Toward Attaining Cyber Dominance

Martin R. Stytz
Sheila B. Banks

It's not what you don't know that kills you; it's what you know for sure that ain't true.

—Mark Twain

Achieving global cyber superiority or global cyber control by any organization is no longer technically possible. Instead, the proper overarching objective should be dominance of one or more of the elements of cyberspace of most importance to the organization at any given time.[1] The successful nation is the one that achieves and maintains strategic and tactical dominance in its critical elements of cyberspace when required.[2] Two important questions related to the strategic aspects of cyber conflict are: what should be the basic technological building block(s) for strategic cyber defense to assure dominance of one's own critical elements of cyberspace, and what are the classes of strategic data target(s) strategic cyber defense must protect?

Strategic cyber conflict enables surprise, shock, and confusion to be inflicted upon an adversary at the time of the attacker's choosing, in a manner of the attacker's choosing, and in a manner that exploits the adversaries' decision-making biases. *Strategic offensive cyber dominance* exploits adversary biases by a combination of data exfiltration and manipulation to lead adversaries to make decisions that we want them to make. It undercuts the opponents' effective decision making and mission command. Strategic cyber offensive targeting should be based upon the desired effects on the data and decision processes of the opponent and not

Retired lieutenant colonel Martin R. Stytz is the Collegiate Professor for Cybersecurity at the University of Maryland and associate research professor at Georgetown University. He received a BS degree from the Air Force Academy in 1975, an MA from the University of Central Missouri, an MS from the University of Michigan, and a PhD in computer science and engineering from the University of Michigan in 1989. His research interests include distributed simulation, software protection, and cyber security.

Dr. Sheila B. Banks is president of Calculated Insight. She received her BS from the University of Miami in 1984, a BSEE and MS in electrical and computer engineering in 1987 from North Carolina State, and her PhD in computer engineering (artificial intelligence) from Clemson University in 1995. Her research interests include artificial intelligence, human behavior and cognitive modeling, and cyber security.

upon the material damage that may, or may not, be inflicted. Conversely, *strategic defensive cyber dominance* enables effective decision making for one's own side. It ensures accurate, trustworthy, relevant data is provided to friendly decision makers. The vast amount of open-source cyber-attack literature demonstrates that no combination of tactical cyber defense technologies is impervious. Therefore, one's own systems and decision makers must be prepared technologically and psychologically to function despite strategic cyber attacks designed to undermine situational awareness (SA), decision-making ability, and mission command by attacking their data and other elements of cyberspace.

Strategic cyber defense dominance arises from a combination of tactical cyber defense technologies, a resilient cyber defense system architecture, and decision-maker preparation for psychological effects of a strategic cyber attack. Technologically, a resilient strategic cyber defense should be based on an active, dynamic layered cyber defense (DLCD). Strategic cyber defense preparation requires training decision makers via exposure to the effects of cyber attacks so they can surmount the challenges posed by a strategic cyber attack. Because of the obvious dangers posed by training using cyber attacks in the real world, the decision-maker training venue must be a simulation environment. The DLCD, situational awareness, and decision-support approach we describe complements the joint information environment (JIE) or similar dataflow architectures and their cyber defenses.

This article addresses strategic cyber dominance, with a focus on strategic cyber defense. It contains a background discussion on strategic cyberspace and situational awareness while examining the active DLCD concept.[3] The article also presents an approach to strategic cyber defense training and simulation to prepare decision makers for the data uncertainties and confusion that will occur in a cyber conflict.

Strategic Versus Tactical Cyberspace

Strategic cyber warfare is a contest for access, control, use, and manipulation of the opponents' data coupled with protection and confident use of your own data. In contrast, the offensive tactical level of cyber warfare comprises the technologies used to penetrate opponents' cyber defenses and technologies to exfiltrate, alter, or manipulate their data. Examples of tactical offensive cyber warfare technologies are worms, viruses, botnets, port scanners, Trojans, backdoors, and social engineering attacks (like phishing). We use the term *malware* to denote all offensive tactical cyber warfare technologies. The defensive tactical level of cyber warfare concerns the technologies used to protect one's systems and data. Examples of technologies used for defensive tactical cyber warfare purposes are encryption, firewalls, onion routing, air-gapped networks, biometric logon, and address space randomization. We differentiate between tactical and strategic cyber operations to highlight the difference between the tactical struggle to control access to systems and their data and the struggle to access and control cyberspace elements to achieve strategic objectives. Tactical cyber conflict is dominated by technological considerations; strategic cyber conflict is dominated by data, SA, and decision-making considerations. We contend that any physical effects of tactical-level cyber activities, while important, are also irrelevant at the strategic cyber warfare level.

Cyber conflict is different from information operations. Information operations can be executed by a number of technologies, even humans, whereas the data alterations achievable in a cyber conflict are unique, of greater scope, adaptable, and more rapid than in information operations. Therefore, we consider cyberspace technology as a capability that is distinct from information operations. As noted above, the challenges faced by the strategic cyber defender are increasing, and there is little prospect for achieving complete trustworthiness for any portion of a defender's cyberspace short of complete isolation from the Internet (which obviously negates the utility of that set of the defender's cyber systems).[4] There are several clear causes for the severity and scope of the tactical cyber defense challenge. First, blended tactical cyber attacks are becoming more commonplace and should be expected. Tactical cyber attacks commonly employ cross-channel, cross-domain, and cross-functional components, thereby both significantly increasing the complexity of the tactical cyber attack and the difficulty of detecting or defending against it. Second, while defenses against known tactical cyber attacks are necessary, they are not sufficient to ensure a successful tactical cyber defense because new attack technologies are always under development. As a result, tactical cyber defenses cannot expect to repel or mitigate every attack. Complicating the problem is the existence of an unknown number of zero-day attacks. Third, cyber adversary resources are increasing due to nation-state involvement and criminal involvement, which accelerate the rate of advance in cyber-attack technologies. Fourth, computer and network technology advancements have traditionally favored tactical cyber attack, which undermines the ability of cyber defenses to repel or mitigate such an attack. Finally, tactical cyber standards compliance does not guarantee cyber security or even effective tactical cyber defense but does increase its costs. For these reasons, cyber defenders should expect their tactical defenses to be breached, they should expect breaches to be increasingly difficult to detect, and they should be prepared to operate successfully despite a successful breach while also recovering from and sealing the breach.

Despite the challenges posed by the adversary's strategic cyber-attack objectives and tactical cyber attacks, strategic cyber defense must endeavor to secure the cyberspace elements vital to the current decision-making context. The approach used to secure these elements is the cyber defense strategy; typically a cyber defense strategy is static or changes slowly on a human time scale. A decrease in trust or a delay in delivery of a crucial cyberspace element or component of an element is a strategic cyber defense "loss." Specifically, the strategic cyber defense loses if the attacker can (1) retard the delivery of cyberspace elements or components needed for critical decisions, (2) reduce the velocity of dataflow in the defender's cyber systems, (3) force the use of outdated/outmoded equipment or systems to secure cyberspace elements or components, (4) impede the exchange of cyberspace elements or components among the defenders, or (5) retard improvements or adoption of cyberspace technologies. Clearly, cyber attackers will attempt to increase their capabilities in all five areas. Of critical importance during a cyber attack is that not all elements of cyberspace or components of each element are of equal value *and* the value of each element or component varies over time due to changes in the decision context. Decision context alone determines element importance. Because element value varies, the key question for the strategic cyber defender is which of the five areas are crucial to the strategic attacker's success and which are crucial to strategic cyber defense. Cyberspace element priorities, and therefore cyber defense resource allocation, must change as circumstances and decision context change. We contend that the cyber defense strategy should also change as rapidly.

To respond rapidly to changes in cyberspace element priorities, strategic cyber defenses must be able to dynamically, seamlessly, and stealthily change to improve the defenses for the cyber elements and components that have the greatest value and importance at any given time. However, changes in the defense strategy or tactics undertaken to increase protection for crucial elements or components must not sacrifice lower-value elements or components (obviously, an element's value may increase in the next decision context.) Instead, the higher-value elements and components must be provided with additional protection(s) while preserving the value of components and elements not under attack or of less importance in the current decision context. The foundation for these capabilities rests upon DLCD and its ability to support rapid changes in cyber-defense strategy and tactics.

Executing an effective strategic cyber attack upon an important strategic and tactical target is not a technologically simple undertaking. A successful strategic or tactical cyber attack requires a high degree of technical sophistication, patience, and a deep, thorough understanding of computing technologies, human cognition, decision making, and individual and group situational awareness development. Perversely, cyber attackers need not possess these technological abilities; they can be purchased from people who do have them. However acquired, technological advances are enabling attacks not previously possible as well as increasing the likelihood of success of known types of tactical cyber attacks, which has resulted in an increased ability to target specific elements of cyberspace.[5] The challenges posed by increasingly capable malware are both compounded and offset by the widespread use of virtual machine (VM) and cloud computing technologies.[6] Cyber attackers have, and likely will retain, the tactical technical advantage and the initiative requiring that we assume that all cyberspace elements are at risk. Recent technological developments demonstrated by the Stuxnet, Bluepill, Flame, and Conficker tactical cyber attacks indicate the likely character of future attacks as well as their likely consequences upon decision makers.

Stuxnet highlighted the challenges faced by strategic cyber defense. It apparently only activated if the infiltrated system was one of its targets. In a targeted system, it proceeded to alter the software at the target and to search for new targets from within the system. Humans or computer systems did not direct or manage the Stuxnet campaign. Instead, the Stuxnet software autonomously conducted the cyber attack. The same degree of autonomy must be expected to occur in the future. Of greater concern is the primacy of cyber elements, especially data, over physical systems as illustrated by the Stuxnet attack. Tactically, Stuxnet altered the performance of the targeted centrifuges; however, its success was critically dependent upon its capability to alter data. Stuxnet altered the centrifuge performance data available to human decision makers; the human operators believed that centrifuge performance was correct. Without this key cyber-element tampering capability, the Stuxnet cyber attack would have been easily detected and would have failed.

Clearly, future cyber attacks will target systems in a more sophisticated manner than Stuxnet or Flame. They will transmit data from the targets and/or subtly modify the data to corrupt it in a malicious but not immediately apparent manner. We expect that future cyber attacks will be structured to introduce false information, to target specific individuals as well as systems for information degradation, and to precisely corrupt information that reaches decision makers within ongoing cyber campaigns of tactical and strategic significance. Cyber attacks will be coordinated and mounted in campaigns designed to maximize confusion and maximally, automatically exploit tactical and strategic successes.

As Conficker demonstrated, the technology exists to create a cyber weapon consisting of millions of computer systems and maintain command and control of that weapon despite changes to tactical cyber defenses during the tactical cyber attack. Stuxnet demonstrated the technology for a cyber weapon that behaves like a "smart munition" due to its capability to alter, damage, or destroy specific data on specific physical systems. Eventually, nations will possess cyber arsenals containing a variety of these and other classes of controlled, precision cyber weapons as well as broad cyber-attack weapons. We should expect that cyber campaigns will employ a wide variety of malware that operates cooperatively and strategically to disorient and confuse decision makers, delay decisions, and lead decision makers to incorrect conclusions and poor decisions without being aware the information they are using is corrupted. Despite the clear and increasing cyber threat, scant attention has been devoted to either decision making or strategic cyber defense training during a cyber attack when decision-critical portions of cyberspace have been compromised. We can prepare for and to some degree prevent the disruption caused by a strategic cyber attack by exposing decision makers to simulated strategic cyber attacks as well as by pursuing new strategic defense technologies with the intent of improving decision maker situational awareness during cyber attacks.

Situational Awareness

The unique peril posed by cyber attacks arises from the use of information technologies, including computers, software, networks, and sensors in the network-centric warfare (NCW)/data-centric warfare (DCW) paradigm.[7] NCW/DCW leverages data and the other elements of cyberspace to improve operational performance and outcomes. The improvements in shared situational awareness and group decision making provided by NCW/DCW capabilities reduce information uncertainty between and among decision makers.[8] These two significant advantages provide a detailed, shared, composite insight into the state of the conflict. The cyberspace elements that support NCW/DCW are the only way to achieve the timely, accurate decisions needed in current and future cyber conflicts. A strategic cyber attack undermines the data and other cyberspace elements used for decision making and impairs development of individual and group situational awareness. The vulnerabilities exploited by a tactical cyber attack in support of a strategic cyber attack are inherent to the technologies used to achieve the advantages provided by modern cyberspace technologies. The advantages offered by cyberspace technologies make them profitable targets. A strategic cyber attack can prevent valuable data from reaching decision makers, corrupt decision-relevant data, corrupt decision-support systems, and corrupt the other elements of cyberspace. However, it is not the corruption of the cyberspace elements that is a concern; it is the corruption of decision making. The rise of modern computing and networking technologies has given rise to the expectation that correct individual and shared situational awareness will develop and facilitate decision making. The rapid acquisition of individual and group situational awareness can enable a faster, coherent response to evolving circumstances. A strategic cyber attack adversely affects group and individual situational awareness.

Situational awareness is the result of a dynamic process of perceiving and comprehending events in an environment.[9] It enables reasonable projections of how the environment may change and permits predictions concerning future circumstances and outcomes. The process (see fig.1) bears some similarity to Col John Boyd's observe-orient-decide-act (OODA) loop formulation for situational awareness.[10] The components of the process are not stages, but instead are interlocking cycles that progress in relation to each other using an action progression schema. The factors promoting individual SA are both structural and situational.

Structural factors include background, training, experience, personality, interests, and skill. Situational factors include the mission that is being performed and the circumstances at the time of the mission. Structure and situational factors affect situational awareness as illustrated in figure 2.

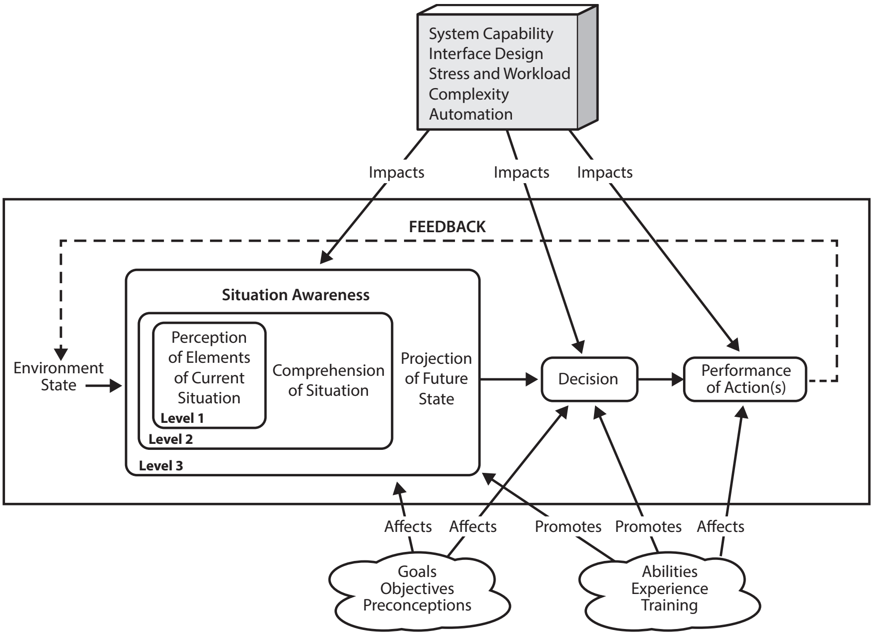

Figure 1. The situation awareness cycle
(*Adapted from* Mica Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 [1995])

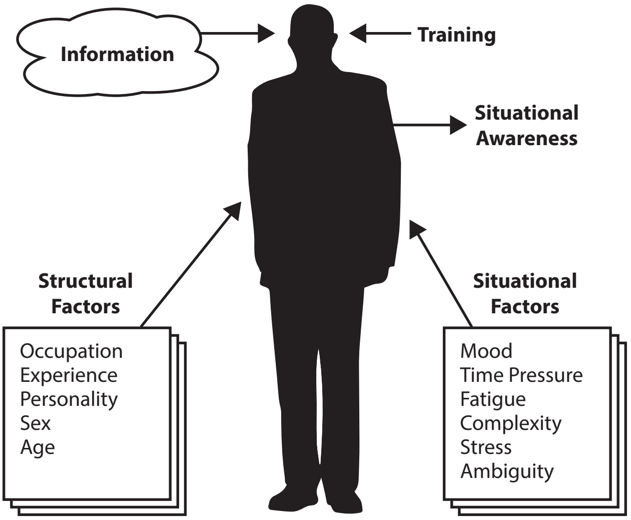

Figure 2. Situation awareness formation

Shared (or group) SA can be defined as a common relevant mental model of an environment or as the degree to which an individual's perception of the environment mirrors the same situation as perceived by others in the group. Achieving shared SA benefits from cyberspace dominance and an interoperable information representation, both of which demand an effective strategic and tactical cyber defense. Group SA ensures that a clear and accurate, common, relevant picture of the situation is possessed by leaders at all levels. Shared situational awareness requires 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.

There are many factors that are known to degrade shared SA across a group: (1) false group mind-set, (2) the "press on regardless" mind-set (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 set of information across a group, and (9) the absence of nonverbal cues. In general, physically distributed workers have poorer shared SA than do collocated workers, a problem that is exacerbated by the tendency to rarely discuss contextual information among distributed workers.[11] A modern, well-planned strategic cyber attack will assuredly target and undercut both individual and shared SA by magnifying the impact of one or more factors that degrade both. In light of these and other foreseeable developments in tactical cyber-attack capabilities, we suggest that the current *static defense-in-depth* best practice for tactical cyber defense is becoming outmoded and unviable in the face of foreseeable tactical cyber-attack capabilities. To enable an effective, flexible strategic cyber defense, a transition to a tactical cyber defense based upon an *active*, *dynamic layered cyber defense-in-depth* is necessary.

Diminishing Cyber-Attack Effectiveness through DLCD

Dynamic layered cyber defense-in-depth requires active tactical cyber defense of data and other cyberspace elements in a manner that provides rapid and robust response to a cyber attack by isolating the infected systems as they are detected and augmenting the tactical cyber defense of uninfected systems to prevent the spread of the malware infestation and to preserve cyberspace elements' value. The key to deploying effective, mutually supportive, and coherent dynamic, active defense-in-depth lies in continuous, rapid analysis of the status and quality of the protection for cyberspace elements and systems and using the resulting evaluation to immediately alter and improve tactical cyber defenses for the targeted data and systems. However, since there can and will undoubtedly be multiple infestations and multiple cyber-attack campaigns mounted at the same time, the ability to successfully wall off multiple infestations and deploy multiple, independent defensive rings around uninfested cyberspace elements (and their components) are needed. Data valuation and cyber-attack categorization are essential to the success of this approach because the value of the threatened data should determine the resources dynamically devoted to cyber element's defense.

Fundamentally, every cyber attack has as its primary objective control of the defender's cyberspace elements (typically data) by either the execution of the attacker's computer instructions upon the defender's computational resource(s) or the execution of the defender's high-privileged instructions upon the defender's computational resource(s) using parameters chosen by the cyber attacker. We can restate these objectives as either executing attacker's instructions upon the defender's computer's "bare metal" or executing privileged defender system commands using the attacker's input values. Logically, the primary objective of the tactical cyber defense must be to prevent achievement of both objectives. In practice this has been difficult for the tactical cyber defense due to the traditional emphasis placed upon computational throughput and efficiency and the resulting reliance upon perimeter tactical cyber defenses. The emphasis has become self-defeating, because it enables tactical cyber-attack success, promotes strategic cyber-attack success, and leaves the defender vulnerable to poor situational awareness and the inevitable surprises that are a consequence of poor SA.

Strategic cyber defense should have as its objectives preventing penetration of the tactical cyber defenses, and in the event of penetration, preventing the attacker from determining the cyber terrain, preventing the attacker's malware from executing, and if the malware executes, preventing it from accessing its target and/or communicating. While these objectives are pursued somewhat in current tactical cyber-defense technologies, the first objective listed receives the greatest emphasis, and a successful penetration usually results in a successful cyber attack. The strategic cyber defensive need is to dramatically increase the ability to achieve these objectives while maintaining flexibility and robustness in response to a cyber attack.

Because any static layered tactical cyber defense can be defeated, a DLCD must be able to change any aspect of its configuration at any time. By doing so, a DLCD (1) makes defeating a tactical cyber defense configuration as difficult as possible, (2) provides cyber defenders with a tactical cyber defense environment whose defenses can be dynamically altered, (3) provides the cyber defenders with tools for rapid detection of tactical cyber attacks, (4) enables cyber defenders to successfully operate despite a breach in tactical cyber defenses, (5) provides an environment that enables rapid recovery from tactical cyber penetration and compromise, and (6) eliminates any advantage a tactical cyber attacker may have due to transitory knowledge of some aspect of the tactical cyber defenses.[12] To complement these objectives, we rely on principles of cyber security,[13] employ state-of-the-art tactical cyber security technologies, and require a means for identifying, modeling, and prioritizing the key components of each element of cyberspace in any decision context.

Current strategic and tactical cyber-defense technologies give the defender control of the cyber terrain, allowing the cyber defense to determine the conditions of engagement in a cyber attack. Some current tactical cyber-defense technologies, like application control and address space randomization, can be effective in preventing some unauthorized applications from executing and in preventing access to some dangerous URLs, but current tactical cyber defense technologies are static and not completely effective. DLCD appears to be more promising and effective. Using DLCD, the cyber defender can erect an ever-varying maze of tactical cyber defenses based on virtual machines, each with a different combination of properties and operational characteristics that serve to complicate the tactical cyber-attackers' challenge. Examples of the tactical cyber defenders' control include but are not limited to halting computing processes, migrating computational processes from a compromised computational environment to a secure one, changing network communications ports and addresses, changing M2M authentication codes and encryption keys, changing virtual machine configuration and nesting, purging software, engaging additional firewalls, altering firewall properties, altering applications, altering authentication protocols, and/

or disconnecting portions of the defended system from the Internet. The challenge posed to the tactical cyber attacker can be further complicated if the cyber defender feeds false information concerning the state of the tactical cyber attack back to the cyber attacker, which can be very effective because the cyber attacker almost always lacks a noncyber information channel to ascertain the accuracy of the information.

Nevertheless, as of this writing, tactical cyber defensive changes must be implemented before, not during, the cyber engagement, thereby forfeiting a tremendous advantage possessed by the tactical cyber defense. Altering the tactical cyber defense during the attack as well as controlling the tactical cyber-attack information received by the attacker would amplify the tactical cyber defense's advantages and diminish the effectiveness of the tactical cyber attack, which is the reason for the use of DLCD. The layers in DLCD do not correspond to layers of security but rather to layers of independent virtual machines that an attacker must navigate to penetrate a system and to exploit a successful tactical cyber attack. Diminishing the effectiveness and ease of tactical cyber attacks minimizes the opportunity for surprise, minimizes the exploitation of surprise, and improves protection and employment of the four elements of cyberspace by the cyber defense. Altering the cyber terrain by using DLCD complicates the tactical cyber attackers' ability to assess the progress of the attack and decreases their ability to achieve attack objective(s). By increasing the rate at which the cyber terrain changes using DLCD, the tactical cyber defense could force the attacker to adapt so frequently and to be so uncertain of the information coming back that the tactical cyber attack's chances for success significantly diminish. In the next section we further discuss DLCD operation.

Active Cyber Defense

Traditionally, the principles for securing cyber systems include (1) the system must be substantially undecipherable, (2) the system must not require secrecy and can be stolen by the enemy without causing trouble, (3) the system must be easy to change or modify at the discretion of the correspondents, and (4) the system must be easy to use and must neither stress the mind nor require the knowledge of a long series of rules. These principles have been employed to a degree since the earliest research in computer security.[14] In the cyber-security systems context, these principles demand (1) the tactical cyber attacker cannot determine the tactical cyber defenses before or during the cyber attack, (2) possession of a system that implements the tactical cyber defenses provides no insight into the tactical cyber defense configurations of similar systems, (3) the tactical cyber defenses must be easy to change at any time by the cyber defenders, and (4) the tactical cyber defenses are essentially invisible to people that have no cyber-security responsibilities. The need for dramatic improvement in tactical cyber defense points to the need for DLCD. DLCD implements the principles by being architected and designed to isolate malware infestations, complicate the tactical cyber attacker's perspective of the cyber terrain, and maintain sufficient, accurate, and trustworthy cyberspace elements despite attack. This approach differs from current tactical cyber-defense attempts in its extreme emphasis on the four principles as the foremost property and requirement for the cyber system without regard for their impact on system performance.

DLCD also emphasizes the importance of three additional desirable properties of a cyber system: maximizing information velocity within the system when it is under attack, maximizing the objective reasons for user trust of the system and its data, and maximizing the ability of the cyber system to modify tactical cyber defenses by either increasing or decreasing their complexity and security properties. The change in properties is based upon the importance of the information being processed by the system in relation to the current decision-making context. By prioritizing the security of the cyber system, we enable the attainment of these three additional properties.

In DLCD, the outermost layer of the tactical cyber defense has access to the computing hardware; each additional nested layer further isolates the hardware from the cyberspace component, and vice-versa. The innermost layer of the DLCD defense encloses the component. Because software probes are used to instrument the operation and performance of each layer, DLCD can give decision makers sufficient time and information to recognize and counteract a cyber attack. DLCD also allows the cyber defenders to alter tactical cyber-defense complexity and configuration at any time, which further complicates the challenges posed to an attacker. We contend that human oversight and judgment is crucial to the operation of DLCD and for insuring that a cyber attacker does not trigger tactical cyber-defense responses that squander resources. As a result, while some responses in the tactical cyber defense must be automatic, the human decision makers provide overall guidance and management of the defense. Figure 3 illustrates the essence of the DLCD approach for a single element of cyberspace. Figure 4 illustrates its use for application protection.

The key to DLCD is the protection of each element of cyberspace by one or more nested Type 1 virtual machines, each operated by its own virtual machine monitor (VMM) using different configurations.[15] Each virtual machine provides a layer of cyber-defense protection, having its own set of virtual machine (VM) properties and traditional tactical cyber defenses, as illustrated in figure 3. Additional virtual machines are added to the layered protection as warranted by the threat and importance of the component in the current decision context. End-to-end security within the DLCD environment is accomplished along the lines described by Cricket Liu and Paul Ablitz in *DNS and BIND*.[16] For example, communication between virtual machines must be secure and reliable. Therefore, data is encrypted before transmission between virtual machines or between applications. Secure communication is enhanced using virtual private network (VPN) technology to secure interprocess communication within the computer system. Issuing virtual machines and authorized applications a digital certificate for authentication provides additional security. Defensive tactical cyber security is further improved by using DNSSEC and IPSEC for communication within and between layers and IPv6 addresses to identify individual applications and virtual machines (IPv6 addresses are not shared or inherited).[17] The combination of VM with other tactical cyber-defense technologies enables secure, dynamic alteration of the defensive cyber terrain that the attacker must overcome to achieve cyber-attack objectives.

By using multiple nested virtual machines and other cyber-defense technologies to protect the elements of cyberspace, DLCD supports dynamic allocation of tactical cyber-defense resources by enabling the addition of virtual machines to the layers of protection of an element or component, by altering the mix of VM types and configurations, or by changing tactical cyber-attack detection systems within each VM without altering or influencing the other VMs or cyberspace elements within a system. Using DLCD, the defensive cyber terrain can be altered in a significant, useful, unpredictable manner that cannot be detected or prevented by the cyber attacker or by malware that has breached the system's defenses. DLCD presents tactical cyber attackers with a reconfigurable maze that they must continuously solve to penetrate defensive cyberspace and exploit a penetration. Note that for each VM layer added to protect a component or an element, the poorer the performance of the enclosed element or component, which inevitably degrades the utility of the cyberspace element or component for broader mission accomplishment. It is therefore vital that decision makers alter protection only in response to actual threats against cyberspace resources; otherwise the performance of the elements and components can be degraded to such a degree that they lose utility for a decision maker. The complexity of the tradeoffs between element security and timeliness is the basis for our contention that humans must manage tactical cyber defenses even though rapid responses must be executed by intelligent systems.

By using a multilayered, nested virtual machine approach (figs. 3 and 4) as the basis for DLCD, the tactical cyber defense can respond to a tactical cyber attack while the attack is in progress. A dynamic layered tactical cyber defense based upon nested VM technologies can effectively protect the four cyberspace elements.

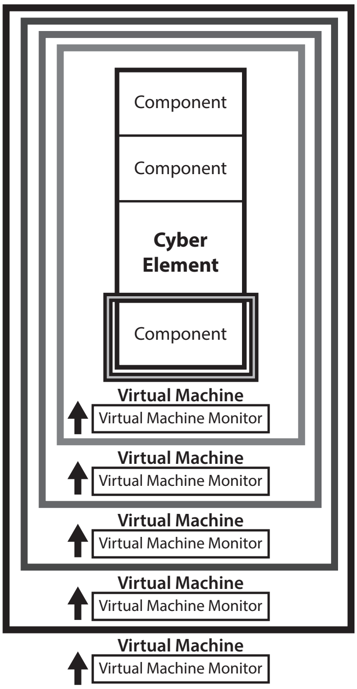

Figure 3. Nominal dynamic layered cyber defense architecture for an element showing VMM placement

The importance of timely and accurate delivery of cyberspace elements to decision-making success is hard to overstate.[18] Delay leads to failure to gain or maintain situational awareness, to failure to make decisions, and to incorrect decisions. The need to share some portions of each cyberspace element to develop and maintain group SA further compounds the challenge of timely and accurate delivery, because in modern conflict there are generally many decision makers involved in the assessment and decision process for each decision, as envisioned in the JIE. While cyberspace elements increase in value when shared, the sharing process also increases the vulnerability of the element and of the decision-making process. As a result, when decision makers are assessing tactical cyber-defense approaches, they must not only consider how best to protect the elements that are crucial to the current decision context, but also how to protect the elements and components delivered to all others involved in the same decision. The tactical cyber defense challenge is increased by the variability in the elements and components of cyberspace across different decisions, by the variability in the ability of a cyberspace element or component to decrease uncertainty, by the differences in the tolerances of elements, components, and decision makers to risk, and by varying perceptions of the importance of each decision within the evolving situation.

The well-known difficulty of cyberspace element value assessment, especially data, is increased when the number of decision makers using the same elements increases. The clear solution to the problem is to assess cyberspace element and component value in a variety of situations and use these valuations as guides to cyber-defense action during attacks. We can conduct cyberspace element and component value assessments by monitoring the protection choices and cyberspace element usage choices made during decision making in a simulation environment. To make the assessment, we assume that the relevant cyberspace elements and components employed for the decision are important and that the other cyberspace elements and components that are not considered are not as important in that particular circumstance. Nevertheless, the cyberspace elements and components not employed in a decision must be protected to a degree. Human participation is crucial in making and revising element and component priorities for tactical cyber defense because of the complexities involved when making priority assessments. The simulation-derived priorities can be used to guide decision-maker cyberspace element and component tactical cyber defense choices during real-world cyber attacks.

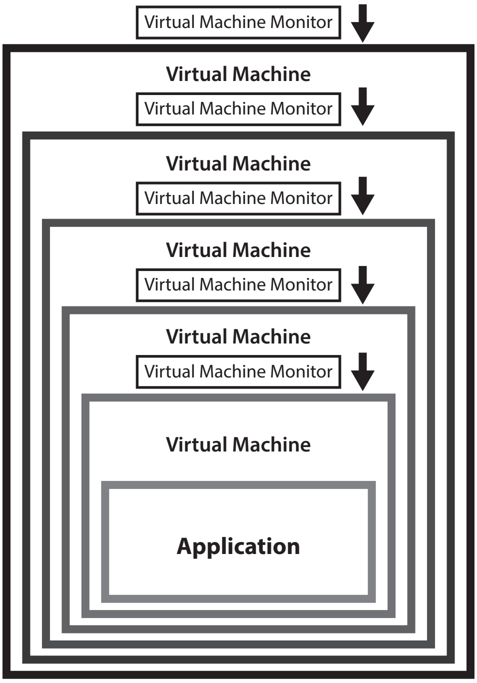

Figure 4: Using nested virtual machines to protect an application in DLCD

Training Cyber Defense

As cyber attacks increase in technical sophistication they can increase their ability to target specific information, data, and physical resources, which can be disorienting. Even an attack that does not disorient users can still produce confusion, which in turn decreases group SA, individual SA, and decision-making quality. The inevitable result of increased technical sophistication by cyber attackers is improvement in their ability to cloud situation awareness, disrupt decision dissemination, and prevent accurate feedback. Preparation for decision making during a cyber attack requires training to prepare for a cyber attack's psychological, SA, and decision-making challenges coupled with the tools for information analysis and management needed to help decision makers evaluate the information available to them, assess the trustworthiness of the information, and develop situational awareness. The pursuit of cyberspace

SA is crucial to securing cyberspace and to attaining SA in the other parts of the conflict—air, ground, sea, or space. Because cyberspace SA for both individuals and groups of decision makers is vital, developing training environments for decision makers and strategic cyber defenders to provide experience and expertise in addressing cyber attacks and their attempts to undercut SA is imperative. The needs of the strategic cyber defender are clear: strategies that protect elements and their components when under cyber attack while ensuring decision makers have the components of the cyberspace elements they need.

In light of these complementary requirements, strategic cyber defender and decision-maker training must address two needs. *First*, to prepare defenders and decision makers for the confusing, contradictory, and misleading cyberspace elements present during a cyber attack. Training can prepare them to cope with the psychological stresses caused by variations in cyberspace element availability and quality. A key aspect of this training must be learning to assess cyberspace element value, both as it relates to the value (importance) of available elements in relation to current decisions as well as relative to the value of the elements compromised. Decision makers must learn that cyberspace element value is not correlated with security classification. The defenders also need to evaluate effectiveness of various strategies to counter cyber attacks and campaigns. The *second* need is to prepare decision makers to exploit cyberspace dominance via effective employment of trustworthy data analysis/comprehension (such as analysis based upon big data) and data interaction/management technologies. Analysis, comprehension, and interaction must be performed, in part, automatically due to the volume of data available. Nevertheless, decision makers must learn how to navigate cyberspace, how to use visualizations as viewports into critical portions of cyberspace, how to compare and compose visualizations to provide needed insights, how to identify and exploit key data, and how to coordinate their navigation, analysis, and comprehension efforts despite cyber attacks designed to undermine these efforts.

The challenges posed to strategic cyber defense in addressing these two needs are significant, because achieving and maintaining broad-spectrum defensive cyberspace dominance is increasingly difficult and unreliable due to improvements in tactical cyber-attack technologies. The crucial challenge in strategic cyber defense lies in determining which defense to employ in light of which elements require improvement in tactical cyber defense and which elements are adequately defended in the current decision-making context. Because of the volume of data that must be considered and the rapid pace of activity, the strategic cyber defender as well as the decision maker must be prepared for the confusing and novel information circumstances they will encounter. Exposure to simulated cyber attacks can prepare the strategic cyber defender to accomplish proper assessment of cyber circumstances and to select the most advantageous strategic and tactical cyber defense responses to cyber attacks.

Preparation of strategic cyber defenders is critical because instinctive behaviors exhibited in the face of uncertainty are invariably incorrect and counterproductive. Under stress, instinctive behaviors are adopted. Stress-induced behaviors lead to the use of emotional bias to make decisions (making the decision that enables the person *feel* that a more positive outcome is likely), to expectation bias (the expectation that the things the person *wants* to happen will happen), to loss/risk aversion (the tendency to value choices that *seem* to minimize risk and loss in spite of any evidence or data to the contrary), and to the adoption of the sunk-cost fallacy (wherein the tendency is to *continue* an action because the decision maker believes the situation will not get worse or because the decision maker has a vested emotional and ego interest in continuing the same course of action). Finally, instinctive behaviors may also lead to past-fixation (the tendency to make decisions based on the expectation that conditions that existed in the past *will recur* despite the fact that they can never recur). Countering instinctive, counterproductive behaviors is difficult and should be one of the main concerns of strategic cyber defense training via simulation.

The tools and training required by strategic cyber defenders and decision makers to prepare them for the challenges of cyber conflict must address three classes of cyber situations: operations during normal conditions, operations during a cyber attack, and operations after a cyber attack.[19] The training, techniques, and tools that are vital in these three circumstances can be developed using simulation environments designed to provide the following capabilities: (1) improve understanding of the challenges posed during a cyber attack, (2) test and evaluate cyber defense tools, techniques, and training, (3) practice using cyber defense tools and techniques to acquire expertise, and (4) assess cyber element value during a wide array of circumstances to determine how best to deploy cyber defenses. The tools, techniques, and training must be extensive and flexible so they can be readily altered to address new cyber threats and tactical cyber attacks as they arise or become possible.[20]

Training Cyber Defense through Simulation

Cyber-attack simulation is the only means to prepare decision makers for the complexity of the inevitable attacks upon cyberspace elements. It is the best means available to determine the strategies to be used to secure the critical elements of cyberspace in support of the decision makers' needs.

Simulation provides a safe and flexible way to prepare strategic cyber defenders and decision makers for the challenges faced in a cyber attack as well as for assessing cyberspace element protection techniques and defense strategies. Cyber-attack simulation can provide an environment that allows decision makers and strategic cyber defenders to practice so that their decisions and activities in the real world will produce an effective strategic cyber defense, adequate SA, and effective decisions. To scale as technologies evolve, cyber-attack simulation must portray attack and defense actions in a manner that corresponds to how these actions are perceived by humans, even as the attack proceeds and defenses succeed or fail in the simulation environment. To achieve these goals, the cyber simulation environment must capture and represent the activities of the decision makers and strategic cyber defenders, the attacker and defender goals, the sequence of operations the attacker will execute, the activities of the tactical cyber defense, logical and physical data location(s), and the potential responses of the attackers and defenders to each others' actions. In previous works, we described cyber-attack simulation techniques that can be used to model cyber operations, their components, and possible responses to defensive actions.[21]

The simulation of cyber attacks presents a number of analysis and assessment challenges, all of which concern determining the status and importance of the cyberspace elements available to decision makers. Previous studies of the importance of data to decision making as well as the challenges posed by contradictory or confusing data can be used as a basis for determining how to alter cyberspace elements and their components in response to a simulated cyber attack. To simulate a cyber attack, we need only affect the cyberspace elements available to users;

we do not need to infect or corrupt computers or their software. For realistic simulation, the stimuli and cyberspace elements provided to decision makers must contain the noise, discontinuities, and errors of the type that would be caused by the actual cyber activity so the decision maker and cyber defenders are accustomed to cyber attacks as they might unfold in the real world. The same simulation environment can be used to assess cyberspace element value and to develop procedures for continuing operations in the face of cyber attacks.

Four simulation goals are necessary to prepare decision makers and cyber defenders for cyber attacks. *First*, teaching them how to determine the targets of cyber attacks. *Second*, teaching them the techniques and tactics likely to be used against targets. *Third*, teaching the decision makers and cyber defenders the effects of each type of attack and the techniques and tools that should be used to counteract each type of cyber attack. *Fourth*, teaching them the means for explicitly assessing cyberspace element value and deploying cyber defenses to protect the highest value information. An additional consideration for defenders is exploring strategies and tactics to assess their usefulness. Cyber simulation can achieve these goals. To minimize the development cost of simulation environments, current simulation systems can be coupled with cyber simulation systems, as illustrated in figure 5. The scenarios to be executed in the cyber simulation are described using the Unified Modeling Language (UML).[22] To create realistic cyber simulation environments, the components of the cyber simulation environment must exchange information about the cyber attack and cyber defense, the status of the cyber event, and portray the results of the cyber attack and defensive responses.

The key to this approach is recognizing that simulating a cyber attack only requires affecting the information presented to the users in the simulation environment. Therefore, to prepare for the SA and decision-making challenges faced during a cyber attack, only the presentation of the cyberspace elements must be altered; the “true” elements and their values need not be altered. Three approaches are available to affect element presentation: increase the amount of information presented via an element, block information needed by a user that is provided by an element, and substitute false information for the actual information presented via an element. For example, a user can be given an overwhelming amount of data, denied data, or given a mixture of accurate and false data. Other techniques that can be used to simulate a cyber attack are: instructing every simulation host to replicate every message received at the host but with the number of messages received changed by a random but small amount, instructing every simulation host to duplicate the same information in numerous windows, or instructing every simulation host to remove random words from each message. The effects of these simple measures can be compounded if false messages are repeated at random time intervals after the first receipt of the message.

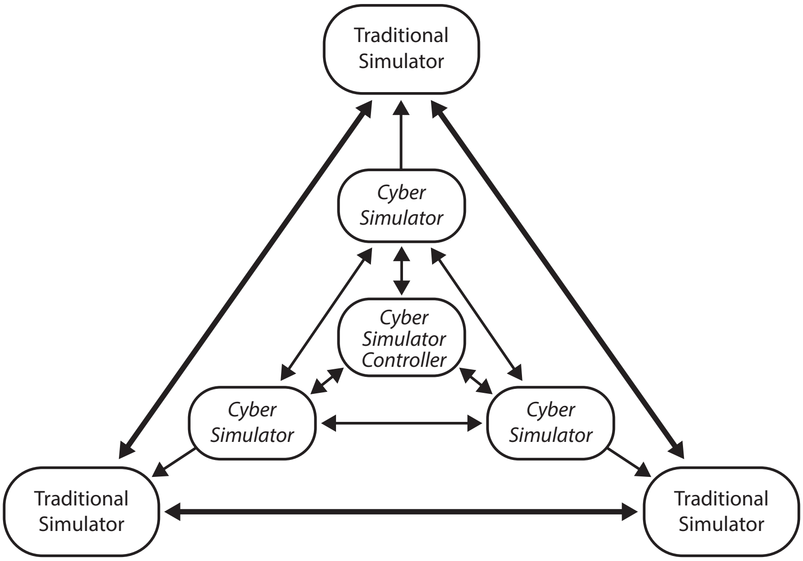

Figure 5. Conceptual cyber simulation environment

A cyber training simulation environment (see fig. 5) must accomplish three tasks to achieve its training goals: determine if a simulated cyber attack is successful, determine the effect of the simulated cyber attack upon each host and its data, and portray simulated cyber defensive responses to the simulated attack. In the illustrated approach, each host has a cyber simulator that services the host and provides these three capabilities. The cyber simulator provides each host with inputs needed to portray the effects of simulated attacks and defense responses. The simulation systems communicate with each other using a logically separate cyber simulation network to achieve a consistent cyber state across the simulation environment.

At each step of the cyber attack and cyber-defensive response, the simulation environment must provide appropriate, realistic indications of the status of the attack and cyberspace elements status/values so they reflect the delays and alterations that would occur in the corresponding real-world cyber attack. For example, changes in the tactical cyber defense that increase or decrease the depth of defense would be reflected in increased or decreased delays in data transport. The simulation architecture allows cyber defenders to alter the types and configurations of the tactical cyber defense at any time. As a result of exposure to a realistic cyber defense and attack environment, the defender and decision maker can experience the effects of their defensive choices and experiment with dynamic techniques.

An example scenario illustrates how the cyber simulation environment can be used to prepare decision makers and strategic cyber defenders for attacks. The cyber simulation environment could be tasked to provide experience in using information analysis and navigation technologies to detect the presence of a botnet. The botnet detection methods introduced could include analysis of specific network and/or cloud traffic flows, analysis of aggregate network and/or cloud traffic data, variations in data volume, variations in network traffic sources and destinations, and other atypical behavior. The training environment would prepare the decision makers and defenders for the real world where one indicator of infection is not enough. In practice, confirmation of a botnet infection requires multiple indicators to achieve robustness of confirmation by providing both the ability to corroborate data of dubious or variable dependability and minimize the false alarm rate.

In figure 6, "protection" or "value" rings are used to prioritize the four cyberspace element components. The rings correspond to the value and priorities assigned to each cyberspace element's protection. For the strategic cyber defender, the ring model can be used to guide resource allocation as well as decisions to isolate systems or subsystems that are compromised. In the ring-modeling approach, the closer the rings are to the center, the greater value, importance, and usefulness (of that cyber element) is in the decision context. The number of rings and the content of each ring are determined by the decision-making context. As a result, the number and content of rings for each element vary dynamically. We use one set of rings for each of the four elements. Each cyberspace element ring contains components of approximately the same importance for that element in a decision-making context. The ring model also serves to simplify the cyber-attack simulation challenge. To simulate an attack within a decision-making context, we affect the elements and components needed in the decision context by simulating the modification of the content of the specific rings for those elements of defensive cyberspace that are compromised. The decision, type of cyber attack, the tactical 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 element's components that are altered.

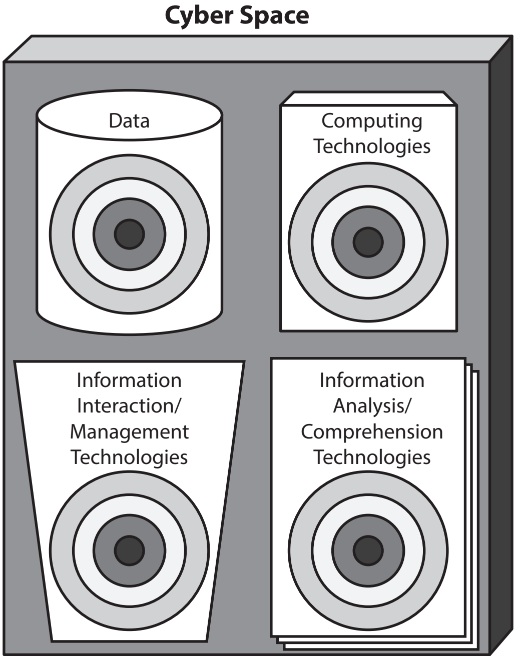
Cyber Space
Data
Computing Technologies
Information Interaction/ Management Technologies
Information Analysis/ Comprehension Technologies

Figure 6. Framework for modeling relative importance of the components of cyberspace elements

A cyber simulation training environment can prepare decision makers to proactively alter tactical cyber defenses, prioritize data, prioritize the elements of cyberspace, and operate during a strategic cyber attack wherein some cyberspace elements and components are compromised to an uncertain degree.

The simulation approach described above allows us to address the four decision-maker and cyber defender training considerations with minimal risk to real-world cyberspace coupled with high fidelity in the cyberspace simulation environment. The simulation problem that remains is determining cyberspace metrics for assessing both simulated and real-world cyberspace status and for developing situational awareness. Cyberspace metrics must provide insight into cyberspace state, cyber-attack attempts, cyber-attack targets, the degree of a cyber attack's success, and the effectiveness of deployed cyber defenses at the element and component levels.[23]

Summary and Open Issues

Cyber dominance has one goal, the command of cyberspace elements. While decision makers implicitly expect cyberspace dominance, it is not assured in light of current tactical cyber-attack technologies and tactical cyber defense technologies. Achieving cyber dominance will not guarantee victory for a data centric force; however, the lack of cyber dominance will almost certainly ensure its defeat. Any approach to cyber dominance must possess two crucial traits: the approach must enhance defensive cyber security and maintain system reliability during cyber attack. The approach described above for achieving defensive cyber dominance calls for DLCD coupled with simulation training to assist decision makers and strategic cyber defenders. It can provide experience needed to allow decision makers to operate within a compromised defensive cyber environment and to identify, analyze, and predict the objectives and presence of cyber attacks. The same approach also permits the development and evaluation of strategic cyber defense options to employ against various cyber attacks and campaigns. The approach complements the JIE or similar dataflow architectures and their tactical cyber defense technologies.

As cyber technologies improve, the challenges to achieving cyber dominance will increase. Additionally, the intricacy of future cyber systems and cyberspace will increase, as witnessed by the development of intercloud technologies, "smart grid" technologies for remote control and management of real-world infrastructure (SCADA systems),[24] IPv6 deployment, and the "Internet of Things."[25] We expect that the increasing power of computing technologies and the increasing complexity of tactical and strategic cyber attacks will compound the difficulties posed to the cyber defender and create new pathways for executing cyber attacks.

Preparation for future cyber attacks requires the development of training systems that impart the experience and expertise needed to make effective strategic and tactical cyber defense possible. While the requisite training systems can now be deployed, before an all-inclusive cyber simulation environment can be fielded for training purposes, further research and development to advance cyber battle understanding, human behavior modeling, intent inferencing, information display, data mining, and decision making during cyber conflict and strategic cyber defense must be conducted. An additional important area of investigation is gaining 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. The required research in high-data-volume environments lies at the intersection of machine learning, data mining, game theory, large-scale data analysis, and SA development technologies. A final area of further research is assessment of the effectiveness of tactical cyber defense options best suited to achieve each desired cyber-defense strategy.

While deception and information denial operations are as ancient as warfare itself, technically sophisticated cyber attacks permit, for the first time, a wide-scale, persistent, and virtually undetectable attack upon the data, tools, and other elements of cyberspace that a decision maker routinely employs. The technically sophisticated cyber attack of the future will destroy or corrupt data, surprise decision makers, generate confusion, delay response, and greatly increase what Clausewitz calls the "fog and friction" in war. Because cyberspace will be contested, decision makers must be prepared for strategic cyber attacks designed to undermine their decision-making ability. To be unprepared for the effects of a strategic cyber attack is to remain in needless peril. In the future, addressing the strategic cyber-attack challenge will become more, not less, critical to success.[26]

Glossary

cloud computing—a model for enabling ubiquitous, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

component-level metrics—measure the performance of specific characteristics of a cyberspace component. Example components include (1) the number of page swaps per time interval in each virtual machine, (2) the average elapsed time before a page is swapped in a virtual machine,

(3) average elapsed time to migrate a virtual machine from one host to another, and (4) the average time to execute RC4 encryption a set number of times on a specified clear text input among different virtual machines and others.[27]

cyber attack—an application of cyber security technologies within cyberspace with the intent of degrading an adversary's data, computing technologies, information analysis/comprehension and/or information interaction/management capability to one's advantage.

cyber defense—the application of cyber security technologies to protect one's portion of cyberspace to secure data and computing technologies as well as protect information analysis/comprehension and information interaction/management capabilities.

cyber security technologies—the subset of computing technologies used either to protect one's own data, information analysis/comprehension technologies, computing technologies, and information interaction/management technologies or to undermine those of an adversary.

cyberspace—composed of four 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 (including information visualization, artificial intelligence, collaboration, data mining technologies, and big data technologies), and (4) information interaction/management technologies (including human-computer interaction, intelligent agents, human intent inferencing, and database technologies).

digital certificate—a signed public key. A trusted authority signs the digital certificate before it is issued.

DNSSEC (Domain Name System Security Extensions Convention)—a set of Internet engineering task force (IETF) specifications for securing certain kinds of information provided by the Domain Name System (DNS) on Internet protocol (IP) networks. A domain name server manages the domain names repository and provides name resolution for an internet zone. The DNSSEC specifications are covered by Request for Comments (RFC) 4033, 4034, 4035, and 3833 at http://www.ietf.org/rfc.html.

exploit—software that attacks a cyber security vulnerability.

(human) intent inferencing—an artificial intelligence-based technique used to provide an intelligent user interface in which the goals of the user are deduced based upon a history of user actions and a computable representation of the current mission.[28]

information stream—a logical path through the architecture from an information source to a designated information sink.

IPSEC (Internet Protocol Security) is a set of protocols for securing IP communications at the network layer, layer 3 of the OSI model, by authenticating and/or encrypting each IP packet in a data stream. IPSEC includes protocols for cryptographic key establishment.

intercloud—a model for computing based on a cloud composed of computing clouds.

malware—software used to disrupt computer operation, gather sensitive information, or gain access to private computer system. It includes computer viruses, ransomware, backdoors, worms, Trojan horses, rootkits, spyware, rogue security software, and other malicious software. The type of malware is classified based on how it is executed, how it spreads, and what it does. A **virus** is malware that can execute itself by placing its own code in the execution path of another program and can replicate itself by replacing existing computer files with copies of itself. A **Trojan** is a hidden program that masquerades as a benign application. A **worm** does not require a host program to propagate but enters a computer through a weakness in the computer system defenses and propagates using network traffic security flaws. A **backdoor** is software that allows access to the computer system by bypassing normal authentication procedures.

rootkit—malware that hides traces of an attack, installs Trojans and backdoors, provides the attacker with root control of the system, and enables further malicious activity.

situational awareness (SA)—"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."[29] 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). These stages are similar to but not identical with Boyd's observe-orient-decide-act (OODA) loop construct.[30]

smart grid—employs computer-based remote control and automation on all elements of electrical power delivery to optimize electrical power generation and distribution.

software gauge—software that converts data collected by a software probe into a measure that is meaningful for a particular system for the purpose of performance tuning, information assurance, functional validation, compatibility, or assessment of operational correctness.

software probe—software that interacts with an operating system, operational application, or subset of an application to collect data for a gauge(s).

virtualization—a technique for emulating a computing resource and for hiding the physical characteristics of computing resources from the systems, applications, or end-users that interact with those resources. Virtualization exploits virtual machine technologies. Virtualization technologies provide six key benefits: (1) efficient use of computing resources, which reduces information technology infrastructure and environmental (power, cooling, and real estate) requirements; (2) fault isolation in which an application error, operating system crash, or user error in one virtual machine will not affect the use of other virtual machines on the same system; (3) increased security where vulnerabilities or exploits can be contained and quarantined in a single virtual machine without affecting the entire system; (4) rapid provisioning through file copy or volume cloning used to rapidly create new virtual machines; (5) flexibly in managing change to include the ability to scale according to the demand for services, unique operating systems, and service provisioning; and (6) portability through the abstraction of devices combined with the encapsulation of virtual data in virtual disks. Virtualization is a key technology for cloud computing.

Additional definitions are available at http://www.sans.org/security-resources/glossary-of-terms/and http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf.

Notes

[1] For our purposes, the four elements (or aspects) of cyberspace are (1) data, (2) computing technologies, (3) information interaction and management technologies, and (4) information analysis and comprehension technologies.

[2] Chris Buckley, "China PLA Officers Call Internet Key Battleground," Reuters, 3 June 2011. Senior Col Ye Zheng and his colleague Zhao Baoxian, stress in *China Youth Daily* the importance of China's cyber warfare capabilities, concluding that "just as nuclear warfare was the strategic war of the industrial era, cyber-warfare has become the strategic war of the information era, and this has become *a form of battle that is massively destructive and concerns the life and death of nations*." See also R. A. Clarke

and R. Knake, *Cyber War: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010); A. F. Krepinevich, *Cyber Warfare: A Nuclear Option?* (Washington: Center for Strategic and Budgetary Assessments, 2012); Gen Keith Alexander, *Testimony before the House Armed Services Committee*, 23 September 2010; D. E. Geer and J. Archer, "Stand Your Ground," *IEEE Security and Privacy* 10, no. 4 (2012): 96; "Panetta Warns of Dire Threat of Cyberattack on U.S.," *New York Times*, 11 October 2012; and B. H. Liddell Hart, *The Revolution in Warfare* (New Haven, CT: Yale University Press, 1932), 121.

[3] This and other terms are discussed in a glossary at the end of the article.

[4] Val Smith and Chris, "Why Black Hats Always Win," *Blackhat.com*, January 2010; Joanna Rutkowska, "Subverting Vista Kernel for Fun and Profit," Black Hat USA, July 2006; J. Levine, J. Grizzard, and H. Owen, "Detecting and Categorizing Kernel-Level Rootkits to aid Future Detection, *IEEE Security and Privacy* 4, no. 1 (January/February 2006): 24–32; Rutkowska, "Rootkit Hunting vs. Compromise Detection," Black Hat Federal 2006, Washington, DC, 25 January 2006; A. Lakhotia, "Analysis of Adversarial Code: Problems, Challenges, and Results," Black Hat Federal 2006; William J. Lynn III, "Defending a New Domain: The Pentagon's Cyberstrategy," *Foreign Affairs* 89, no. 5 (September/October 2010); A. Acquisti and J. Grossklacs, "Privacy and Rationality in Individual Decision Making," *IEEE Security and Privacy* 3, no. 1 (2005): 26–33; I. P. Cook and Pfleeger, "Security Decision Support: Challenges in Data Collection and Use," *IEEE Security and Privacy* 8, no. 3 (2010): 28–35; J. Giffin, "The Next Malware Battleground: Recovery after Unknown Infection," ibid., 77–82; K. J. Hole and L. Netland, "Toward Risk Assessment of Large-Impact and Rare Events," ibid., 21–27; J. R. Kenney and C. Robinson, "Embedded Software Assurance for Configuring Secure Hardware," *IEEE Security and Privacy* 8, no. 5 (2010): 20–26; M. E. Johnson and Pfleger, "Addressing Information Risk in Turbulent Times," *IEEE Security and Privacy* 9, no. 1 (2011): 49–58; J. Schiffman et al., "Network-Based Root of Trust for Installation," ibid., 40–48; B. Stone-Grosset et al., "Analysis of a Botnet Takeover," ibid., 64–72; P. Ning, Y. Cui, and D. S. Reeves, "Intrusion Detection: Constructing Attack Scenarios through Correlation of Intrusion Alerts," *Proceedings of the 9th ACM Conference on Computer and Communications Security*, November 2002; M. M. Pillai, J. H. P. Eloff, and H. S. Venter, "An Approach to Implement a Network Intrusion Detection System Using Genetic Algorithms," *Proceedings of the 2004 Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, October 2004; E. Skoudis and L. Zeltser, *Malware: Fighting Malicious Code* (Upper Saddle River, NJ: Prentice Hall, 2003); C. C. Zou, W. Gong, and D. Towsley, "Formation and Simulation: Worm Propagation Modeling and Analysis under Dynamic Quarantine Defense," *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, October 2003; R. Graham and D. Maynor, "SCADA Security and Terrorism: We're Not Crying Wolf," Black Hat Federal 2006; M. Jakobson and Z. Tamzan, *Crimeware: Understanding New Attacks and Defenses* (Upper Saddle River: Addison-Wesley, 2008); J. V. Antrosio and E. W. Flup, "Malware Defense Using Network Security Authentication," *Proceedings of the Third IEEE International Workshop on Information Assurance (IWIA'05)*, March 2005; J. Aycock and K. Barker, "Viruses 101," *ACM SIGCSE Bulletin: Proceedings of the 36th SIGCSE Technical Symposium on Computer Science Education* 37, no. 1 (February 2005); D. Ellis, "Formation and Simulation: Worm Anatomy and Model," *Proceedings of the 2003 ACM Workshop on Rapid Malcode*, October 2003; D. M. Kienzle and M. C. Elder, "Internet WORMS: Past, Present, and Future: Recent Worms: A Survey And Trends," ibid.; J. Nazaro, *Defense and Detection Strategies against Internet Worms* (Boston: Artech House, 2004); S. T. King and P. M. Chen, "Backtracking Intrusions," *ACM Transactions on Computer Systems (TOCS)* 23, no. 1, January 2005; C. Kruegel, W. Robertson, and G. Vigna, "Detecting Kernel-Level Rootkits through Binary Analysis," *Proceedings of the 20th Annual Computer Security Applications Conference*, December 2004; C. P. Pfleeger and S. L. Pfleeger, *Analyzing Computer Security: A Threat, Vulnerability, Countermeasure Approach* (Upper Saddle River: Prentice Hall, 2012); Pfleeger and Pfleeger, *Security in Computing*, 4th ed. (Upper Saddle River: Prentice Hall, 2007); R. Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, 2nd ed. (Indianapolis: Wiley, 2008); and M. Maras, *Computer Forensics: Cybercriminals, Laws, and Evidence* (Burlington, MA: Jones & Bartlett, 2012).

[5] Ibid.

[6] J. M. Graaido, R. Schlesinger, and K. Hoganson, *Principles of Modern Operating Systems*, 2nd ed. (Burlington, MA: Jones & Bartlett, 2013); P. A. Karger and D. R. Safford, "I/O for Virtual Machine Monitors: Security and Performance Issues," *IEEE Security & Privacy* 6, no. 5, (2008): 16–23; H. Takabi, J. B. D. Joshi, and G. Ahn, "Security and Privacy Challenges in Cloud Computing Environments," *IEEE Security & Privacy* 8, no. 6, (2010): 24–31; Qian Liu et al., "An In-VM Measuring Framework for

Increasing Virtual Machine Security in Clouds," *IEEE Security & Privacy* 8, no. 6, (2010): 56–62; R. L. Krutz and R. D. Vines, *Cloud Security: A Comprehensive Guide to Secure Cloud Computing* (Indianapolis: Wiley, 2010); A. Belapurkar et al., *Distributed Systems Security: Issues, Processes, and Solutions* (Indianapolis: Wiley, 2009); C. Cachin and M. Schunter, "A Cloud You Can Trust," *IEEE Spectrum* 48, no. 12 (2011): 28–51; and K. Jamsa, *Cloud Computing* (Burlington, MA: Jones & Bartlett, 2013).

7. D. S. Alberts et al., *Understanding Information Age Warfare* (Washington: CCRP Press, 2001); and Alberts and R. E. Hayes, *Power to the Edge* (Washington: CCRP Press, 2003)

8. Ibid.

9. Mica Endsley, "Toward a Theory of Situation Awareness in Dynamic Systems," *Human Factors* 37, no. 1 (1995): 35–64.

10. Frans Osinga, *Science, Strategy and War: The Strategic Theory of John Boyd* (Abingdon, UK: Routledge, 2005).

11. L. Ying, L. Bingyang, and W. Huiqiang, "Dynamic Awareness of Network Security Situation Based on Stochastic Game Theory," 2nd International Conference on Software Engineering and Data Mining (2010), 101–5; K. Smith and P. A. Hancock, "Situation Awareness is Adaptive, Externally Directed Consciousness," *Human Factors* 37, no. 1 (1995): 137; VADM A. K. Cebrowski, "Network-Centric Warfare: An Emerging Military Response to the Information Age," 1999 Command and Control Research and Technology Symposium, 29 June 1999, http: //www.nwc.navy.mil/press/speeches/ccrp2htm; and P. Hinds, *Perspective Taking among Distributed Workers: The Effect of Distance on Shared Mental Models of Work*, World Trade Organization Working Paper # 7 (Stanford, CA: Center for Work, Technology, and Organization, 1999).

12. Lynn, "Defending a New Domain."

13. J. H. Saltzer and M. D. Schroeder, "The Protection of Information in Computer Systems," *Proceedings of the IEEE* 63, no. 9, (1975): 1278–1308; Saltzer and M. F. Kaashoek, *Principles of Computer System Design* (Indianapolis: Wiley, 2009); R. E. Smith, *Elementary Information Security* (Burlington, MA: Jones & Bartlett, 2013); A. Kerckhoffs, "La Cryptographie Militare," *Journal Sciences Militaires* 9 (February 1883): 161–91; B. Schneier, "Secrecy, Security, and Obscurity," *Cryptogram Newsletter*, 15 May 2002, http://www.schneier.com/crypto-gram-0205.html; C. E. Shannon, "Communication Theory of Secrecy Systems," *Bell System Technical Journal*, October 1949, 656–715; D. E. Denning, "A Lattice Model of Secure Information Flow," *Communications of the ACM* 19, no. 5 (1976): 236–43; DoD 5200.28-STD, *Department of Defense Trusted Computer System Evaluation Criteria*, 26 December 1985; P. A. Karger and R. R. Schell, *Multics Security Evaluation: Vulnerability Analysis*, ESD-TR-74-193, vol. II, HQ Electronic System Division, June 1974; K. Thompson, "Reflections on Trusting Trust," *Communications of the ACM* 27, no. 8 (1984): 761–63; R. E. Smith, "A Contemporary Look at Saltzer and Schroeder's 1975 Design Principles," *IEEE Security and Privacy* 10, no. 6, (2012): 20–25; R. Smith, *Elementary System Security* (Burlington, MA: Jones & Bartlett, 2013); S. Smith and J. Marchesini, *The Craft of System Security* (Upper Saddle River: Addison-Wesley, 2008); S. Lipner, T. Jaeger, and M. E. Zurko, "Lessons from VAX/SVS for High-Assurance VM Systems," *IEEE Security and Privacy* 10, no. 6 (2012): 26–35; J. C. Wray, "An Analysis of Covert Timing Channels," *Proceedings of the IEEE Symposium on Security and Privacy*, (1991): 52–61; L. J. Fraim, "SCOMP: A Solution to the Multilevel Security Problem," *IEEE Computer* 16, no. 7 (1983): 26–34; C. Larman, *Agile and Iterative Development: A Manager's Guide* (Boston: Pearson Education, 2004); H. Shrobe and D. Adams, "Suppose We Got a Do-Over: A Revolution for Secure Computing," *IEEE Security and Privacy* 10, no. 6 (2012): 36–39; R. J. Feiertag and P. G. Neumann, "The Foundations of a Provably Secure Operating System," *Proceedings of the National Computer Conference*, 1979, 329–34; and W. H. Ware, *Security Controls for Computer Systems: Report of the Defense Science Board Task Force on Computer Security* (Santa Monica, CA: RAND, 1970).

14. Ibid.

15. R. J. Adair et al., "A Virtual Machine System for the 360/40," Cambridge Scientific Center Report 320, IBM, May 1966; G. M. Amdahl, G. A. Blaauw, and F. P. Brooks, "Architecture of the IBM System/360," *IBM Journal of Research and Development* 8, no. 2 (1964): 87–101; Paul Barham et al., "Xen and the Art of Virtualization," *Proceedings of the 19th ACM Symposium on Operating System Principles (SOSP)*, Bolton Landing, NY, October 2003, 164–77; A. Bieniusa, J. Eickhold, and T. Fuhrman, "The Architecture of the Decent VM: Towards a Decentralized Virtual Machine for Many-Core Computing," Virtual Machines and Intermediate Languages (Systems Programming Languages and Applications: Software for Humanity), Reno, NV, 17–21 October 2010; Sean Campbell and Michael Jeronimo, *Applied Virtualization Technology: Usage Models for IT Professionals and Software Developers* (Santa Clara, CA: Intel Press, 2006), chap. 9; R. P. Case and A. Padegs, "Architecture of the IBM System/370," *Com-*

munications of the ACM 21, no. 1 (January 1978): 73–96; R. J. Creasy, "The Origin of the VM/370 Time Sharing System," *IBM Journal of R&D* 25, no. 5 (September 1981): 483–90; R. W. Doran, "Amdahl Multiple-Domain Architecture," *Computer*, October 1988, 20–28; R. C. Daley and J. B. Dennis, "Virtual Memory, Processes, and Sharing in MULTICS," *Communications of the ACM* 11, no. 5 (May 1968): 306–12; T. Egawa, N. Nishimura, and K. Kourai, "Dependable and Secure Remote Management in IaaS Clouds," 2012 IEEE 4th International Conference on Cloud Computing Technology and Science, 3–6 December 2012, Taipei, Taiwan, 411–18; D. Gifford and A. Spector, "Case Study: IBM's System 360-370 Architecture," *Communications of the ACM* 30, no. 4 (April 1987): 291–307; P. H. Gum, "System/370 Extended Architecture: Facilities for Virtual Machines*," IBM Journal of Research and Development* 27, no. 6 (1983): 530; K. Hwang and D. Li, "Trusted Cloud Computing with Secure Resources and Data Coloring," *IEEE Internet Computing* 14, no. 5 (September/October 2010): 14–22; A. S. Lett and W. L. Konigsford, "TSS/360: A Time-Shared Operating System," *Proceedings of the Fall Joint Computer Conference*, AFIPS, vol. 33, part 1 (1968): 15–28; A. Mann, "The Pros and Cons of Virtualization," *Business Trends Quarterly*, First Quarter 2007; R. A. Meyer and L. H. Seawright, "A Virtual Machine Time-Sharing System," *IBM Systems Journal* 9, no. 3 (1970): 199–218; Seawright, and R. A. McKinnon, "VM/370–A Study of Multiplicity and Usefulness," *IBM Systems Journal* 18, no. 1 (1979): 4–17; A. V. Anderson et al., "Intel Virtualization Technology," *IEEE Computer* 38, no. 5,(2005): 48–56; B. Yee et al., "Native Client: A Sandbox for Portable, Untrusted x86 Native Code," 2009 30th IEEE Symposium on Security and Privacy, Oakland, CA, 17–20 May 2009, 79–93; and Y. Wen and K. Du, "Pollux VMM: A Virtual Machine Monitor for Executing Untrusted Code," 1st International Conference on Information Science and Engineering (ICISE2009), Nanjing, China, 28–29 December 2009, 1785–1788.

16. Cricket Liu and Paul Ablitz, *DNS and BIND*, 5th ed. (Sebastopol, CA: O'Reilly & Associates, 2006).

17. A. Karasidis, *DNS Security* (New York: Springer, 2012); and N. Doraswamy and D. Harkins, *IPSEC: The New Security Standard for the Internet, Intranets, and Virtual Private Networks* (Upper Saddle River: Prentice Hall, 2003).

18. D. L. Rulke and J. Galaskiewicz, "Distributed Knowledge, Group Network Structure, and Group Performance," *Management Science* 46, no. 5 (May 2000): 612–22; M. R. Stytz and S. B. Banks, "Metrics for Assessing Command, Control, and Communications Capabilities," 11th International Command and Control Research and Technology Symposium, San Diego, CA, 20–26 June 2006; P. Barton, "What Happens to Value of Information Measures as the Number of Decision Options Increases?" *Health Economics* 20 (2011): 853–63; D. Bellin, "The Economic Value of Information," *Science Communication* 15, no. 2 (1993): 233–40; A. Cleveland, "Harvesting the Value of Information," *Journal of Management and Engineering* 15, no. 4 (1999): 37–42; P. Delquié, "The Value of Information and Intensity of Preference," *Decision Analysis* 5, no. 3 (2008): 129–39, 169; R. Glazer, "Measuring the Value of Information: The Information-Intensive Organization," *IBM Systems Journal* 32, no. 1 (1993): 99; T. Hulme, "Unlocking the Business Value of Information: Information on Demand," *Business Information Review* 26, no. 3 (2009): 170–81; M. E. Johnson and S. L. Pfleger, "Addressing Information Risk in Turbulent Times," *IEEE Security and Privacy* 9, no. 1 (2011): 49–58; A. Kangas, "Measuring the Value of Information in Multicriteria Decision Making," *Forest Science* 26, no. 6 (2010): 558–66; C. Oppenheim et al., "Studies on Information as an Asset I: Definitions," *Journal of Information Science*, vol. 29, no. 3, (2003): 159–66; Oppenheim et al., "Studies on Information as an Asset II: Repertory Grid," *Journal of Information Science* 29, no. 5 (2003): 419–32; Oppenheim et al., "Studies on Information as an Asset III: Views of Information Professionals," *Journal of Information Science* 30, no. 2 (2003): 181–90; Oppenheim et al., "The Attributes of Information as an Asset," *New Library World* 102, no. 11/12 (2001): 458–63; R. Fattahi and E. Afshar, "Added Value of Information and Information Systems: A Conceptual Approach," *Library Review* 55, no. 1–2 (2006): 132–47; A. Repo, "The Dual Approach to the Value of Information: An Appraisal of Use and Exchange Values," *Information Processing & Management* 22, no. 5 (1986): 373–83; A. Shepanski, "The Value of Information in Decision Making," *Journal of Economic Psychology* 5, no. 2 (1984): 177–94; and J. Sillince, "A Stochastic Approach of Information Value," *Information Processing & Management* 31, no. 4 (1995): 543–54.

19. M. R. Stytz, and S. B. Banks, "Toward Improved Software Security Training Using a Cyber Warfare Opposing Force (CW OPFOR): The Knowledge Base Design," *Proceedings of the SPIE Conference on Data Mining, Intrusion Detection, Information Assurance, and Data Networks 2005,* 5812, no. 28–29 (March 2005): 130–41; Stytz and Banks, "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 (April 2006): 17–21; Stytz and Banks, "Requirements and Issues in Cyberwarfare Simulation," *Proceedings of the 2000 Fall Simulation Interoperability Workshop*, Orlando, FL, 17–22 September 2000, 1–10; Stytz and Banks, "Toward Computer Generated Actors As Cyberspace Opposing Forces Used In Network Centric Warfare Simulations," *Proceedings of the 2004 Spring Simulation Interoperability Workshop*, Washington, DC; 18–23 April 2004, 84–95.

20. An approach that does not use simulation for user preparation for cyber attacks is discussed by S. L. Garfinkel and G. Dinout, "Operations and Degraded Security," *IEEE Security and Privacy* 9, no. 6 (2011): 43–48.

21. Ibid.; and Stytz and Banks, "Metrics for Assessing Command, Control, and Communications Capabilities," 11th International Command and Control Research and Technology Symposium, 20–26 June 2006, San Diego, CA.

22. G. Booch, J. Rumbaugh, and I. Jacobson, *The Unified Modeling Language User Guide* (Reading, MA: Addison-Wesley, 1999).

23. Our first efforts toward development of tools for cyberspace performance metrics are discussed in previously cited references. The metrics are similar to the online, one-pass algorithms used in high frequency trading and derive from digital signal processing.

24. *Communications of the ACM* 55, no. 4: special issue on smart grid technology.

25. *IEEE Computer* 46, no. 2: special issue on the "Internet of Things."

26. J. Carr et al., Project Grey Goose Report on Critical Infrastructure: Attacks, Actors, and Emerging Threats (McLean, VA: Grey Logic, 2010), 12.

27. A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt* (Upper Saddle River: Addison-Wesley, 2007).

28. S. Banks and C. Lizza, "Pilot's Associate: A Cooperative, Knowledge-Based System Application," *IEEE Expert* 6, no. 3 (1991): 18–29.

29. Mica Endsley, "Situation Awareness Global Assessment Technique (SAGAT)," *Proceedings of the IEEE 1988 National Aerospace and Electronics Conference*, 789–95.

30. Osinga, *Science Strategy and War.*

Disclaimer

The views and opinions expressed or implied in SSQ are those of the authors and are not officially sanctioned by any agency or department of the US government. We encourage you to send comments to: strategicstudiesquarterly@us.af.mil.