# CYBER WARFARE SIMULATION TO PREPARE TO CONTROL CYBER SPACE


***Martin R. Stytz, Ph.D.***
*UMUC/Calculated Insight/Georgetown*
*Washington, DC*
*(407) 497-4407, (703) 349-6411*
*mstytz@att.net , mstytz@gmail.com*

***Sheila B. Banks, Ph.D.***
*Calculated Insight*
*Orlando, Fl 32828*
*(407) 353-0566*
*sbanks@calculated-insight.com*



**ABSTRACT**

*Accurate simulation of cyber warfare can prepare decision-makers for its challenges. With cyber warfare, it is possible to control an adversaries' information, target the portions of cyber space used for situational awareness and decision-making, lead the adversary to make desired decisions, and strike directly at the opposition's mind. A cyber attack diminishes individual and group situational awareness and command and control by undermining one or more elements of cyberspace. The cyber space threat is magnified by the technologies of the network centric warfare (NCW) paradigm. The vulnerabilities exploited by cyber warfare are inherent to NCW technologies. Due to the importance of cyber space to success in warfare, proper assessment of real-world and cyber circumstances must be trained via exposure to simulated cyber attacks.*

*To simulate a cyber attack, we need only alter the information presented to the decision-makers. Appropriately configured simulation environments can be used to develop expertise in dealing with cyber warfare and provide an environment for the development of cyber warfare strategies and tactics. In the paper, we discuss the effects of cyber attacks upon individual and group situational awareness and an approach to cyber warfare simulation.*

# CYBER WARFARE SIMULATION TO PREPARE TO CONTROL CYBER SPACE


***Martin R. Stytz, Ph.D.***
*UMUC/Calculated Insight/Georgetown*
*Washington, DC*
*(407) 497-4407, (703) 349-6411*
*mstytz@att.net , mstytz@gmail.com*

***Sheila B. Banks, Ph.D.***
*Calculated Insight*
*Orlando, Fl 32828*
*(407) 353-0566*
*sbanks@calculated-insight.com*



**ABSTRACT**

*Accurate simulation of cyber warfare can prepare decision-makers for its challenges. With cyber warfare, it is possible to control an adversaries' information, target the portions of cyber space used for situational awareness and decision-making, lead the adversary to make desired decisions, and strike directly at the opposition's mind. A cyber attack diminishes individual and group situational awareness and command and control by undermining one or more elements of cyberspace. The cyber space threat is magnified by the technologies of the network centric warfare (NCW) paradigm. The vulnerabilities exploited by cyber warfare are inherent to NCW technologies. Due to the importance of cyber space to success in warfare, proper assessment of real-world and cyber circumstances must be trained via exposure to simulated cyber attacks.*

*To simulate a cyber attack, we need only alter the information presented to the decision-makers. Appropriately configured simulation environments can be used to develop expertise in dealing with cyber warfare and provide an environment for the development of cyber warfare strategies and tactics. In the paper, we discuss the effects of cyber attacks upon individual and group situational awareness and an approach to cyber warfare simulation.*


## 1. INTRODUCTION – CYBER SPACE

"*Great part of the information obtained in War is contradictory, a still greater part is false, and by far the greatest part is of a doubtful character. ... This is not a trifling difficulty even in respect of the first plans, … but it is enormously increased when in the thick of War itself one report follows hard upon the heels of another;*" - Clausewitz, *On War*[1]

Surprise produces confusion. Confusion leads to uncertainty and inaction. Uncertainty and inaction lead to disadvantage. The accumulated weight of disadvantages results in defeat. This causal chain is as old as war. Cyber warfare allows both surprise and confusion to be inflicted upon an adversary at a time of our choosing, in a manner of our choosing, and in a way that exploits the adversaries' decision-making biases. By using cyber warfare, it is possible to control an adversaries' information, target the portions of cyber space used for situational awareness and decision-making, lead the adversary to make desired decisions, and strike directly at the opponent's mind, decision processes, and situational awareness. Using cyber warfare, it is possible to lead the adversary to make the decisions that we desire. Because of the inherent uncertainties in warfare, the informational challenges posed by cyber warfare may overwhelm decision-makers when first experienced. Therefore, decision-makers should be prepared for the environment that they will encounter in cyberspace. We contend that accurate simulation of cyber warfare may prepare decision-makers for the challenges they will encounter in cyber warfare. In this paper, we discuss the informational aspects of cyber warfare and present an approach to preparing decision makers for cyber warfare's effects using a simulation environment that exploits virtual machine technology and the effect of information uncertainty upon situational awareness.

[1] Clausewitz. (1968) *On War*. Penguin Books: Middlesex, UK, translation by J.J. Graham, 1908, p. 162.

*Cyber space* is composed of four main elements: 1) *data*, 2) *computing technologies* (such as computer hardware, computer software, computer networks/infrastructure, network protocols, virtualization, and cloud computing), 3) *information analysis/comprehension technologies* (such as information visualization, artificial intelligence, collaboration, and data mining technologies), and 4) *information interaction/management technologies* (such as human-computer interaction, intelligent agent, human intent inferencing, intelligent system intent inferencing, personalization technologies, and database technologies.)

The threat posed by cyber attacks arises from the adoption and use of information to leverage operational performance in the network centric warfare (NCW) paradigm [1,2]. The improvements in shared situational awareness and group decision-making enabled by Network Centric Warfare (NCW) capabilities can increase military effectiveness by reducing decision-maker information uncertainty and by maximizing information sharing between and among decision-makers. NCW makes information, computers, software, and the network profitable targets for attack because they enable information exploitation. The vulnerabilities exploited by cyber warfare are intrinsic to the technologies used to achieve the advantages provided by Network Centric Warfare. As noted by Geer and Archer [3], the challenges posed to the cyber defender are increasing. Therefore, we believe that cyber defenders must always expect their cyber defenses to be breached and be prepared to operate successfully despite the successful breach while also recovering from and sealing the breach.

Cyber space dominance in a network centric environment is critical because cyber space dominance enables effective, trustworthy decision-making [4]. Cyber space dominance insures that accurate, trustworthy, relevant information is provided to the decision-makers. Because cyber space dominance is not assured; systems and decision-makers must be prepared for cyberwarfare attacks designed to undermine decision-making ability by attacking information. There are two needs that the preparation must address. The *first* is the need to prepare decision-makers for the confusing, contradictory, and misleading information that will be presented to them during a cyberwarfare attack. The *second* aspect is preparing decision-makers to exploit cyber space dominance by effective employment of trustworthy information analysis/comprehension, and information interaction/management technologies.

As cyber attacks of all types increase in sophistication, cyber attack technology has increased in its ability to target specific data and physical resources [5-17], which in turn will undercut the usefulness and value of information for decision making and situational awareness [18-24]. This increase in sophistication has been clearly demonstrated by the Stuxnet, Flame, Red October, and DuQu malware deployments. The challenges posed by increasingly capable malware are compounded by the introduction of virtual machine [NIST 800-125] and cloud computing technologies [25-31]. The combination of more capable malware coupled with virtual machine and cloud computing technologies indicates that a reassessment of modes of information protection and the associated reasoning about protection of data and computational resources during an attack is required. Future malware attacks will, inevitably, target systems in the same sophisticated manner as Stuxnet and transmit data from the targets and/or subtly modifying the data so as to corrupt data in a malicious but not immediately apparent manner. We expect that future cyber attacks will be structured to support the introduction of false information, to target individuals for information degradation, and to precisely corrupt information that reaches decision-makers. Cyber attacks will be coordinated and mounted in campaigns in order to maximize confusion and maximally exploit cyber successes.

Simulation environments allow us to prepare decision-makers for the inevitable cyber attacks upon the information they need for decision-making and to develop cyber warfare experience, strategies, and tactics that preserve information value and insure that decision-relevant information reaches decision-makers. Training in effective cyber response is imperative because uncertainty, confusion, and information overload are known to lead to improper and counter-productive human behaviors; and these three outcomes are the intended outcome of a cyber attack. Because of the volume of information that must be considered and the rapid pace of activity in the cyber battlespace, the decision-maker and decision support personnel must be prepared for the confusing and novel information circumstances that will occur.

The tools and training needed to prepare decision-makers for the challenges of cyber conflict must address three classes of cyber situations that they may face: 1) operations in a NCW environment during normal conditions, 2) operations in a NCW environment during a cyber attack, and 3) operations in a NCW environment after a cyber attack. The training, techniques, and tools needed by decision-makers in these three circumstances may be developed using simulation environments designed to achieve the following goals: 1) to improve understanding of the challenges posed to decision-makers during a cyber attack, 2) to test and evaluate the cyber defense tools, techniques, and training, 3) to practice using cyber defense tools and techniques, and 4) to determine information

value during a wide array of circumstances in order to deploy cyber defenses. The tools, techniques, and training must be extensible and flexible so that they can readily altered to address new cyber threats and tactics. The remainder of this paper addresses these issues. The paper is organized as follows. The next section contains background information concerning information transmission measurement, situational awareness, and virtual machine technology. Section Three contains a discussion of the use of simulation to acquire experience in cyber warfare. Section Four presents an approach to reducing cyber attack effectiveness by the use of virtual machine technology. Section Five contains a summary and future work.

## 2. BACKGROUND

In this section we discuss information movement modeling equations, situational awareness, and virtual machine technology.

### 2.1 Information Movement Modeling Equations

The movement of information through the organization is important to the development of situational awareness. Based on our prior work regarding network centric organizations [39-42, 132], there are two sets of entities that must be considered when assessing data movement: 1) sources of data and 2) recipients of data. To represent these entities, let *r* be the set of data recipients and allow them to be arbitrarily and uniquely labeled from 1 to n. Within the same organization, let *s* be the set of data sources and allow them to be arbitrarily and uniquely labeled from 1 to m. Let $I_r$ be the data required by/destined for a particular recipient of data *r* and let *n* be the number of these data recipients and let $I_s$ be the data sent from any source of data *s* and let *m* be the number of these data sources. Then, $I_r \leftarrow I_s$ represents the instantaneous data volume (in bytes) between a source, *s*, and a recipient, *r*, of data. We can then define the **total information in movement** at any time, $\mathbf{I_1}$, as the following (note that this formulation encompasses unicast, multicast, and broadcast network transmissions underway at any time as well as other modes of communication):

$$\mathbf{I_1} = \left( \sum_{i=1}^{n} I_{r_i} \right) \leftarrow \sum_{j=1}^{m} I_{s_j} \qquad \textbf{(1)}$$

$\mathbf{I_1}$ represents the total amount of information in transit (in bytes) from all sources of information to all recipients of information within an organization at any given time. The maximum value for $\mathbf{I_1}$ corresponds to the maximum demand for data transmission within an organization at any time. $\mathbf{I_1}$ indicates that for a network centric force to be effective, its data capacity must accommodate peak demands for transmission of data in conjunction with peak demand for transmission of network management data, and therefore indicates the minimum data carrying capacity required by the organization's communications infrastructure.

Using $\mathbf{I_1}$, we can define the **instantaneous data velocity** $\boldsymbol{\varpi}$ within an organization at a given time $\boldsymbol{\tau}$ using equation 2. Data velocity is a measurement of the change in the amount of data moving through the organization's communications infrastructure, a data velocity of zero means that the amount of data in the organization's communications infrastructure has not changed between the two time intervals. A high value for information velocity means that the requirement for data transport has increased and that the information infrastructure has been able to respond to the increase in demand for data transport.

$$\boldsymbol{\varpi}_{\tau} = (I_{1_{\tau}} - I_{1_{\tau-1}}) / I_{1_{\tau-1}} \qquad \textbf{(2)}$$

The **mean data velocity** $\boldsymbol{\varpi_m}$ for an organization over a time interval, $\boldsymbol{\gamma}$, is defined in equation 3. A large change in $\boldsymbol{\varpi}$ and/or $\boldsymbol{\varpi_m}$ may indicate a cyber attack is underway. A large decrease in $\boldsymbol{\varpi}$ may indicate that cyber defenses are imposing significant delays upon information delivery. If we let ($r_i \leftarrow s_i \neq 0$) indicate that there is network traffic between the indicated recipient and sender of information, then we can define $\mathbf{I_{2_\tau}}$, the **average time required for data to move from sources to recipients** within an organization during a time interval $\boldsymbol{\tau}$, using equation 4. $\mathbf{I_2}$ for a given time interval, $\boldsymbol{\gamma}$, is calculated using Equation 5.

$$\boldsymbol{\varpi_m} = \left( \sum^{\gamma} \varpi_{\tau} \right) / \gamma \qquad \textbf{(3)}$$

$$\mathbf{I_{2_\tau}} = \left( \prod_{i=1}^{n} I_{r_i} \leftarrow \prod_{j=1}^{m} I_{s_j} \right) \div \sum_{i=1,j=1}^{n,m} \left( \Delta t \left( r_i \leftarrow s_j \right) \right) \forall \left( \left( r_i \leftarrow s_j \right) \neq 0 \right) \quad \textbf{(4)}$$

$$\mathbf{I_2} = \left( \sum_{\tau=1}^{\gamma} I_{2_\tau} \right) / \gamma \quad \textbf{(5)}$$

Equations 1-5 provide both a means to assess the effects of a cyber attack as well as insight into the effects of cyber attacks upon an organization's infrastructure. Additionally, we can gain insight into those occasions when decision-makers are being overloaded with information, indicated by an increase in $I_1$ and $I_2$ and when they may be lacking the information they need, which could be indicated by a decreasing $I_1$ and a decreasing $\boldsymbol{\varpi_m}$.

Additional metrics can be derived to provide further insight into the state of cyber space and function as indicators of malware infestation and cyber attack. Equations 6 – 10 provide examples of derived metrics. The $\mathbf{I_{1_{metric}}}$ measure, defined in equation 6, is the data transport metric. The $\mathbf{I_{1_{metric}}}$ assesses the volume of relevant data moving through the system in relation to the volume of data required by the decision-maker. A low value for the measure indicates that the decision-maker may lack required information, whereas a high value indicates that the decision-maker is receiving the information that is required.

$$\mathbf{I_{1_{metric}}} = \mathbf{I_{1_{actual}}} / \mathbf{I_{1_{required}}} \quad \textbf{(6)}$$

Another indicator that can be derived to determine if a cyber attack is underway and to assess the effectiveness of cyber defenses is the ratio between the actual data transport rate from source to recipient and the required data transport rate from source to recipient, called the $\mathbf{I_{2_{\tau metric}}}$, (defined in equation 7). The higher the value achieved for the $\mathbf{I_{2_{\tau metric}}}$ the less likely that a successful cyber attack is underway and the higher the likelihood that the cyber defenses are performing effectively. Conversely, a low value for $\mathbf{I_{2_{\tau metric}}}$ indicates that a cyber attack is retarding data transport, which can interfere with decision-making and situational awareness.

$$\mathbf{I_{2_{\tau metric}}} = \mathbf{I_{2_{\tau actual}}} / \mathbf{I_{2_{\tau required}}} \quad \textbf{(7)}$$

Like the $\mathbf{I_{2_{\tau\ metric}}}$, the $\mathbf{I_{2_{\gamma\ metric}}}$ (defined in equation 8) measure assesses data transport from sources to recipients, but over a longer time interval. The $\mathbf{I_{2_{\gamma\ metric}}}$ sacrifices sensitivity to transient events to achieve insight into ongoing, low-level disruptions of information transport. The $\mathbf{I_{2_{\tau\ metric}}}$ is useful for detecting cyber attacks, whereas the $\mathbf{I_{2_{\gamma\ metric}}}$ is more effective in its ability to assess the effectiveness of cyber defenses as well as low data volume cyber attacks. The higher the value of the $\mathbf{I_{2_{\gamma\ metric}}}$, the less likely that a successful cyber attack is underway and the more likely that cyber defenses are performing adequately. Conversely, a low value for $\mathbf{I_{2_{\gamma\ metric}}}$ indicates that it is more likely that a cyber attack is retarding data transport, which can interfere with decision-making. More importantly, a low value for $\mathbf{I_{2_{\gamma\ metric}}}$ indicates that cyber defenses are likely being ineffective against the cyber attack.

$$\mathbf{I_{2_{\gamma metric}}} = \mathbf{I_{2_{\gamma actual}}} / \mathbf{I_{2_{\gamma required}}} \quad \textbf{(8)}$$

Additional insight into the state of data transport and adequacy of cyber defenses in the face of cyber attack can be achieved by looking for changes in mean data velocity at times $\Psi$ and $\Psi+1$, as captured in the $\boldsymbol{\varpi_{m\ metric}}$ defined in equation 9. The $\boldsymbol{\varpi_{m\ metric}}$ assesses changes in data velocity over long, non-overlapping, and not necessarily consecutive time periods. A value for $\boldsymbol{\varpi_{m\ metric}}$ close to 1.0 indicates that data velocity is consistent and that cyber defenses are adequate, values either very much greater than 1.0 or less than 1.0 indicates that data velocity is being affected either by a blockage, diversion of data, or by the introduction of malicious data into the system. In equation 9, the value of 1 added into the numerator and denominator insures that a "divide by zero" does not occur and that if the mean data velocity is optimal (i.e., $\boldsymbol{\varpi_m}$ is equal to zero) that the $\boldsymbol{\varpi_{m\ metric}}$ has a value of 1.0

$$\varpi_{m\ metric} = (1+\varpi_{m\ \Psi+1}) / (1+\varpi_{m\ \Psi}) \quad (9)$$

To help insure that a cyber attack is detected and that cyber defenses are being effective, we can compare performance ratios over time to gain insight into the stability and accuracy of the components of the ratios. Obviously, the components of the metrics to be compared must be gathered at the same point in time in order to provide a valid comparison. An example of this type of metric is the information transport stability metric, $\varphi$ (defined in equation 10), for assessment of $I_{2_{\gamma metric}}$ and $\varpi_{m\ metric}$. A value for $\varphi$ less than 1.0 and that is relatively constant would be a good sign that information is moving to decision-makers as needed and that the system has not been corrupted or compromised by a cyber attack.

$$\varphi = I_{2_{\gamma metric}} / \varpi_{m\ metric} \quad (10)$$

We can determine the desired values for equations 1 – 10 using simulation environments to develop guidance for decision-makers concerning assessments of the state of cyber space, determining the information that they require across a variety of circumstances, determining the rate at which information should move from source to recipient, and suggesting the time intervals that should be used for metrics-related measurements. Simulation environments will also be key to determining where to place the probes for gathering required data to compute the metrics.

## 2.2 Situational Awareness Background

The development of information technologies, network centric warfare, and modern electronic networking technologies has given rise to the belief that military staffs will quickly develop a shared correct situational awareness that will greatly facilitate decision-making, thus permitting faster response to challenges by reducing the complexities of the military administrative and command structure. Cyber warfare undercuts these assumptions about situational awareness for the individual and groups.

The concept of shared situational awareness is not well defined, but much research has been devoted to determining the process by which *shared situational awareness* arises [32-49]. There is a some agreement on *what* situational awareness is: situational awareness is the result of a dynamic process of perceiving and comprehending events in one's environment, leading to reasonable projections as to possible ways that the environment may change, and permitting predictions as to what the outcomes will be in terms of performing one's mission, as illustrated in Figure 1. There is also some agreement on what constitutes *shared* situational awareness and how it develops via a process of integrating the mission-essential overlapping portions of the situational awareness of individual team members—thus, developing a group dynamic mental model of the battlespace [33, 34]. For the purposes of our discussion, we adopt Endsley's definition [33, 34], wherein she defines situational awareness (SA) as the following: "the perception of the elements in the environment within a volume of space and time, the comprehension of their meaning, the projection of their status into the near future, and the prediction of how various actions will affect the fulfillment of one's goals." Endsley identifies four components of situational awareness, PERCEPTION (what are the facts), COMPREHENSION (understanding the facts), PROJECTION (anticipation based upon understanding), and PREDICTION (evaluation of how outside forces may act upon the situation to affect your projections)[2]. These components are not stages, but instead interlocking cycles that progress in relation to each other. Factors promoting individual SA are both structural and situational. Structural factors include background, training, experience, personality, interests, and skill, as well as situational factors that include the mission that is being performed and the circumstances prevailing, all affect situational awareness as illustrated in Figure 2. Several factors are known to cause degradation of individual situational awareness, including: 1) ambiguity (arising from discrepancies between equally reliable sources, 2) fatigue, 3) expectations and biases, 4) p*rior* assumptions, 5) psychological stress, 6) misperception, 7) task overload (too much to do, 8) boredom (not enough to do on the tasks to maintain focus), 9) information shortage, 10) information overload, 11) information interruption, 12) irrelevant information, 13) mission complexity, 14) fixation/attention narrowing, 15) erroneous expectations, and 16) lack of experience.

[2] These stages are similar to Boyd's Observe-Orient-Decide-Act (OODA) loop construct [50].

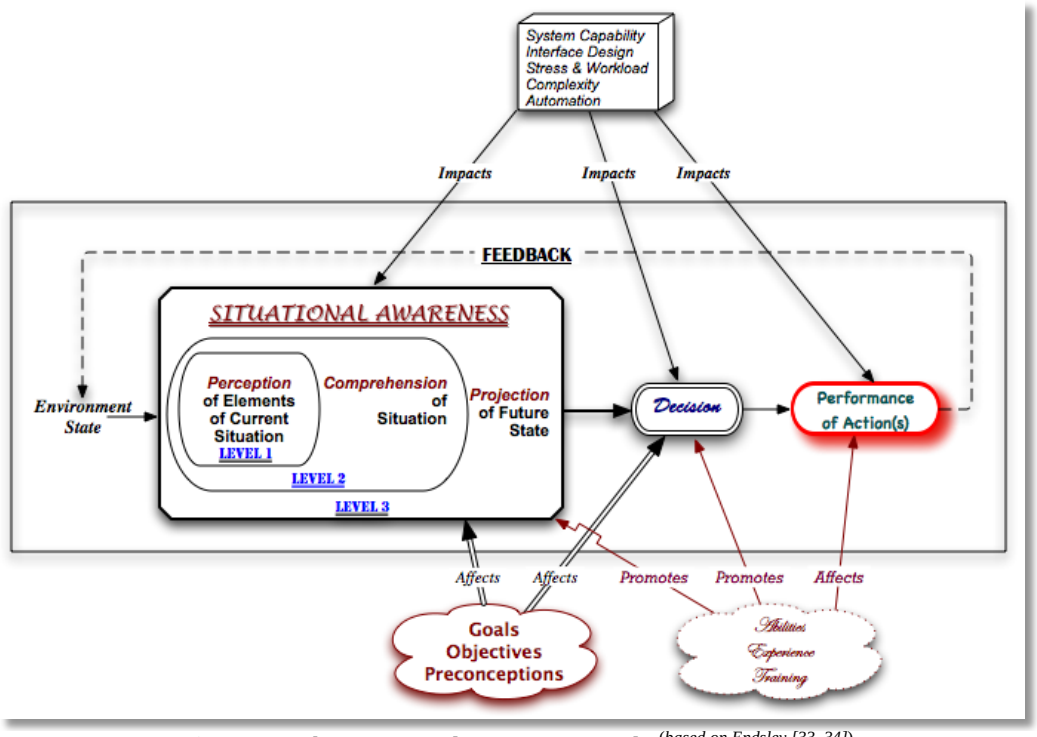


**Figure 1:** The Situational Awareness Cycle (*based on Endsley [33, 34]*)

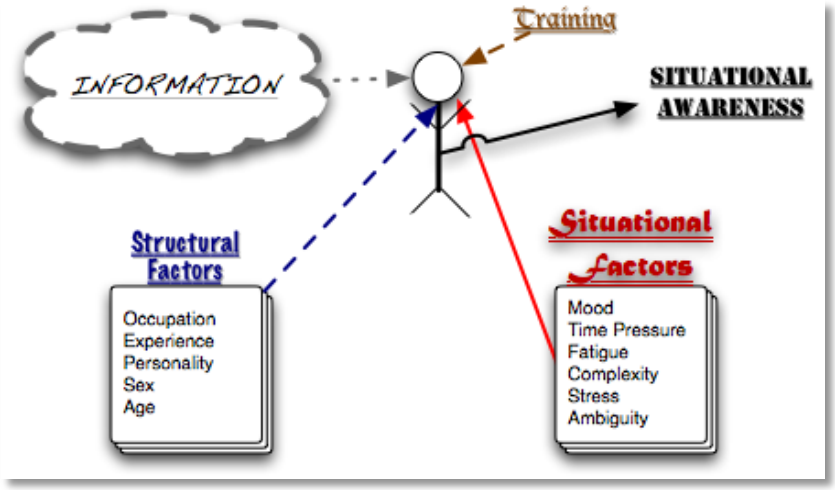


**Figure 2:** A Paradigm for Situational Awareness Formation

Shared situational awareness can be defined as a common relevant mental model of a distributed environment; an accurate, common, picture of a battlespace; or the degree of accuracy by which one's perception of current environment mirrors the situation as perceived by others. Shared situational awareness benefits from information superiority and a flexible and interoperable information picture, but relies upon communications in order to share information. Shared situational awareness can provide a common operational picture, which is essentially the same near-real-term mental model of the battlespace. Shared situational awareness insures that a clear and accurate, common, relevant mental model of the battlespace is possessed by leaders at all levels. Shared situational awareness also provides a common comprehension of relevant policy and strategy as well as the state of operations, technology, logistics, tactics, plans, command structure, personalities, and readiness posture. By improving and augmenting tools for shared and individual situational awareness, we can increase the ability to develop situational awareness in crisis situations and better assess an enemy's situational awareness of our state. As with individual

situational awareness, there are many factors that are known to degrade shared situational awareness, including: 1) false group mindset, 2) the press on regardless mindset (allowing mission accomplishment to affect objective assessment), 3) insufficient training/variable skill levels, 4) poor personal communications skills, 5) perception conflicts, 6) frequent changes in personnel, 7) degraded operating conditions, 8) lack of a common information across the group, and 9) the absence of non-verbal cues. In general, distributed workers have less overlap in their mental models than do co-located workers.

## 2.3 Virtual Machine Technology

A virtual machine, illustrated in Figure 3, is software that creates a virtualized environment between the computer platform and its operating system, so that software (including an operating system) can execute on an abstract machine [57-79]. A virtual machine, as described in several seminal papers [57-79], is a software-based impersonation of a computer. A virtual machine presents the illusion of the real computing machine to a user and associated software. In a virtual machine, all components of a given computer hardware/operating system combination are replicated within a host operating system to provide the computational illusion that all applications executing within the virtual operating system are running on the original software/hardware combination hardware; however, this situation is not the case. A virtual machine does not add functionality to the operating systems (and applications within them) that it hosts but instead provides functionality and a software interface to them that is identical to the replicated system and also controls communication between the virtual machines. In this environment, there is complete protection of all actual system resources and hardware from each of the virtual machines; each virtual machine is also isolated from all other virtual machines. Communication between virtual machines is possible, and is usually patterned upon network communication. Achieving a virtual machine capability requires the use of technology for management of virtual processors, virtual storage, virtual memory, and virtual I/O devices.

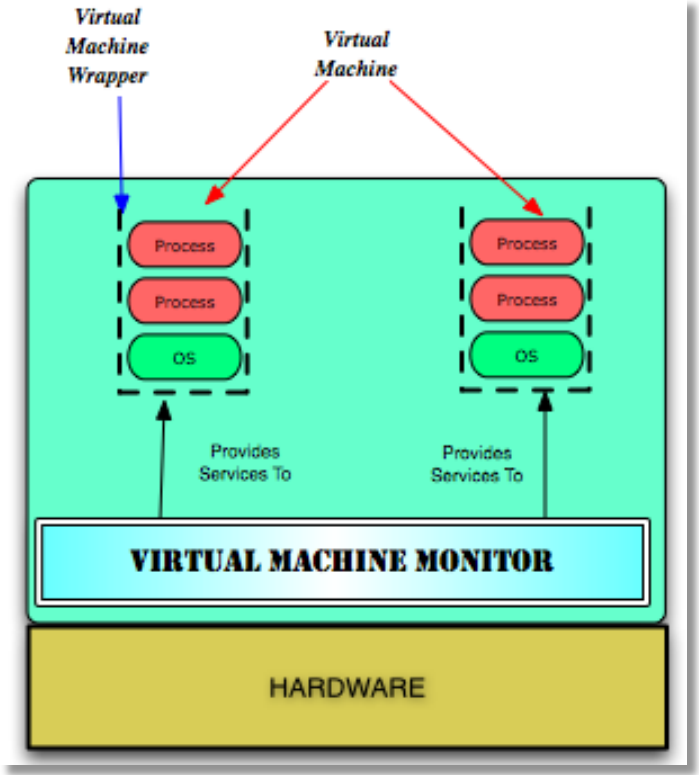


**Figure 3:** Virtual Machine Architecture

The supervision and oversight of executing software in each virtual machine (VM) is performed by the virtual machine monitor. The virtual machine monitor (VMM), sometimes referred to as a hypervisor, or virtualization manager, is a program that allows multiple operating systems, which can include different operating systems or multiple instances of the same operating system, to share a single hardware processor. A VMM is usually designed for a particular CPU architecture. When running under the control of a hypervisor, each operating system on a

computer appears to have a dedicated processor, memory, and other computing resources. However, the VMM actually controls the real processor and its resources, allocating and scheduling them for each operating system in turn. Because an operating system is often used to run a particular application or set of applications in a dedicated hardware configuration, the use of a VMM makes it possible to run multiple operating systems (and their applications) within a single computer architecture.

There are three technologies that are needed to assemble a virtual machine: virtual memory, software emulation, and context switching. With these technologies, it is possible to build a host operating system that can provide virtual machine capabilities to any given guest operating system. In 1974, Popek and Goldberg defined the formal necessary conditions for achieving a virtualizable computer architecture: "For any computer a virtual machine monitor may be constructed if the set of sensitive instructions for that computer is a subset of the set of privileged instructions." In other words, the most essential requirement that the computer architecture must exhibit in order to be virtualizable is that privileged instructions[3] must trap. This requirement means that when a guest virtual machine (while running directly on the real processor) attempts to execute a privileged instruction, the processor halts instruction execution and returns software program execution flow control to the virtual machine monitor (VMM) so that the VMM can decide whether or not to execute the instruction or simulate execution of the instruction by some other means. Furthermore, Popek and Goldberg determined that a true virtual machine architecture must exhibit three essential characteristics. The first characteristic is that any program run under the VMM should exhibit behavior identical with what would be observed if the program had been run directly on the original machine. They offered one exception to this rule, timing; ie. execution in a virtual machine can be slower than it would be on the actual machine. The software (or hardware) supporting the virtual machine environment needs to manage the resources used by the virtual machine(s), and to intervene in their operation occasionally, thus altering the timing characteristics of the running virtual machine(s). The second characteristic is that a statistically dominant subset of the virtual processor's instructions execute directly by the real processor. The third characteristic is that the VMM is in complete control of system resources. A virtual machine running on the system does not have direct access to any of the system's real resources, it must go through the VMM, which means that all behaviors and instructions executed by a virtual machine on the computer can be monitored and halted or modified as necessary.

## 3. SIMULATION FOR ACQUIRING EXPERIENCE IN CYBER WARFARE

As cyber attacks increase their technical sophistication, the old modes of information protection and reasoning about data protection during an attack must be re-assessed. Simulation provides a safe and flexible way to prepare decision-makers for the challenges of cyber attacks as well as to re-assess data protection techniques and cyber defenses. To be useful as cyber attack technologies evolve, cyber simulation must portray cyber attack and defense actions in a manner that corresponds to the manner in which humans perceive them. Therefore, the simulation must capture and represent the activities of the decision-maker and staff, the attacker and defender goals, the sequence of operations that the attacker will execute, the activities of the cyber defender, logical and physical data location(s), and the potential responses of the attackers and defenders to each others' actions. In previous work we presented a technique for cyber simulation that can be used to model cyber operations, its components, and the possible responses to defensive actions [51,52,53]. The same simulation approach can be used to develop procedures for cyber defense training.

To prepare decision makers for cyber warfare, there are four key training considerations. First, teaching how to determine the targets of attacks. Second, teaching the techniques and tactics likely to be used against targets. Third, teaching techniques and tools that should be used to counteract each type of attack and the effects of each type of attack. Fourth, teaching means for explicitly assessing information value and targeting cyber defenses to protect the highest value information. Cyber simulation can be used to achieve these four goals. To minimize the cost of the development of cyber simulation environments, we couple existing simulation systems with cyber simulation systems that provide effects of cyber simulation and cyber attack upon the existing simulation systems, as illustrated in Figure 4. To create cyber simulation environments that impart the required cyber defense knowledge and experience, the components of the cyber simulation systems must exchange information about the attack and defense, the status of the cyber event, and portray the results of the cyber attack and defensive responses.

[3] A privileged instruction is one that can only be executed by the operating system kernel; ie., it is a powerful and dangerous machine command executed only when the system is in the system administrator state.

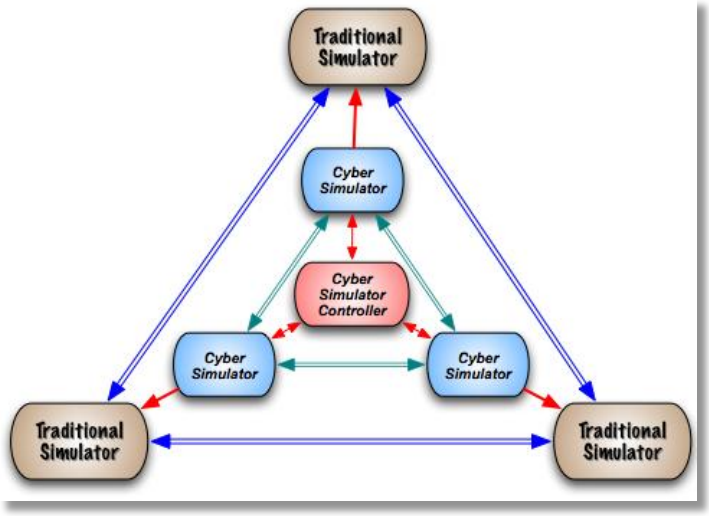


**Figure 4:** Conceptual Cyber Simulation Environment

The key to this approach is that to simulate a cyber attack, we need only affect the information presented to the simulation environment decision-makers. To do so, there are three basic approaches that we can use to simulate the effect of a cyber attack: 1) an increase in information presented, 2) blocking information needed by a user, and 3) substituting false information for the actual information requested by the user. In all cyber attacks, the actual target is the human operator's ability to make an effective decision, in effect increasing the decision-maker's decision uncertainty. There are two central problems that a decision-maker faces: 1) determining which information to use to make a decision and 2) determining when the information in hand does not permit a decision to be made based upon the information. This second problem is well-known and occurs in many situations, yet the problem persists and only training can equip a decision-maker with the experience and expertise needed to recognize either situation. The second situation is especially treacherous because it leads to a decision-maker taking the wrong action or no action at a critical moment. To prepare the decision-maker for the information issues that will arise during different types of cyber attacks, a few general techniques can be employed. The decision-maker can be given an overwhelming amount of information, denied information, given a mixture of accurate and false information, or a mixture of these techniques that varies over time.

Cyber warfare simulation uses cyber simulation systems in conjunction with existing simulation hosts. The cyber simulation system must perform three key tasks: 1) determine if a cyber attack is successful, 2) determine the effect of the cyber attack upon each host and its data, and 3) portray defensive responses to the cyber attack. In our approach, each host has a cyber simulator that services it and provides these capabilities. The cyber simulator provides each host that it serves with the inputs needed to portray the effects of simulated cyber attacks. Because each cyber simulator services only one simulation environment host, the cyber simulators communicate with each other using a logically separate cyber simulation network. The approach requires two logical but separate communications networks. One logical network links the simulation systems that form simulation environments identical to those in use today. The second logical network links the cyber simulators and is used to exchange data concerning cyber attacks and defensive responses to the cyber attacks. Each cyber simulator is connected to a simulation environment host, allowing the cyber simulator to control the information presented by the host so that the data available to decision-makers will approximate the information available to them in a real-world cyber event.

To simulate cyber events, we use the cyber simulators to compute the probability that the cyber attack would penetrate the host's simulated cyber defenses and, if the attack is successful, the initial state for the cyber attack that the host system should enter. Cyber attack probabilities are computed by combining the historical success rate for similar cyberattacks upon similar target systems combined with a weighting for desired success rate for cyberattacks within the simulation and a weighting for the desired success rate for the same class of cyberattacks within the simulation. After computing the initial state for a successful cyber attack, the cyber simulator then advances from state to state in the attack and drives their host systems through the appropriate information availability states as determined by the state of the simulated cyber event. At each step of the cyber attack and defensive response, the decision-makers are provided with indications of the status of the attack and information behaviors that mirror the delays and alterations that would occur in the corresponding real-world attack. Changes to the cyber defense that

increase or decrease the depth of the cyber defense are reflected in increased or decreased delays in information movement through the systems. To employ this approach, each cyber simulation system computes an identical representation for the progression of the cyber event based upon the initial description of the cyber attack and the associated probability for transition from state to state in the cyber attack. To keep the cyber control message size reasonable, we pre-position the states for the cyber events at each cyber simulator. Determining the states and documenting them in a manner that a computer can use is accomplished using the Unified Modeling Language (UML) [54, 55].

Because the cyber simulators communicate between themselves to exchange information, shared information includes the type of cyberattack being simulated, the defenses that are present, the cyber defenses that have been activated, the status of cyber defenses, the probability of success of the attack given the defenses and defensive response, and the variations of the cyber attack that are being simultaneously launched. Other information that needs to be shared and would typically come from the simulation cyber controller includes data sources to be interfered with, the probability of success for interference with each source, the types of data from each source to be corrupted, and the probability of data corruption, the frequency of corruption, and technique for corruption for each type of data from each source. Additional information provided by the cyber simulator controller includes the types of data from each data source to be faked/inserted into the data stream, the probability of a successful insertion, the frequency of data insertion, the types of data to be inserted instead of the actual data, the types of data from each data source to be blocked, the probability of success for each attempt at blockage, the frequency of attempts for blockage, and the length of each successful blockage. Additional cyber simulator control and response information can be encapsulated, at a minimum, within a few probability statements transmitted from the cyber simulator controller to the cyber simulators and, as the cyber simulation capabilities improve, the information that is exchanged can be elaborated upon so that the cyber simulation can increase its sophistication. The probabilities for the success and progress of a cyber attack can be derived using a combination of assessments of the vulnerability of the software being attacked and the historical likelihood of success of similar attacks as computed using statistics gathered by the various computer attack response agencies and the National Threat Database.

## 4. DIMINISHING CYBER ATTACK EFFECTIVENESS

Diminishing the effectiveness of cyber attacks results in improved protection and use of the elements of cyber space (data, computing technologies, information analysis/comprehension technologies, information interaction/management technologies) in order to minimize the opportunity for surprise and exploitation of surprise. To diminish the effectiveness of the cyber attack and thereby preserve usable SA and integrity for the elements of cyber space requires training in assessing and counteracting cyber attacks and their effects upon decision-making. The distributed environment training environment architecture allows us to prepare decision-makers to protect cyber space, to prioritize information, to prioritize the elements of cyber space, and to operate in a cyber warfare environment wherein some cyber space elements, especially data, are compromised to an uncertain degree.

### 4.1 Cyber Defense Technology Considerations

Because any cyber defense can and will be defeated, our cyber defense goals are the following: 1) to make defeating a cyber defense as difficult as possible, 2) to provide cyber defenders with dynamic defenses, 3) to provide the cyber defenders with a foundation for the development of tools for rapid detection of cyber attacks, 4) to enable cyber defenders to successfully operate despite a breach in cyber defenses and 5) to provide an environment that enables rapid recovery from cyber penetration and compromise. To complement these technical goals, we require a means for identifying, modeling, and prioritizing the key components of each element of cyber space in any decision context. To model the relative priorities of each of the components of the four elements of cyber space we use protection rings. For the cyber defense, the rings correspond to priorities for information protection and can be used to guide resource allocation as well as decisions to isolate systems or subsystems that are compromised. Rings "closer" to the center of each element's ring conceptually contain components of that cyber space element that are of greater value, importance, and usefulness to the decision context at hand. The number of rings and the content of each ring are determined by the decision-making context. We use one set of rings for each element of cyber space. Each ring for each cyber space element contains information of approximately the same importance for a decision-making context. Therefore, to simulate cyber warfare we affect the specific information that will be used in a decision-context by modifying the information content of specific rings for those elements that are to be compromised by the cyber attack. The type of cyber attack, the cyber defenses, the expertise of the decision-maker, and the learning outcome(s) for the simulation exercise determine the number of rings affected for each element and the value of the element's components that are altered.

In our approach, we determine which information rings are compromised using the probability that the simulated cyber defenses that protect the information in each ring can be compromised. These probabilities are based upon the operations and outcomes of similar real-world cyber attacks. To determine which information in a compromised "ring" to alter, the simulation environment maintains a record of the cyber attacks that have succeeded as well as the decision-making context faced by the decision-maker in the simulation environment. These two pieces of information are used to compute an estimate of the likelihood that the cyber attack can alter, destroy, or falsify each component of a compromised ring. The cyber controller then simulates the required change and passes the result on to its simulation host. To enhance realism, not all of the information of equal importance to a decision context (i.e., in the same ring) is altered, only some of the information in each affected ring is changed.

### 4.2 Active Cyber Defense

As evidenced by the continued increase and severity of cyber defense breaches, current approaches to cyber defense are minimally effective. Furthermore, in light of foreseeable developments in malware capabilities [5-17], we suggest that the current ***static*** *defense-in depth* for information systems soon will become unviable in the face of new cyber attack capabilities and that cyber warfare simulation can aid in the development of new techniques for cyber defense. The challenges faced by cyber defense points to the need for the use of ***dynamic layered cyber defense*** technologies (DLCD). DLCD is designed to isolate malware infestations and to maintain sufficient, accurate, and trustworthy cyberspace elements throughout the organization in spite of the attack, insure mission accomplishment, and give decision-makers sufficient time to recognize and counteract the attack. Figure 5 illustrates the essence of the approach for a single element of cyber space. In DLCD, each element of cyber space is protected by one or more virtual machines, with the capability to protect one or more components in each element with additional virtual machines with an ever-decreasing number of privileged instructions as warranted by the threat and importance of the component to the current decision. The successive layers in the VM layering for an element have increasingly restrictive sets of privileged instructions and may even have no privileged instructions. The number of rings in a cyber space element and the number of virtual machines deployed to protect the element and its components are not correlated, the allocation of virtual machines for cyber defense is a decision made by human decision-makers. By using multiple virtual machines to protect each of the elements of cyber space, the approach supports dynamic allocation of cyber defense resources, either by adding additional virtual machines to the protection of an element or component, altering the virtual machine mix, or by changing cyber attack detection systems within each virtual machine for an element.

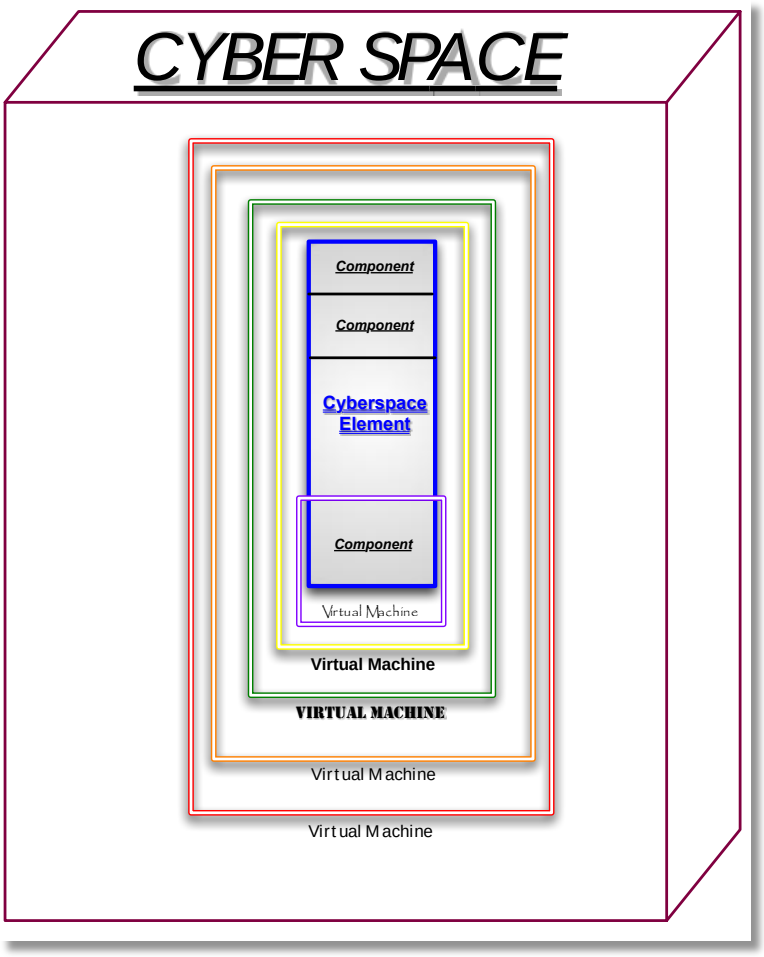


**Figure 5:** Nominal Dynamic Cyber Defense Architecture For an Element

By using a multi-layered virtual machine approach, the defense can take the initiative in responding to a cyber attack while the attack is in progress. For example, if a virtual machine, element, or component is compromised, a portion of it can be selectively abandoned and cyber defense shifted to protect the portions that have not been infected. The compromised portion can also be restarted in a more secure environment from a safe, infestation-free state. DLCD allows for flexible protection of cloud and virtual machine resources as well as data. A cyber simulation environment can prepare decision-makers to manage a dynamic layered cyber defense.

A crucial challenge that the cyber defender must address is how to protect the elements of cyber space, especially important information, during cyber attacks without imposing an unacceptable delay upon information delivery while preserving the value of information relative to the decisions to be made [18-24]. The importance of timely and accurate information delivery to success is hard to overstate, delay leads to incorrect decisions, failure to make decisions, and failure to gain or maintain situational awareness. Further compounding the information delivery challenge is the need to share information in order to develop and maintain group situational awareness; in the modern battlespace there are generally many decision-makers involved in the information assessment and decision process in every decision. While information increases in value when it is shared, the sharing process also increases the vulnerability of the information, the decision support tools, and of the decision-making process. As a result, when decision-makers are assessing cyber space protection strategies they must not only consider how to protect cyber space and the information they require but how to protect the same information as it is delivered to all others involved in the same decision.

In our approach, the cyber warfare training challenge is twofold. First, decision-makers must learn how to assess the metrics for each element, no one metric can provide evidence of a cyber attack or successful cyber defense. While artificial intelligence can be employed to aid the decision-maker, there are no substitutes for human judgment, the ability to maintain situational awareness, and the ability to correlate disparate activities into insight concerning the

state of a cyber space element. The second challenge is that human decision-makers must learn how to substantiate or refute their theories concerning the cyber security state of a given element. Due to the complexity of these two challenges, simulation of the cyber warfare environment is a practical method for acquiring the necessary expertise and familiarity with cyber space activities and threats in order to develop and maintain cyber space situational awareness.

The pursuit of cyber space situational awareness is undertaken in order to secure cyber space and to attain situational awareness in the other parts of the battlespace; air, ground, sea, and space. Because cyber space situational awareness for the individual and groups is so important, training environments designed to provide experience and expertise in addressing cyber space situations is important. However, because of the number of variables involved in assessing the state of cyber attacks and cyber defenses, decision-makers cannot be expected to determine the state of each sub-component of each cyber space element and assess their validity during the press of events. Instead, displays for state, interfaces to support interaction and assessment of the interfaces, and displays that provide indication of the validity of the data are required. To maximize their effectiveness, decision-makers must be able to concentrate on cyber space situational awareness and cyber space status challenges without the distractions of computing and validating the metrics that they use for situational awareness and decision support.

## 5. SUMMARY

The threats posed by technically sophisticated cyber attacks are increasing. Few penetrations are detected while they are underway, most are detected only after the malware is implanted and damage to the elements of cyber space has attained a noticeable level. Possessing cyber superiority will not guarantee victory for a network centric force but the lack of cyber superiority will almost certainly ensure the defeat of a network centric force. While deception and information denial operations are techniques as old as warfare itself, technically sophisticated cyber attacks permit, for the first time, a wide-scale, persistent, and virtually undetectable attack upon the information, tools, and other elements of cyber space that a decision-maker employs to make a decision. The technically sophisticated cyber attack will undermine information, surprise decision-makers, generate confusion, forestall situational awareness development, and corrupt decision-making. As a result, tools for training decision-makers to cope with cyber attacks upon systems coupled with architectures that support real-time alteration of cyber defenses using virtual machine and cloud computing environments are needed. The complexity of future cyber systems will continue to increase, as witnessed by the development of intercloud technologies (essentially a cloud of clouds [56]) and "smart grid" technologies for remote control and management of real-world infrastructure (such as the electrical power grid[4]), which increases the complexity of cyber attacks, and create new vectors for executing cyber attacks.

In this paper, we discussed the need for cyber warfare training environments for decision-makers. As we advance in the use of the NCW paradigm for military operations, the network and associated software will become increasingly important and lucrative targets for an adversary and we must be prepared to counter their cyber attacks. Therefore, decision-makers and information technology specialists must be trained to be able to recognize and counteract a cyber attack against critical information resources early in the cyber attack. The key to the requisite training is the development of simulation environments that impart the experience and expertise needed to make effective cyber defense possible in the face of cyber attacks. We described a means for presenting the effects of cyber attacks to decision-makers in order to prepare them for the challenges of cyber warfare.

Our next efforts will address the question of simulating complex cyber attacks and cost effective but accurate provision of training services. Research targeted at advancing cyber battle understanding, human behavior modeling, intent inferencing, and decision-making in NCW and cyber warfare is needed. We must also gain a better understanding of decision-making and situational awareness within large-scale and high-volume data environments that have noise and uncertainty inherent to the data as well as due to cyber attacks.

## REFERENCES


[1] Alberts, D.S.; Garstka, J.J.; Hayes, R.E.; and Signori, D.T. (2001) *Understanding Information Age Warfare*. CCRP Press, CCRP Publication Series: Washington D.C.

[2] Alberts, D.S. and Hayes, R.E. (2003) *Power to the Edge* CCRP Press, CCRP Publication Series: Washington D.C.

[3] Geer, D.E. and Archer, J. (2012) "Stand Your Ground," *IEEE Security and Privacy*, vol. 10, no. 4, p. 96.

[4] Lynn, William J. III, (2010) "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs*, September/October.


[4] For a discussion of the smart grid, see *Communications of the ACM*, vol. 55, no. 4, 2012.

[5] Acquisti, A. and Grossklacs, J. (2005) "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy*, vol. 3, no. 1, pp. 26-33.
[6] Cook, I.P. and Pfleeger, S.L. (2010) "Security Decision Support: Challenges in Data Collection and Use," *IEEE Security and Privacy*, vol. 8, no. 3, pp. 28-35.
[7] Giffin, J. (2010) "The Next Malware Battleground: Recovery After Unknown Infection," *IEEE Security and Privacy*, vol. 8, no. 3, pp. 77-82.
[8] Hole, K.J. and Netland, L. (2010) "Toward Risk Assessment of Large-Impact and Rare Events," *IEEE Security and Privacy*, vol. 8, no. 3, pp. 21-27.
[9] Johnson, M.E. and Pfleger, S.L. (2011) "Addressing Information Risk in Turbulent Times," *IEEE Security and Privacy*, vol. 9, no. 1, pp. 49-58.
[10] Kenney, J.R. and Robinson, C. (2010) "Embedded Software Assurance for Configuring Secure Hardware," *IEEE Security and Privacy*, vol. 8, no. 5, pp. 20-26.
[11] Schiffman, J.; Moyer, T.; Jaeger, T.; and McDaniel, P. (2011) "Network-Based Root of Trust for Installation," *IEEE Security and Privacy*, vol. 9, no. 1, pp. 40-48.
[12] Stone-Gross, B.; Cova, M.; Gilbert, B.; Kemmerer, R.; Kruegel, C.; and Vigna, G. (2011) "Analysis of a Botnet Takeover," *IEEE Security and Privacy*, vol. 9, no. 1, pp. 64-72.
[13] Skoudis, E. and Zeltser, L. (2003) *Malware: Fighting Malicious Code*, Prentice Hall.
[14] Graham, R. and Maynor, D. (2006) "SCADA Security and Terrorism: We're not crying Wolf," *Blackhat Federal 2006*, Washington, DC, January.
[15] Levine, J.; Grizzard, J.; and Owen, H. (2006) "Detecting and Categorizing Kernel-Level Rootkits to aid Future Detection, *IEEE Security and Privacy Magazine*, vol. 4, no. 1, January-February, pp. 24-32.
[16] Naraine, R. (2006) "'Blue Pill' Prototype Creates 100% Undetectable Malware," *eWeek.com*, http://www.eweek.com/article2/0,1895,1983037,00.asp
[17] Rutkowska, J. (2005) Rootkits vs Stealth by Design Malware," *BlackHat Europe*, Amsterdam, March.
[18] Delquié, P. (2008) "The Value of Information and Intensity of Preference," *Decision Analysis*, vol. 5, no. 3, pp. 129-139,169.
[19] Kangas, A. (2010). "Measuring the Value of Information in Multicriteria Decision Making," *Forest Science*, vol. 26, no. 6, pp. 558-566.
[20] Lumsden, K., & Mirzabeiki, V. (2008) "Determining The Value Of Information For Different Partners In The Supply Chain," *International Journal of Physical Distribution & Logistics Management,* vol. 38, no 9, pp. 659-673.
[21] Oppenheim, C. et.al. (2003). "Studies on Information as an Asset I: Definitions," *Journal of Information Science*, vol. 29, no. 3, pp. 159-166.
[22] Oppenheim, C. et.al. (2003). "Studies on Information as an Asset II: Repertory Grid," *Journal of Information Science*, vol. 29, no. 5, pp. 419-432.
[23] Oppenheim, C. et.al. (2003). "Studies on Information as an Asset III: Views of Information Professionals," *Journal of Information Science*, vol. 30, no. 2, pp. 181-190.
[24] Shepanski, A. (1984). "The Value of Information in Decision Making," *Journal of Economic Psychology*, vol. 5, no. 2, pp. 177-194.
[25] Graaido, J.M.; Schlesinger, R.; and Hoganson, K. (2013) *Principles of Modern Operating Systems, 2nd Ed.* Jones & Bartlett:Burlington, MA.
[26] Takabi, H.; Joshi, J.B.D.; and Ahn, G. (2010) "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 24-31.
[27] Liu, Q.; Weng, C.; Li, M.; and Luo, Y. (2010) "An In-VM Measuring Framework for Increasing Virtual Machine security in Clouds," *IEEE Security & Privacy*, vol. 8, no. 6, pp. 56-62.
[28] Krutz, R.L. and Vines, R.D. (2010) *Cloud Security: A Comprehensive Guide to Secure Cloud Computing*. Wiley Publishing: Indianapolis, IN.
[29] Cachin, C. and Schunter, M. (2011) "A Cloud You Can Trust," *IEEE Spectrum*, vol. 48, no. 12, pp. 28-51.
[30] Krutz, R.L. and Vines, R.D. (2010) *Cloud Security*. Wiley Publishing: Indianapolis, IN.
[31] Jamsa, K. (2013) *Cloud Computing*. Jones & Bartlett: Burlington, MA.
[32] Boytsov, A.; Zaslavsky, A. (2011) "From Sensory Data to Situation Awareness: Enhanced Context Spaces Theory Approach," *2011 IEEE Ninth International Conference on Dependable, Autonomic and Secure Computing (DASC)*, 2011, pp. 207 - 214.
[33] Endsley, M. (1995) "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors*, vol. 37, no. 1, p. 35-64.
[34] Endsley, M.R. (1995) "Measurement Of Situation Awareness In Dynamic Systems," *Human Factors*, vol. 37, no. 1, pp. 65–84.
[35] Endsley, M.R. (2000) "Direct Measurement Of Situation Awareness: Validity and use of SAGAT," in *Situation Awareness Analysis And Measurement*, M. R. Endsley and D. J. Garland, Eds. Mahwah, NJ: Erlbaum, pp. 147–174.
[36] Gerken, M.; Pavlik, R.; Houghton, C.; Daly, K.; Jesse, L. (2010) "Situation Awareness Using Heterogeneous Models," *2010 International Symposium on Collaborative Technologies and Systems (CTS)*, 2010, pp. 563 - 572.
[37] Guang, T.; Chang, Z. (2011) "A Framework for the Distributed Situation Awareness (DSA) in C2 of NCW," *2011 International Conference on Intelligence Science and Information Engineering (ISIE)*, 2011, pp. 230 - 234.

[38] Holsopple, J.; Sudit, M.; Nusinov, M.; Liu, D.; Du, H.; Yang, S. (2010) "Enhancing Situation Awareness Via Automated Situation Assessment," *IEEE Communications Magazine*, Vol. 48, No. 3, pp. 146 - 152.
[39] Jones, R.E.T.; Connors, E.S.; Endsley, M.R. (2011) "A Framework For Representing Agent And Human Situation Awareness," *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 226 - 233.
[40] Lan, F.; Chunlei, W.; Guoqing, M. (2010) "A Framework For Network Security Situation Awareness Based On Knowledge Discovery," *2010 2nd International Conference on Computer Engineering and Technology (ICCET)*, Vol. 1, pp. V1-226 - V1-231.
[41] Ma, J.; Zhang, G. (2008) "Team Situation Awareness Measurement Using Group Aggregation And Implication Operators," *3rd International Conference on Intelligent System and Knowledge Engineering, ISKE 200*8,Vol. 1, pp. 625 - 630.
[42] Mihailovic, A.; Chochliouros, I.P.; Georgiadou, E.; Spiliopoulou, A.S.; Sfakianakis, E.; Belesioti, M.; Nguengang, G.; Borgel, J.; Alonistioti, N. (2009) "Situation Awareness Mechanisms For Cognitive Networks," *International Conference on Ultra Modern Telecommunications & Workshops, ICUMT '09*, pp. 1 - 6.
[43] Nwiabu, N.; Allison, I.; Holt, P.; Lowit, P.; Oyeneyin, B. (2011) "Situation Awareness In Context-Aware Case-Based Decision Support," *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 9 - 16.
[44] Parvar, H.; Fesharaki, M.N.; Moshiri, B. (2010) "Shared Situation Awareness System Architecture for Network Centric Environment Decision Making," *2010 Second International Conference on Computer and Network Technology (ICCNT),* pp. 372 – 376.
[45] Rahman, M. (2011) "Somatic Situation Awareness: A Model For SA Acquisition Under Imminent Threat And Severe Time Stress," *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 257 - 263.
[46] Stanton, N.A.; Salmon, P.M.; Walker, G.H.; and Jenkins, D.P. (2010) "Is Situation Awareness All In The Mind?," *Theoretical Issues in Ergonomics Science*, vol. 11, nos. 1–2, pp. 29–40.
[47] St. John, M. and Smallman, H. S. (2008) "Staying Up To Speed: Four Design Principles For Maintaining And Recovering Situation Awareness," *Journal of Cognitive Engineering and Decision Making*, vol. 2, pp. 118–139.
[48] Vachon, F.; Lafond, D.; Vallières, B.R.; Rousseau, R.; Tremblay, S. (2011) "Supporting Situation Awareness: A Tradeoff Between Benefits And Overhead," *2011 IEEE First International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, pp. 284 - 291.
[49] Xi, R.; Jin, S.; Yun, X.; Zhang, Y. (2011) "CNSSA: A Comprehensive Network Security Situation Awareness System," *2011 IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, pp. 482 - 487.
[50] Osinga, Frans. (2005) *Science Strategy and War, The Strategic Theory of John Boyd*, Abingdon, UK: Routledge.
[51] Stytz, M.R. and Banks, S.B. (2006) "Metrics for Assessing Command, Control, and Communications Capabilities," 2006 *11th International Command and Control Research and Technology Symposium,* 20-26 June, San Diego, CA.
[52] Stytz, M.R. and Banks, S.B. (2006) "Metrics to Assess Command, Control, and Communications (C3) Performance within a Network-Centric Warfare Simulation," *Proceedings of the SPIE Conference on Enabling Technologies for Simulation Science X*, vol. 6227, 17-21 April, CD-ROM.
[53] Stytz, M.R. and Banks, S.B. (2004) "Toward Computer Generated Actors As Cyber space Opposing Forces Used In Network Centric Warfare Simulations," *Proceedings of the 2004 Spring Simulation Interoperability Workshop*, Washington, DC; 18-23 April, pp. 84-95.
[54] Albir, S.S. (1998) *UML in a Nutshell*, O'Reilly Press, Sebastopol, CA.
[55] Booch, G.; Rumbaugh, J.; and Jacobson, I. (1999) *The Unified Modeling Language User Guide*, Addison Wesley, Reading, MA.
[56] Bernstein, D. and Vij, D. (2010) "Intercloud Security Considerations," *2nd IEEE International Conference on Cloud Computing Technology and Science*, pp. 537-544.
[57] Adair, R.J.; Bayles, R.U.; Comeau, L.W.; and Creasy, R.J. (1966) "A Virtual Machine System for the 360/40," Cambridge, MA*: IBM Scientific Center Report 320-2007*, May.
[58] Amdahl, G.M.; Blaauw, G.A.; and Brooks, F.P. (1964) "Architecture of the IBM System/360," *IBM Journal of Research and Development*, vol. 8, no. 2, pp. 87-101.
[59] Barham, P.; Dragovic, B.; Fraser, K.; Hand, S.; Harris, T.; Ho, A.; Neugebauer, R.; Pratt, I.; and Warfield, A. (2003) "Xen and the Art of Virtualization," *Proceedings of the 19th ACM Symposium on Operating System Principles (SOSP)*, Bolton Landing, NY, October, pp. 164-177.
[60] Case, R.P. and Padegs, A. (1978) "Architecture of the IBM System/370," *Communications of the ACM*, vol. 21, no. 1, January, pp. 73-96.
[61] Creasy, R.J. (1981) "The Origin of the VM/370 Time Sharing System," *IBM Journal of R&D*, vol. 25, no. 5, September, pp. 483-490.Doran, R.W. (1988) "Amdahl Multiple-Domain Architecture," *Computer*, October, pp. 20-28.
[62] Daley, R.C. and Dennis, J.B. (1968) "Virtual Memory, Processes, and Sharing in MULTICS," *Communications of the ACM*, vol. 11, no. 5, May, pp. 306-312.
[63] Fabry, R.S. (1973) "Dynamic Verification of Operating System Decisions," *Communications of the ACM*, vol. 16, no. 11, November, pp. 659-668.

[64] Fraser, K.; Hand, S.; Pratt, I.; and Warfield, A. (2004) "Safe Hardware Access with the Xen Virtual Machine Monitor," *Proceedings of the 1st Workshop on Operating System and Architectural Support for the on-demand IT Infrastructure*, Boston, MA, October.
[65] Gifford, D. and Spector, A. (1987) "Case Study: IBM's System 360-370 Architecture," *Communications of the ACM*, vol. 30, no. 4, April, pp. 291-307.
[66] Goldberg, R.P. (1974) "Survey of Virtual Machine Research," *IEEE Computer*, vol. 7, no. 6, June, pp. 34-45.
[67] Gum, P. H. (1983) "System/370 Extended Architecture: Facilities for Virtual Machines," *IBM Journal of Research and Development*, vol. 27, no. 6, pp. 530.
[68] King, S. T.; Dunlap, G. W.; and Chen, P. M. (2002) "Operating System Support for Virtual Machines," in *USENIX Technical Conference*.
[69] Lampson, B.W. and Sturgis, H.E. (1976) "Reflections on an Operating System Design," *Communications of the ACM*, vol. 19, no. 5, May, pp. 251-265.
[70] Laureano, M.; Maziero, C.; and Jamhour, E. (2004) "Intrusion Detection in Virtual Machine Environments," *Proceedings of the 30th EUROMicro Conference (EUROMICRO '04)*.
[71] Lett, A.S. and Konigsford, W.L. (1968) "TSS/360: A Time-Shared Operating System," *Proceedings of the Fall Joint Computer Conference*, AFIPS, vol. 33, part1, pp. 15-28.
[72] Shapiro, J.S.; Vanderburgh, J.; Northrup, E.; and Chizmadia, D. (2004) "Design of the EROS Trusted Window System," *Proceedings of the 13th USENIX Security Symposium*, pp. 165-178.
[73] Meyer, R.A. and Seawright, L.H. (1970) "A Virtual Machine Time-Sharing System," *IBM Systems Journal*, vol. 9, no. 3, pp. 199-218.
[74] Peterson, J.L., Silberschatz, A., and Gagne, G. (1983-2004) *Operating System Concepts*. Editions 1-7, John Wiley & Sons.
[75] Popek, G.J. and Goldberg, R.P. (1974) "Formal Requirements for a Virtualizable Third Generation Architectures," *Communications of the ACM*, vol. 17, no. 7, July, pp. 412-421.
[76] Popek, G.A. and Farber, D.A. (1978) "A Model for Verification of Data Security in Operating Systems, *Communications of the ACM*, vol. 21, no. 9, September, pp. 737-749.
[77] Seawright, L.H. and McKinnon, R.A. (1979) "VM/370 – A Study of Multiplicity and Usefulness," *IBM Systems Journal*, vol. 18, no. 1, pp. 4-17.
[78] Uhlig, R.; Neiger, G.; Rodgers, D.; Santoni, A.L.; Martins, F.C.M.; Anderson, A.V.; Bennett, S.M. Kagi, A.; Leung, F.H.; and Smith, L. (2005) "Intel Virtualization Technology," *IEEE Computer*, vol. 38, no. 5, pp. 48-56.
[79] Ye, Z.E.; Smith, S.; and Anthony, D. (2005) "Trusted Paths for Browsers," *ACM Transactions on Information Systems*, vol. 8, no. 2, pp. 153-186