IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12707

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

Monitoring-Based Coordinated Defense through the Lens of the Coordination Theory

Shuyuan Mary Ho, School of Information Studies, Syracuse University, USA, smho@syr.edu

U. Yeliz Ereryel, School of Information Studies, Syracuse University, USA, Yliz2002@alum.syr.edu.edu

ABSTRACT
Coordinated defense in the cyber warfare has emerged to protect information assets through the use of technologies, policy and the best management practices to defend against coordinated attacks. However, combining massive security technologies, policies, procedures and security staff does not guarantee effectiveness of defense. Without a well-defined and structured element of coordination, an organization or a nation can not stand firm during coordinated attacks. This paper conceptualizes implicit coordination elements in the realm of monitoring-based coordinated defense, which is built upon the Coordination Theory. The framework is designed to collect and correlate distributed events from the components specified in the Coordination Theory for centralized monitoring mechanism that would result in better group decision-making and maximize chances of success in defending coordinated attacks. This paper contributes to the IT security and defense society by providing a systematic way of approaching coordinated defense; it also benefits the IT security and defense research by introducing the concept of coordinated defense, about which there is little research. Future studies in this area may include empirical analysis of the existing coordinated defense, such as incident response reporting systems against attacks, from the coordination theory perspective.

INTRODUCTION
While elements such as technology, management, policy and procedure are significant requirements for solid coordinated defense against the coordinated attacks, they are not sufficient; human factors have greatly threatened and caused vulnerability to the chains of defense (*C4ISR* Joint Chiefs of Staff 2000, p. 5). Threats from insiders, for instance, cause this chain of defense to be vulnerable (*C4ISR* Joint Chiefs of Staff, 1999, DelZoppo et al, 2004; Park & Ho, 2004). One of the methods in detecting insider threats is to utilize peer employees as network sensors in the workplace to detect malicious acts. In this, coordination becomes critical, as it serves two major functions: explicitly, coordination links humans, technology, management, policies and procedures together for a stronger security defense; implicitly, coordination helps detect anomalies within human network in the workplace. This paper uses the Coordination Theory to understand the human coordination in the coordinated defense efforts, which includes the technology, management and security policies and procedures.

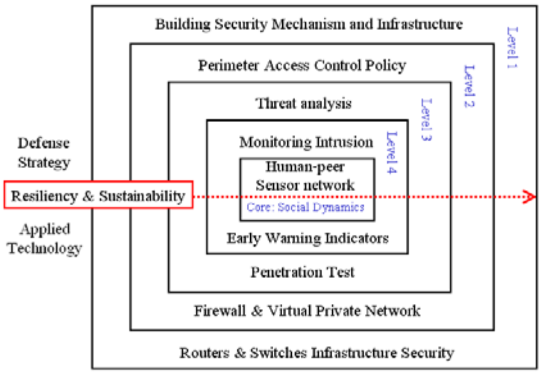
COORDINATED ATTACK AND COORDINATED DEFENSE
In the battlefields, attack strategies have progressed from a single attack to sophisticated distributed coordinated attacks (Cohen, 1996). "Coordinated attack" is defined as "a carefully planned and executed offensive action in which the various elements of a command are employed in such a manner as to utilize their powers to the greatest advantage to the command as a whole" (DOD Joint Doctrine Division, 2005). The 911 tragedy in 2001 was a result of a coordinated attack (National Commission on Terrorist Attacks upon the United States, 2004); which is composed of well-planned and executed synchronous offensive actions. Similarly, coordinated attacks were found and reported in Ingushetia (Amnesty International, 2004) and Iraq (The Hindu, 2004; Taipei Times, 2005).

In the cyber warfare, coordinated attack strategies are massively used to confuse detectors and intrusion detection systems (Ning and Xu, 2004), decoy victims, and distract attention. Most importantly, coordinated attack is an art that combines a large variety of attack strategies to penetrate and collapse the infrastructure and systems of a site (Braynov and Jadliwala, 2003; Green, Marchette and Northcutt, 2000). Distributed Denial of Services (DDoS) or logic bombs are examples of techniques used to distract attention in the cyber warfare while "compromised insider" would weaken the coordination infrastructure and "Trojan attack" could subtly be launched to collapse the infrastructure.

The concept of coordinated defense (Noh and Gmytrasiewicz, 1999) in the cyber warfare has been emerged to protect information assets by combining the use of technologies, policy and best practices to defend against coordinated attacks. Coordinated defense has been a common practice in the military. The Marine Corps, for example, has the Joint Task Force Computer Network (MarAdmin, 1999) and the *C4ISR* (the command, control, communications, computers, intelligence, surveillance and reconnaissance) infrastructure has been developed and carried out by the DOD Joint Chiefs of Staff (*C4ISR* Joint Chiefs of Staff, 1999 & 2000) to guard information from coordinated cyber attacks. In other sectors such as the government, educational institutes and commercial enterprises, coordinated defense is commonly practiced by the building incident response teams against intended or unintended attacks (CMU SEI CERT®CC, 2002).

In order to better understand how to form coordinated defense, we need to first understand the rationale and philosophy of how a coordinated attack would be launched. Sun Tsu said, "If you know yourself but not the enemy, for every victory gained you will… suffer a defeat." "Knowing the enemy enables you to take the offensive, knowing yourself enables you to stand on the defensive," replied Chang in the Art of War (Giles, 1910). According to Sun Tsu's wisdom, knowing your enemy is the key step for avoiding fear and winning battles. The same principle applies in the cyber warfare domain. The attackers typically use more or less the following strategy; they first spy the site and find its vulnerabilities. Then, they find out and target most vulnerable points of a site and probe their accessibility. The vulnerability and accessibility mentioned above can be based on one or more of the security elements of technology, security policies and procedures or information use behaviors of individuals. Finally, the actual attack is launched to intrude and destroy the infrastructure and systems of a site. After the attack is mounted by an attacker, the attackers may cover up their identities and clear off their traces/logs before a severe inflicted damage given (NEWS development rationale slides, 2001). This type of attack strategy has been described in the information warfare literature (Henning, 1997; Libicki 1995) and would be used by both individual hackers as well as

Figure 1. Multi-layered defense mechanism



coordinated circle of attackers. For example, Paul R. Henning, in his "Air Force Information Warfare Doctrine," classified information warfare under counter-information and information assurance groups (Henning, 1997).

Having outlined the nature of coordinated attacks, let's talk about coordinated defense tools (Figure 1). Coordinated defense covers all aspects of defense including social and technical aspects. Building security mechanisms and infrastructure is the first step of this defense strategy. Secondly, a fundamental "deny all unless specified" access control security policy should be implemented. The "deny all" access control policies block out possible social engineering and probing attacks. The "unless specified" access rules at the perimeter firewall provide flexibility to conditionally control unauthorized access and prevent attacker's reconnaissance. Many technologies such as virtual private networks (VPN) and de-militarized zones are also examples of other access-related countermeasures that should be considered. Similarly, closing down unnecessary ports and services on the routers, switches and systems and enhancing the kernel operating systems are also countermeasures of the access control.

The third layer in the coordinated defense model would be to conduct infrastructure threat analysis and intrusion forecasts. These could be done by performing penetration tests to probe the operational processes as well as analysis of business management procedures for potential loopholes. These strategies enable a company to "see the self from the enemy's eyes[1]".

The forth layer in the coordinated defense model would be to monitor and detect intrusion. It is critical to sense and detect precursors in coordinated attacks so that further damages could be avoided. Sensor technology at infrastructure level such as network-based intrusion detection or systems level such as host-based intrusion detection are built to detect and monitor activities. Similarly, human physical activities could be monitored by camera. Furthermore, a more sophisticated detection of malicious anomalies centered as the kernel layer of defense could be assessed through co-workers. Peers serve as social sensors that monitor social activities within the corporate or organizations. At this step, anomalies in the behaviors of human subjects could indicate ill-natured intents and possibly lead to insider threats. Finally, an overarching layer of the defense emphasizes the resiliency and sustainability of the defense infrastructure, where the damage assessment and impact analysis lead to the rebuilding of recovery and response mechanism.

Coordinated efforts themselves are far superior to any of the elements of people, policy, management and technology that make up a coordinated defense. "How well coordinated the actions of a group of people" (Malone and Crowston, 1990) in addition to policy, management and technology becomes the determining factors of a successful battle both in physical and cyber space. "Good coordination is nearly invisible, and we… notice coordination most clearly when it is lacking" (Ibid, p. 357).

After explaining the elements of coordinated defense and giving examples of technologies and mechanism that can be used for each layer of the defense mechanism, we now will focus on understanding the concept of coordination in the realm of social networks. In addition, we will further extend the framework of the coordination to include other elements such as technology and management in a structured framework of coordinated defense through lense of Coordination Theory.

THEORETICAL FRAMEWORK

The theoretical framework of this study examines the implicit coordination concepts of monitoring-based coordinated defense, through the lens of the Coordination Theory developed by Thomas W. Malone and Kevin Crowston (Malone, 1989; 1990 & 1994), at the Center for Coordination Science of MIT. Coordination Theory proposes the identification and systematical analysis of a wide variety of dependencies and their associated coordination process and relevant organizational structures (Malone and Crowston, 1994). Its central concern is to identify and analyze specific coordination process and structure (Ibid, 110). In the following paragraphs, we will conceptually identify and analyze the coordination process through an example of a coordinated defense and we will model how monitoring capability in the coordination process emphasized by the Coordination Theory could enhance the coordinated defense.

Coordination is defined by Malone and Crowston (1994) as managing dependencies between activities. Good coordination is normally done harmoniously, unnoticeably and "invisibly." In the framework of the Coordination Theory, Malone and Crowston define components that are seen as dependencies between activities. Analyzing the defense activities in light of the Coordination Theory requires the analysis of security related technologies as well as behaviors, and the linkages between the two. The security architects should identify the strategic and task related goals in enabling the coordinated defense and subject matter experts (SMEs) should be assigned to each task within specific domain. *Goal selection* enables the identification of a hierarchy of tasks; in the *top-down goal decomposition*, tasks are decomposed to sub-tasks. *Bottom-up goal identification* occurs when the subject matter experts, rather than the security architects, manage task/sub-task dependencies. For example, a firewall system administrator, as a subject matter expert, who is assigned a task to secure the perimeter firewall, actually has a coordination role. The administrator first decomposes this task into sub-tasks and then works with other application system administrators to synchronize their tasks such as allowing or blocking certain traffic. If in this case, the system administrator purposefully allows certain traffic or opens unnecessary ports that are not designed or defined in the task assignment, this would create a security loophole and such incidents would be logged. This type of security loopholes can be eliminated through the use of the multi-layered defense mechanism mentioned earlier (Figure 1).

The analysis of task assignment will enable a security architect to estimate potential security loopholes and use various layers of the defense mechanism to create buffers against potential breaches of security. When the tasks are assigned to the subject matter experts, classified information would be involved in the process. Monitoring of the task assignments would enable the detection of whether the document classification level is changed and whether information is disclosed, copied or modified. Monitoring of shared resources such as data repositories is another component in this framework that provides traces of who accesses the data at what time, as well as which information at which classification level is being retrieved and operated on. To sum up, we believe that analyzing coordination mechanism such as shared resources, tasks, among others will provide the glue between the layers of the coordinated defense mechanism that we suggested in Figure 1.

Participatory design is another element in the coordination theory that contributes to the success of the coordinated attacks. In our previous example, we talked about the detection of loopholes. It is fairly easy to detect the firewall ports that ought to be open, but is closed. The system would give an alert, and the attempts of connection from other users or applications would be dropped. However, it is very difficult to detect the open firewall ports that ought to be blocked. One way to detect such unacceptable open ports on the firewall is that there would be either some attempts to talk to backdoor programs or illegitimate connections. The coordination loopholes can also be found when the firewall system administrator fails to *transfer* defined firewall access policy, as assigned tasks, to other subject matter experts, in this case, other application system administrators. *Participatory design* within the context of coordinated defense would include the analysis and feedback of the firewall system administrator and/or the subject matter experts to foresee and solve these kinds of problems. Two additional coordination elements are seen as dependencies: *transferability* and *usability*. *Transferability* refers to a managerial or operational concept, a physical entity, or an intellectual substance. *Usability* on the other hand serves to *standardize* the design and the coordination process in addition to the *participatory design*. While *usability* ensures the standardization of the process design and enhance the participatory design, *transferability* among the system administrator, subject matter experts (as the participants), and the firewall policy increases. *Transferability* further allows sensors whether they refer to human sensor network or technical sensor network to jointly perceive and collect incidents and produce collaborative incident responses.

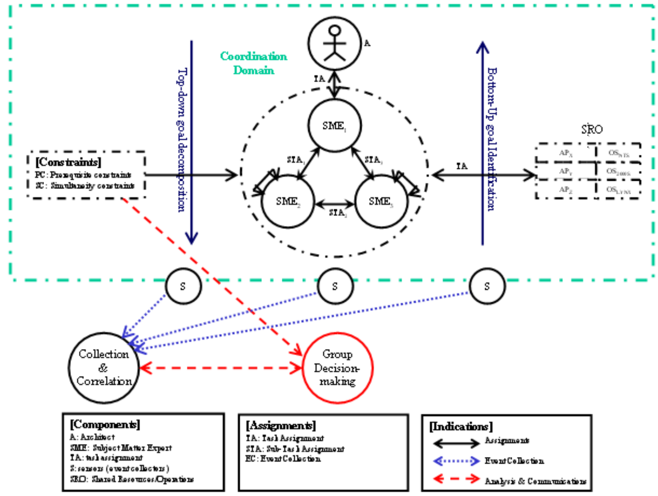
Last but not the least is the emphasis on the constraints applied in the coordination process. Constraints are set for boundary control, which would exclude unnecessary or redundant processes in the coordination. Two constraints are mentioned in the Coordination Theory: prerequisite constraints and simultaneity constraints. Prerequisite constraints serve to exclude pre-conditioned events in the monitoring process for group decision-making accuracy. For example, a classified top-secret application could be seen as a backdoor application with access privileges, which might cause noise to the firewall. Simultaneity constraints include sub-components such as scheduling and synchronization. For example, in the phase of an extensive scope of coordination, subject matter experts (humans) and technology (machines) might face problems of synchronizations and scheduling. The baseline analysis would help to consider the tolerance thresholds of the synchronization. When correlating notifications or sequencing events, both prerequisite and simultaneity constraints would serve to pre-analyze potential threats.

MODEL OF MONITORING-BASED COORDINATED DEFENSE

The model of monitoring-based coordinated defense is directly derived from the Coordination Theory as illustrated in Figure 2. In this model, the architect(s) (represented as A in the Figure 2) work(s) within a coordination domain. The architect either works within his or her own team (or an individual) or with teams from other departments or outside agencies, specified as subject matter experts (SME). Under such condition, the architect determines and selects a goal; this goal selection implies a task hierarchy, where tasks are divided structurally and subtasks are derived from the tasks. The architect works with other subject matter experts through task (or sub-task) assignments (TA). In Figure 2, SME_1, SME_2 and SME_3 inter-communicate cooperatively and self-sufficiently without the architect's participation. Sub-task assignments (STA_1, STA_2, and STA_3) could be assigned among subject matter experts (SME_1, SME_2 and SME_3). The inter-communication among subject matter experts was done through the governance of the standardization of the usability and the accessibility to the shared resources/operations (SRO). An alternative loop is designed in this model where participatory design could be done through the feedback of the participants (mainly, the architect and the subject matter expert). It could enhance the performance of the coordination, reduce the possibility of the prerequisite constrains, and enhance simultaneity. Outputs from the coordination activities ought to be transferable from the producer activity to the subject matter expert activity. (Ibid, 94) These above are what have been defined as the visible framework of the coordination.

An invisible layer of coordination is constructed in this framework of the coordinated defense, where the transferability (represented by the blue dot and red dot lines in the Figure 2) dominates the baseline analysis. Sensors (represented by S in the Figure 2) of various kinds are built in

Figure 2. Model of the monitoring-based coordinated defense



to collect atomic events for upper level correlation analysis. The results of the event collection and correlation are communicated with and analyzed by the group decision-making entity where the decision-making entity will take constraints into account.

The group decision depends on the dependency analysis in the Coordination Theory. In this framework, we have identified two dependency components: *usability* and *transferability*. The *usability* governs the standardization among corporate policy, system policy, interactions among SMEs, interactions among the SMEs and the systems, and automated interactions among systems, etc. First, if discrepancies are found within the interactions among the SMEs and the systems, the *usability* dependency would be found problematic and the group decision has to reevaluate the entity itself. The entity here represents policy, SME, resources such as application or system settings. For example, if the firewall system policy complies with the corporate security policy, but violates with the policy of another application run by another division, the *usability* dependencies would be found inefficient and problematic. If a time constraint to a response is set and trigger, a warning indicator would be sent to the group decision. This type of problems is categorized as usability dependency that governs the standardization of the coordination. Additionally, if discrepancies are found in the interoperated task assignments including sub-task assignments among different entities, the *transferability* dependency would be found problematic and the group decision has to reevaluate task assignments including sub-task assignments. For example, if while the corporate security policy governs all application system administration policy, discrepancies are found in the task assignments that the firewall SME has allowed a backdoor application program to access, the *transferability* dependencies would be found problematic in the interactions between the firewall SME and the firewall system. The *transferability* dependency could be utilized and implemented through the human-peer sensor network mentioned in Figure 1 or periodic internal and/or external security auditing. Third, prerequisite and simultaneity constraints would be considered in the dependency analysis in the decisions for the coordinated defense.

CONCLUSION

To conclude, we emphasized the importance of coordination among technologies, management, policies, procedures and personnel in the context of monitoring-based defense. We have analyzed the procedures of coordinated attacks to explain the nature of these attacks and we provided the countermeasures of coordinated defense. Specifically, we identified the human aspects as the weakest link in the layered defense (Figure 1). Later, we provided an example of coordinated defense mechanism in order to further explain the components of human behavior, technology, policies, and the management practices. Lastly, we provided a conceptual framework of building monitoring-based coordinated defense (Figure 2). This paper contributes to the IT security and defense society by providing a systematic way of approaching coordinated defense. It also benefits the IT security and defense research by introducing the concept of coordinated defense, about which there is little research. Future studies in this area may include empirical analysis of the existing coordinated defense, such as incident response handling/reporting systems run by Computer Incident Response Team (CIRT) or the security operation mechanisms run by Security Operation Center (SOC) against attacks, from the coordination theory perspective.

REFERENCES

9/11 Commission Report. (2001). *Commission on Terrorist Attacks upon the United States*. 9/11 Commission Report. Extracted on May 20, 2005 from http://www.9-11commission.gov/.

Amnesty International. (2004). *Russian Federation: Coordinated attacks in Ingushetia* Public Statement News Service No: 159. Extracted on May 25, 2005 from http://www.amnesty.ie/user/content/view/full/2423, June 22, 2004.

Braynov, Sviatoslav, and Jadliwala, Murtuza. (2003). *Representation and Analysis of Coordinated Attacks*. FMSE'03, October 30, 2003, Washington, D.C. 2003 ACM 1-58113-781-8/03/0010.

C4ISR Joint Chiefs of Staff (1999). *Information Assurance: Legal, Regulatory, Policy and Organizational Considerations*, 4th Edition, Washington D. C., August 1999.

C4ISR Joint Chiefs of Staff (2000). *Information Assurance Through Defense In Depth*. Washington D. C., February 2000.

Carnegie Mellon Software Engineering Institute CERT® Coordination Center. (2002). *Creating A Computer Security Incident Response Team: A Process for Getting Started*. Extracted on October 04, 2005 from http://www.cert.org/csirts/Creating-A-CSIRT.html.

Cohen, Fred. (1996). *Strategic Security Intelligence: A Note on Distributed Coordinated Attacks*. Extracted on May 29, 2005 from http://www.all.net/books/dca/background.html.

Commercial Perspectives on Information Assurance Research: Report to the President's Commission on Critical Infrastructure Protection [1997]. Institute for Defense Analyses, Alexandria, VA, October 1997.

DelZoppo, R., Browns, E., Downey, M., Liddy, E. D., Symonenko, S., Park, J. S., Ho, S. M., D'Eredita, M., and Natarajan, A. (2004). *A Multi-Disciplinary Approach for Countering Insider Threats*. Workshop on Secure Knowledge Management (SKM), Amherst, NY, September 23-24, 2004.

DOD Joint Doctrine Division. DOD Dictionary of Military Terms. "*Coordinated attack*." Extracted on May 25, 2005 from http://www.dtic.mil/doctrine/jel/doddict/natoterm/c/00332.html. Joint Electronic Library. May 27, 2005 amended.

DOD 4120.24-M *DSP Policies & Procedures Appendix 6: Defense Specifications, Standards and Handbooks*. Extracted on June 1, 2005 from http://www.dsp.dla.mil/documents/4120.24-M/appendix6.htm.

Giles, Lionel. (translated 1910). *Sun Tsu on the Art of War: The Oldest Military Treaties in the World*. Extracted on May 29, 2005 from http://www.kimsoft.com/polwar.htm. British Museum. First Published in 1910.

Henning, P. R. (1997). *Air Force Information Warfare Doctrine: Valuable or Valueless?* Maxwell A.F.B. A.L. Air Command and Staff College. Extracted on May 24, 2005 from http://www.au.af.mil/au/awc/awcgate/acsc/97-0604c.pdf. March 1997.

Herbsleb, J. D. and Mockus, A. (2003). *Formulation and Preliminary Test of an Empirical Theory of Coordination in Software Engineering*. ESEC/FSE'03, September 1-5, 2003, Helsinki, Finland. 2003 ACM 1-58113-743-5/03/0009.

Green, J., Marchette, D., and Northcutt, S. (2000). *Analysis Techniques for Detecting Coordinated Attacks and Probes*. Extracted on May 22, 2005 from http://www.totse.com/en/hack/hack_attack/162442.html. September 22, 2000.

Libicki, M. C. (1995). *What is Information Warfare?* Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University. Washington, D.C., August 1995. U.S. G.P.O.: 1996-405-201:40011.

Malone, Thomas W. (1989). *Center for Coordination Science in Massachusetts Institute of Technology*. CHI '99 Proceedings, May 1989.

Malone, Thomas W. and Crowston, Kevin. (1990). *What is Coordination Theory and How Can It Help Design Cooperative Work Systems*? CSCW 90 Proceedings. October 1990.

Malone, Thomas W. and Crowston, Kevin. (1994). *The Interdisciplinary Study of Coordination*. ACM Computing Surveys, Vol. 26, No. 1, March 1994, pp. 87-119. 1994 ACM 0360-0300/94/0300-0087.

Maradmin. (1999). *Coordinated Defense Of the Marine Corps Enterprise Network*. Maradmin number: 322/99, Marine Corps. July 22, 1999. Extracted on May 29, 2005 from http://www.usmc.mil/maradmins/maradmin2000.nsf/0/9033a8c4684a389785256aab0 04e7dab?OpenDocument.

Ning, P. and Xu, D. (2004). *Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems*. ACM Transactions on Information and System Security, Vol. 7, No. 4, November 2004, pages 591-627. New York, NY. 2004 ACM 1094-9224/04/1100-0591.

Noh, S. and Gmytrasiewicz, P. J. (1999). *Implementation and Evaluation of Rational Communicative Behavior in Coordinated Defense*. Autonomous Agents '99, Seattle W.A. 1999 ACM 1-58113-066-x/99/05.

Northrop Grumman *Network Early Warning Systems (NEWS) News Releases* (2001). http://investor.northropgrumman.com/phoenix.zhtml?c=112386&p=IROL-nrtext&t=Regular&id=373263&, Herndon, VA., August 13, 2001.

Pal, P., Webber, F., and Schantz, R. (2001). *Innovative Solutions: Survival by Defense-Enabling*. Proceedings of the 2001 Workshop on New Security Paradigms, Cloudcroft, New Mexico, September 2001. ISBN: 1-58113-457-6. Pages: 71-78.

Park, J. S. Ho, S. M. (2004). *Composite Role-based Monitoring (CRBM) for Countering Insider Threats*, Second Symposium on Intelligence and Security Informatics (ISI), Tucson, Arizona, June 2004.

Pynadath, D. V. and Tambe, M. (2002). *Multiagent Teamwork: Analyzing the Optimality and Complexity of Key Theories and Models*. AAMAS'02, July 15-19, 2002, Bologna, Italy. 2002 ACM 1-58113-480-0/02/0007.

Report to the Chairman, Committee on Armed Services, House of Representatives—Information Security: Progress and Challenges to an Effective Defense-Wide Information Assurance Program. United States General Accounting Office, March 2001.

Taipei Times. (2005). *Iraq Bleeds as Coordinated Attacks Continued*. Extracted May 28, 2005 from http://www.taipeitimes.com/News/world/archives/2005/05/02/2003252852. Monday, May 02, 2005, Page 7.

The September 11 Digital Archive. Extracted from http://www.911digitalarchive.org/.