A Framework of Coordinated Defense

Shuyuan Mary Ho

School of Information Studies
Syracuse University
smho@syr.edu

Abstract

Coordinated defense in cyber warfare has emerged to protect information as assets through the use of technologies, policy, and best management practices for defending against coordinated attacks. However, combining massive security technologies, policies, procedures and security staff does not guarantee the effectiveness of defense. Without a well-defined and structured element of coordination, an organization can not stand firm during coordinated attacks. The "culture" of coordinated defense must evolve within an organization over time. Organizations that adopt the framework of coordinated defense can develop a set of common assumptions regarding the organizational operations, and build a social firewall through well-structured coordination. The framework forms unique characteristics of an information security culture for that organization. This paper adopts Coordination Theory, and conceptualizes implicit coordination elements in the realm of monitoring-based coordinated defense in a dynamic online environment. While there is little research done in coordinated defense, this paper contributes to the information systems security by providing a framework for approaching coordinated defense. Through analyzing coordination dependencies, a culture of collaboration in a virtual world could be enhanced. Future studies in this area may include empirical analysis of an 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 a solid coordinated defense against 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). Threats from insiders, for instance, may cause this chain of defense to be vulnerable (Ho 2008b). One of the methods for detecting insider threats is to utilize peer employees as network sensors in the workplace to detect malicious acts (Ho 2008a). In this context, coordination becomes a critical indicator, as it serves two major functions: explicitly, coordination links humans, systems, management, policies and procedures together as a social firewall for a stronger security defense; implicitly, when problems occur in coordination, dependency analysis can helps identify anomalies within human network. This paper illustrates dependency analysis of the Coordination Theory that helps to identify problems, particularly, in the human coordination in the web of coordinated defense efforts.

In the following, the problem of coordinated attack – and the associated attack behavior – will be analyzed. Because the conventional technique of simply integrating elements of policy, systems, management practices, and procedures may not be effective, a framework of coordinated defense is proposed. This framework addresses a layered defense mechanism. In this mechanism, the dependencies of coordination are identified, and a methodology for analyzing dependencies is illustrated.

Problem Statement – Coordinated Attacks

In the battlefield of physical space, attack strategies have progressed from single attacks to sophisticated distributed coordinated attacks (Cohen 1996). "Coordinated attack" is organized, requires careful planning and design, and makes it difficult to differentiate between a decoy event and an actual event. Such organized attacks normally combine various elements of resources and are "beyond the power of a single attacker" (Braynov and Jadliwala 2003). The 911 tragedy in 2001 was a result of a coordinated attack (The September 11 Digital Archive 2008); which was composed of well-planned and executed synchronous offensive actions. Similarly, in another case, Turkey shared intelligence with Iran in launching coordinated actions when striking against the Iranian Kurds (Fraser 2008).

Likewise, in cyber warfare, coordinated attack strategies can be used to confuse detectors and intrusion detection systems (Ning and Xu 2004), provide decoys, and distract attention. A coordinated attack is an art that combines a large variety of attack strategies to penetrate and collapse critical systems and infrastructure (Braynov and Jadliwala 2003, Green, Marchette and Northcutt 2000). Distributed Denial of Services or logic bombs are examples of

techniques that have been used to distract attention in the cyber warfare. Attacks get particularly complex if an insider works with outside intruders to penetrate information systems. A "compromised insider" who weakens the coordination infrastructure, might launch a subtle added attack, such as "Trojan attack." In this light, good coordination builds a social firewall that guards the organization from coordinated attacks.

The concept of coordinated defense (Noh and Gmytrasiewicz 1999) in the cyber warfare has 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 U.S. public sectors. In the Secretary of Defense's 1999 Annual Report to the U.S. President and the Congress, coordination among different offices has been emphasized as one of the keys to guard information from coordinated cyber attacks (Cohen 1999). In addition, the Carnegie Mellon Computer Emergency Response Team Coordination Center builds capacity for coordinated response through incident response teams against intended or unintended attacks (West-Brown et al. 2003).

In order to better understand how to strategize on coordinated defense, it is important to first understand the rationale behind how a coordinated attack is 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 on the site and find its vulnerabilities. Then, they identify and target the most vulnerable points of a site and probe their accessibility. The vulnerability and accessibility 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. After the attack is mounted by an attacker, the attackers may cover up their identities and clear off their traces/logs before inflicting severe damage (Huang, Jasper and Wicks 1999). This type of attack strategy has been described well in information warfare literature (Henning 1997, Libicki 1995) and has been used by both individual hackers as well as a coordinated effort of attackers. Paul R. Henning, in his "Air Force Information Warfare Doctrine," illustrated coordinated attacks and classified information warfare under counter-information and information assurance groups (Henning 1997).

Frameworks of Coordinated Defense

After outlining the nature of coordinated attacks, it is necessary to address the concept of layered defense (Figure 1). Understanding the concept of layered defense is a prerequisite that helps to identify the needs for coordination.

Layered defense covers all aspects of defense including social and technical aspects. Building security mechanisms and infrastructure comprise the first layer 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 possible social engineering and probing attacks. The "unless specified" access rules at the perimeter firewall provide flexibility to conditionally control unauthorized access and prevent an attacker's reconnaissance. Many technologies such as virtual private networks and de-militarized zones are also examples of 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 access control.

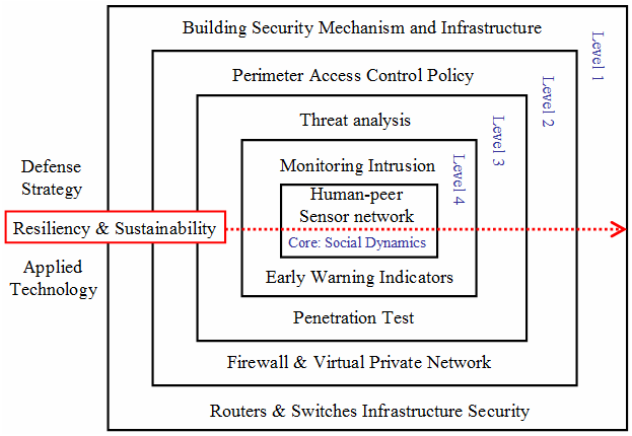

Figure 1: Multi-Layered Defense Mechanism

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 thyself from the enemy's eyes."

The fourth 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 damage can be avoided. Sensor technology at an 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. But even further, a more sophisticated detection of malicious anomalies centered as the kernel layer of defense could be assessed through co-worker observation. Peers already serve as social sensors that monitor social activities within the organization. At this stage, anomalies in the behavior of human subjects could indicate ill-natured intents possibly leading to insider threats (Ho 2008a). 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 mechanisms.

Coordinated efforts themselves are far superior to any of the different 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 enhances the resilience and sustainability among layers of defense within an organization (Figure 1). "Good coordination is nearly invisible, and we… notice coordination most clearly when it is lacking" (p. 357).

Coordinated Defense Mechanisms

The culture of coordinated defense evolves over time. Organizations that form common assumptions of good coordination will invisibly build a social firewall among employees in the workplace. Organizations that adopt this framework of coordinated defense will result in unique characteristics for their corporate security defense. The 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). 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 (p. 110). In the following paragraphs, I will identify coordination process and analyze various types of dependencies through an illustration. Then, I will model how dependencies in the coordination process are analyzed. By understanding this mechanism, we can both explicitly enhance the social firewall within an organization and implicitly build a culture of security awareness.

Malone and Crowston (1994) conceptualize dependencies as arising between tasks rather than individuals or units. This approach has advantage of making the process easier when modeling the effects of reassignments of activities to different actors. This has been a common practice in process redesign efforts. Compared to some earlier research in the Coordination Theory taken from the CSCW literature (Malone and Crowston 1990), Malone and Crowston focused their attention on the need to coordinate, rather than on the desired outcome of coordination.

Types of Dependencies

Coordination, defined by Malone and Crowston (1994), is managing dependencies between activities. Good coordination makes any teamwork or organization joint-effort more harmonious, unnoticeable and even "invisible." In the framework of Coordination Theory, Malone and Crowston define components that are seen as dependencies between activities that are associated with individuals or entities. Activities imply movement, which builds associations such as task assignments among individuals and entities. Analyzing defense activities in light of Coordination Theory requires the analysis of security-related technologies as well as behaviors, and the linkages between the two.

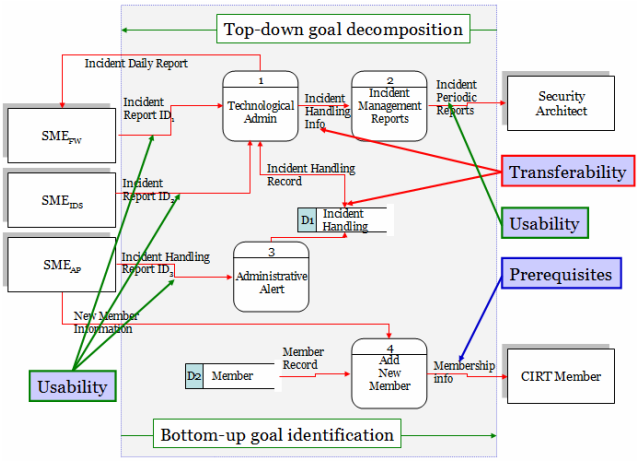

Figure 2: An Illustration of Coordinated Dependencies

In Figure 2, the security architects typically identify the strategic and task-related goals that enable a coordinated defense; the security architect oversees divisional performance, bears overall responsibility, coordinates resources from among different subject-related domains, and makes immediate decisions or judgments if a resource needs to be transferred from one entity to another. Subject matter experts (known as SMEs) are assigned with tasks that fall within a functional domain. An SME is seen as someone at managerial level in a business organization, who determines hierarchy tasks and assignments. In a hierarchical organization structure, goals are divided into tasks, and tasks are decomposed into sub-tasks. Dependency-focused activities can be found within each sub-task and those activities can critically determine

success or failure of a sub-task assignment. If a small sub-task assignment is not managed well, it could create a chain-reaction and cause disharmonious coordination and even lead to corruption at the next level higher. Likewise, it is also possible for an SME, rather than a security architect, to identify a critical need and manage task/sub-task dependencies based on needs and the amount of data or information collected. In this event, an SME may not always get specific instructions from the security architect, but still has to respond quickly based on the amount of data collect. For example, a firewall system administrator, as an SME, who is assigned a task to secure transmission by setting up the rules and policies on the perimeter firewall, actually has a coordination role. The component that a firewall administrator is assigned by a security architect to administrate a firewall is seen as a task assignment; the component that this firewall administrator sets up the firewall policy is seen as another task assignment. In this example, the dependency exists in those two task assignments. The administrator first decomposes this task into sub-tasks by analyzing what protocols and services are required by the internal users. This firewall administrator also needs to identify what back-end servers and services are running through the Internet so that the firewall rules allow permitted traffic. This firewall administrator also needs to work with other application system administrators to synchronize tasks such as allowing or blocking certain traffic run by other servers which have a need to access other network segments or even the Internet. There is a dependency existing in the task-assigning activities of working with other SMEs; there is also another dependency existing in the task-assigning activities of administering other systems. If in this case, the firewall administrator purposely allows certain traffic - or carelessly opens unnecessary ports that are not designed or defined in the task assignments - this would create a security "loophole," which is identified as a dependency problem. Such incidents should be logged for further analysis. A dependency exists when a firewall administrator coordinates with an Intrusion Detection System (IDS) administrator so that if some incidents are identified by IDSs, warning notices and alerts would be sent to firewall administrator to amend the firewall security policy. In these coordination events, two types of critical dependencies are identified: one is the dependency among various task assignments from SME_{FW} administrator to other administrators (such as SME_{IDS}); the other is various dependency activities that require back and forth communications from firewall administrator to other application servers.

Coordination Dependencies

Three critical components are emphasized in the context of a well coordinated defense:

- Quick response timing,
- Effectiveness of incident response, and
- Service availability and continuity of routine work while suffering from coordinated attacks.

These components can be seen as critical dependencies among task assignments - from monitoring phase, to report phase, to response phase and to measuring phase as illustrated in Figure 3.

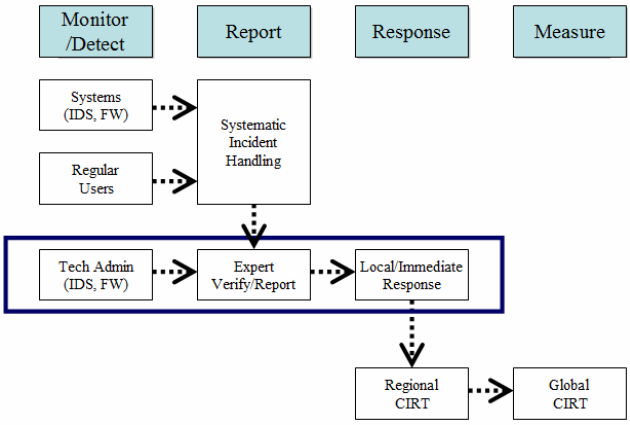

Figure 3: Example of a Context Level View of the Coordinated Defense

In the following paragraphs, I present a common situation as an example of a coordinated defense. If an employee incurs a virus attack, he would report it to technical support personnel for further attack verification and analysis. It depends on the seriousness of such an incident whether it would take down only one computer, or the entire network. The technical support personnel would analyze its impact so as to match the countermeasure and actions in responding to such an incident. Some balancing points during the critical incident handling are found in a just-in-time response. Time is an important factor. A quick response to the incident while the affected area is still small could minimize the response handling effort before the entire network is infected. Effectiveness of incident handling is critical because it minimizes both resources and effort. On the other hand, if an incident is not handled properly and effectively, it might severely affect and even interrupt the routine work, and cause the entire workforce tremendous amount of opportunity loss. Improper judgment with regards to closing down the entire network while the incident is not severe would still cause the unavailability of the service.

How to apply Coordination Theory to address the above mentioned situation is discussed below:

Task-Resource Dependencies. A "resource" in the context of the Coordination Theory can refer to a person (administrator, employee, etc.), a tool, a data file or a system. When the administrator gets a virus-attack incident report, he would diagnose it first, make a judgment call, and assign a *task priority*. If the task is flagged as urgent, he needs to prioritize this incident handling task and put other administrative tasks aside temporarily. Then, he

ought to decide initial actions based on the nature and complexity of task. If a computer virus is contagious and self-propagating, the technical administrator needs to segregate affected areas from non-affected areas, quarantine the virus, and separate physical networks. This solution is necessary and effective, but it causes another task-resource dependency problem. As the server is closed down, those who are not affected by the virus may suffer regular service unavailability and their routine work with outside business partners may be forcefully interrupted. A strategy of "*providing more resources*" could be implemented to solve such a problem. Frequent backups at different service levels such as providing data files backup, redundant applications, and even redundant network infrastructure would provide fail-over functions and assure the service as being uninterruptible. This strategy should be taken and implemented only after a cost-benefit analysis and a business risk management analysis.

Task-Subtask Dependencies. If a virus is hard to handle immediately and individually, this incident handling should be *decomposed into multiple sub-tasks* which should be elevated and handled by an upper level technical support such as a regional incident response team. Again, the time-response would be critical here. Since a quick response time is crucial for business operation, it may shorten the incident handling time for regional personnel to respond to the incident. These incidents have to be handled immediately. In order to expedite the handling response time regionally and globally, this response team should be planned and set up ahead of time to handle incidents in a very short timeframe. Additionally, since some measures are done globally at an enterprise level, senior management might also need to be involved to ensure successful implementation. The role of the senior management is to clarify the different responsibilities of the incident-handling technical members ahead of time, and ensure that performance and integration of sub-tasks will be carried out effectively.

Model of Coordinated Defense

The model of an effective coordinated defense is directly derived from Coordination Theory. The architect(s) and/or senior management work(s) within a coordination domain. The architect either works within his or her own team (or an individual) or along with teams from other departments or outside agencies, specified as SMEs. Under such conditions, the architect determines and selects a goal; this goal selection implies a task hierarchy, where tasks are divided structurally and sub-tasks are derived from the tasks. The architect works with SMEs through task (or sub-task) assignments (TA) such as incident handling procedures, and through joint-access of the resources such as the incident handling report database. Multiple SMEs (such as SME_{FW}, SME_{IDS} and SME_{AP}) communicate cooperatively and self-sufficiently without the architect's participation. Sub-task assignments are assigned among SMEs. The inter-communication among SMEs is done through the governance and of the standardization of the usability and the accessibility to the shared resources/operations, such as the incident handling report database. An alternative loop could be designed in this model, where participatory design could be done through the feedback of the participants (mainly, the architect and the SMEs). This could enhance the performance of the coordination, reduce the possibility of the prerequisite constraints, and enhance simultaneity. Outputs from coordination activities ought to be transferable from producer activity to the subject matter expert activity. (Malone & Crowston 1994) These outputs have been defined as the visible framework of coordination.

Conclusion

To conclude, the importance of coordination among technologies, management, policies, procedures and personnel is emphasized in the context of monitoring-based coordinated defense. The procedures of coordinated attacks to explain the nature of these attacks have been analyzed, and the countermeasures of coordinated defense have been provided. Specifically, the weakest link in the layered defense (the human element) has been identified (Figure 1). Later, some types of dependencies in the coordinated defense mechanism are provided to further explain the components of human behavior, technology, policies, and the management practices (Figure 2). Lastly, I provided a context-level view of coordinated defense (Figure 3) to illustrate dependency analysis. This paper contributes to the information systems security by providing a framework for approaching coordinated defense. It also benefits research into information systems security by introducing the evolutional 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 a Computer Incident Response Team, or security operation mechanisms performed by a Security Operation Center against attacks, from the coordination theory perspective.

Acknowledgments

I thank Kevin Crowston for his advice in using Coordination Theory. I also wish to thank Conrad Metcalfe for his helpful comments and editing assistance.

References

Braynov, S., and Jadliwala, M. 2003. Representation and Analysis of Coordinated Attacks. In *Proceedings of the 2003 ACM Workshop on Formal Methods in Security Engineering*, 43-51. Washington, D.C.

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

Cohen, F. 1996. *Strategic Security Intelligence: A Note on Distributed Coordinated Attacks*. Extracted from http://www.all.net/books/dca/background.html on June 16, 2008.

Cohen, W. 1999. Annual Report to the President and the Congress. Office of the Executive Secretary, U.S. Department of Defense. Extracted from http://www.dod.gov/execsec/adr1999/index.html on June 16, 2008.

Crowston, K. 1994. A Taxonomy of Organizational Dependencies and Coordination Mechanisms. Working Paper Series 174, MIT Center for Coordination Science. Retrieved from http://ccs.mit.edu/papers/CCSWP174.html on June 16, 2008.

Fraser, S. eds. 2008. Turkey, Iran launch coordinated attacks on Kurds. Washington Post. June 5, 2008. Extracted from http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060500659.html on June 16, 2008.

Giles, L. eds. 1910. *Sun Tsu on the Art of War: The Oldest Military Treaties in the World*. 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.

Ho, S. M. 2008a. Attribution-based Anomaly-Detection: Trustworthiness in an Online Community. In *Social Computing, Behavioral Modeling, and Prediction*, 129-140. Tempe, FL: Springer.

Ho, S. M. 2008b. Towards a Deeper Understanding of Personnel Anomaly Detection. *Cyber Warfare and Cyber Terrorism*, 206-215. Hershey, PA: Information Science Reference.

Huang, M.Y.; Jasper, R. J; and Wicks, T. M. 1999. A large scale distributed intrusion detection framework based on attack strategy analysis. *Computer Networks: The International Journal of Computer and Telecommunications Networking* 31: 2465-2475.

Green, J.; Marchette, D.; and Northcutt, S. 2000. *Analysis Techniques for Detecting Coordinated Attacks and Probes*. September 22, 2000. Extracted from http://www.totse.com/en/hack/hack_attack/162442.html on June 16, 2008.

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, T. W. 1989. Center for Coordination Science in Massachusetts Institute of Technology. In *CHI '99 Proceedings*, May 1989.

Malone, T. W. and Crowston, K. 1990. What is Coordination Theory and How Can It Help Design Cooperative Work Systems? In *CSCW 90 Proceedings*, October 1990.

Malone, T. W. and Crowston, K. 1994. The Interdisciplinary Study of Coordination. *ACM Computing Surveys*, 26(1), March 1994, 87-119.

Ning, P. and Xu, D. 2004. Hypothesizing and Reasoning about Attacks Missed by Intrusion Detection Systems. *ACM Transactions on Information and System Security*, 7(4), November 2004, 591-627. New York, NY.

Noh, S. and Gmytrasiewicz, P. J. 1999. *Implementation and Evaluation of Rational Communicative Behavior in Coordinated Defense*. In *Proceedings of the Third Annual Conference on Autonomous Agents*, 1999, 123-130. Seattle, Washington.

The September 11 Digital Archive. Extracted from http://www.911digitalarchive.org/ on April 28, 2008.

West-Brown, M.; Stikvoort, D.; Kossakowski, K.P.; Killcrece, G.; Ruefle, R.; and Zajicek, M. 2003. Handbook for Computer Security Incident Response Teams (CSIRTs). Carnegie Mellon CERT Coordination Center®. CMU/SEI-2003-HB-002.

ICCCD 2008 Proceedings

This paper was published in the *Proceedings of the Second International Conference on Computational Cultural Dynamics,* edited by V. S. Subrahmanian and Arie Kruglanski (Menlo Park, California: AAAI Press).

The 2008 ICCCD conference was held at the University of Maryland, College Park, Maryland, USA, 15–16 September, 2008.