grid. He recently published a book chapter on social dynamics and the future of technology-driven crime. His most recent publications include two chapters dealing with cyber profiling for Reverse Deception: Organized Cyber Threat Counter-Exploitation (McGraw-Hill). Dr. Kilger was a member of the National Academy of Engineering's Combating Terrorism Committee, which was charged with recommending counterterrorism methodologies to the Congress and relevant federal agencies. He is a frequent national and international speaker to law enforcement, the intelligence community, and military commands, as well as information security forums. Dr. Kilger holds a Ph.D. from Stanford University in social psychology.

MICHAEL LOSAVIO teaches in the Department of Justice Administration and the Department of Computer Engineering and Computer Science at the University of Louisville on issues of law, ethics and society, and information security in the computer engineering and justice administration disciplines. He also works on curriculum development on the use and impact of information and computing systems in a variety of disciplines. Mr. Losavio holds a J.D. in law and a B.S. in mathematics from Louisiana State University.

TAREK SAADAWI is a professor and Director of the Center for Information Networking and Telecommunications (CINT), City College, the City University of New York. His current research interests are telecommunications networks, high-speed networks, multimedia networks, ad hoc mobile wireless networks, and secure communications. He has published extensively in the area of telecommunications and information networks. Dr Saadawi has been on the Consortium Management Committee (CMC) for the Army Research Lab Consortium on Telecommunications (known as Collaborative Technology Alliances on Communications and Networks, CTA-C&N), from 2001 to 2009. Dr. Saadawi is a co-author of the book, *Fundamentals of Telecommunication Networks* (John Wiley & Sons, Inc., 1994), which has been translated into Chinese. He is guest co-editor of the Special Issue on "Mobile Ad-Hoc Wireless Networks," *Journal of Advanced Research*, Vol. 2, Issue 3, July 2011, pp. 195-280. He has been the lead author of the Egypt Telecommunications Infrastructure Master Plan, covering the fiber network, IP/ATM, DSL and the wireless local loop under a project funded by the U.S. Agency for International Development. He has joined the U.S. De-

partment of Commerce delegation to the Government of Algeria addressing rural communications. He is a former Chairman of IEEE Computer Society of New York City (1986-87). Dr. Saawadi holds a B.Sc. and an M.Sc. from Cairo University, Egypt, and a Ph.D. from the University of Maryland, College Park.

J. EAGLE SHUTT is a former prosecutor and public defender and currently is an assistant professor at the Department of Justice Administration, University of Louisville, KY. He also serves as a JAG officer in the South Carolina National Guard. His research interests include biosocial criminology, culture, public policy, and law. Dr. Shutt holds a JD, an MCJ, and a PhD.

STUART STARR is the president of the Barcroft Research Institute (BRI). In that capacity, he consults to government and industry in the areas of command and control assessment, modeling and simulation (M&S), and operations analysis. Prior to founding BRI, he was Director of Plans, MITRE; Assistant Vice President, C2 and Systems Assessment, M/A-COM Government Systems; Director, Long Range Planning and Systems Evaluation, OASD(C3I), OSD, where he was a member of the Senior Executive Service (SES); and Senior Project Leader, Institute for Defense Analyses (IDA). He was a Fellow at MIT's Seminar XXI. Dr. Starr is a Fellow, Military Operations Research Society (MORS); Associate Fellow, AIAA; Member of the Army Science Board; a Senior Research Fellow at the Center for Technology and National Security Policy (CTNSP), National Defense University (NDU); and a frequent participant in Blue Ribbon Panels of NATO, the National Research Council, and the Director, Net Assessment, OSD. Dr. Starr holds a Ph.D. in electrical engineering from the University of Illinois.

U.S. ARMY WAR COLLEGE

Major General Anthony A. Cucolo III
Commandant

*****

STRATEGIC STUDIES INSTITUTE
and
U.S. ARMY WAR COLLEGE PRESS

Director
Professor Douglas C. Lovelace, Jr.

Director of Research
Dr. Steven K. Metz

Editors
Dr. Tarek Saadawi
Colonel Louis H. Jordan, Jr.
Dr. Vincent Boudreau

Editor for Production
Dr. James G. Pierce

Publications Assistant
Ms. Rita A. Rummel

*****

Composition
Mrs. Jennifer E. Nevil

U.S. ARMY WAR COLLEGE

SSI

STRATEGIC STUDIES INSTITUTE

ISBN 1-58487-571-2

9 781584 875710

90000>

This Publication

SSI Website

USAWC Website