Modelling the Cognitive Work of Cyber Protection Teams

Colonel Stoney Trent
Dr. Robert R. Hoffman
Lieutenant Colonel David Merritt
Captain Sarah Smith

ABSTRACT

Cyber Protection Teams (CPTs) defend our Nation's critical military networks. While Cyber Security Service Providers are responsible for the continuous monitoring and vulnerability patching of networks, CPTs perform threat-oriented missions to defeat adversaries within and through cyberspace. The research we report here provides a descriptive workflow of cyber defense in CPTs as well as a prescriptive work model that all CPTs should be capable of executing. This paper describes how these models were developed and used to assess technologies and performance of CPTs. Such models offer a variety of benefits to practitioner and research communities, particularly when the domain of practice is closed to most researchers. This project demonstrates the need for continual curation of CPT work models as well as the need for models of work for the other types of cyber teams (i.e. Mission and Support) in the Cyber Mission Force.

INTRODUCTION

Cyber Protection Teams (CPTs) defend our Nation's critical military networks. While Cyber Security Service Providers are responsible for the continuous monitoring and vulnerability patching of particular networks, CPTs perform threat-oriented missions to defeat adversaries within and through cyberspace. Each 39-person CPT must be able to work with network security teams and other CPTs to counter cyber threat actors. When fully operational, the Cyber Mission Force will include 68 CPTs, which will be manned, trained and equipped by the Military Service Departments. [1] Within the Cyber Mission Force, CPTs are allocated to an operational command and aligned with one

Stoney Trent is a Cognitive Engineer and Army Cyber Warfare Officer, currently serving as a U.S. Army War College Fellow at the National Security Agency. Previously he served as the Chief of Experimentation and Director of the Cyber Immersion Laboratory at U.S. Cyber Command. He has 22 years of experience in operations and intelligence assignments in tactical, operational and strategic echelons. His research has focused on team cognition in mission command, intelligence and cyberspace operations. His current work is focused on improving technology innovation for cyberspace operations.

of four mission areas: Combatant Command (CCMD), Service Department (Army, Navy, Air Force, and Marine Corps), Department of Defense Information Network (DODIN), and National Threats. To maximize flexibility, these teams must be able to perform reliably as well as be interchangeable and interoperable.

CPTs must be able to perform three basic types of missions. [2]

1. Survey: Short duration assessments that provide the supported organization with recommended mitigations based on an assessment of network vulnerabilities.
2. Secure: Harden and defend cyber key terrain; and
3. Protect: Time-sensitive deployments that include Survey and Secure tasks, but also include helping an organization recover from the effects of a cyber intrusion.

The research we report here provides a descriptive workflow of cyber defense in CPTs as well as a prescriptive work model that all CPTs should be capable of executing.

Work models, such as the one described here, provide a foundation for improvements to work processes. As an illustration of required or desired workflows, work models provide a bridge to common ground between researchers and practitioners, particularly when the work domain is difficult to access, or is esoteric. The model in this report has multiple purposes. The first purpose is to inform the design of experiments to assess current and emerging technologies for operational fit. The second is to educate developers, who may have limited knowledge of CPT work, about the tasks that require technical support. The third is to inform revisions to operational doctrine. Finally, this model is meant to provide the basis for operational and strategic planning of defensive cyberspace operations.

David Merritt is the Experimentation Branch Chief at U.S. Cyber Command, where he leads capability assessments and experiments to bridge the gap between research and operations. David's interest in human-system cyber issues stems from his previous experience leading the incident response efforts of the Air Force Computer Emergency Response Team, as well as his Ph.D. research on leveraging a mix of expertise between humans and machine learning agents.

Developing the model

To develop an initial model of CPT work, the research team started with a review of the literature, including doctrine, published reports, and conference proceedings. Prior research on defensive cyber work had established multiple workflow models. [3][4][5] One of these models was aimed at the development of a computer simulation of the work process of cyber incident response teams. [6] Reed and colleagues worked with cyber analysts at the Sandia National Laboratories to develop and implement a workflow model (using the ACT-R computational cognitive model). The workflow model they developed was similar in many respects to another workflow model developed at U.S. Cyber Command. [7] These prior models described defensive cyber work at a very high level of primary tasks (e.g. Review Alerts, Evaluate Risk, Understand, Engage Mitigation).

Beginning with these models, we created an initial model with the benefit of a former CPT member who is a co-author of this paper (SJS). Our initial model is presented in Figure 1. For the model to satisfy our purposes, we needed to elaborate and validate it with input and suggestions from CPT members from all the various Mission Types previously mentioned. To do so, we interviewed current team members from across the Cyber Mission Force.

The research team solicited 50 volunteer interviewees from 19 CPTs. Army (8 CPTs), Air Force (3 CPTs), Navy (4 CPTs) and Marine Corps (4 CPTs) representing DODIN, National, CCMD, and Service mission areas. As individuals and as teams, participants had a range of experience in addition to their foundational cyber training. Some had participated in exercises but had not yet been on actual missions. Most had some background in computer or information science; some had experience in information security.

Robert R. Hoffman received his Ph.D. in experimental psychology from the University of Cincinnati. He is a Senior Member of the Institute of Electrical and Electronics Engineers (IEEE), a Fellow of the Association for Psychological Science, a Fellow of the Human Factors and Ergonomics Society, a Senior Member of the Association for the Advancement of Artificial Intelligence, and a Fulbright Scholar. He has been recognized internationally for his research on the psychology of expertise, the methodology of cognitive task analysis, and the issues for the design of complex cognitive work systems, including cyber work systems.

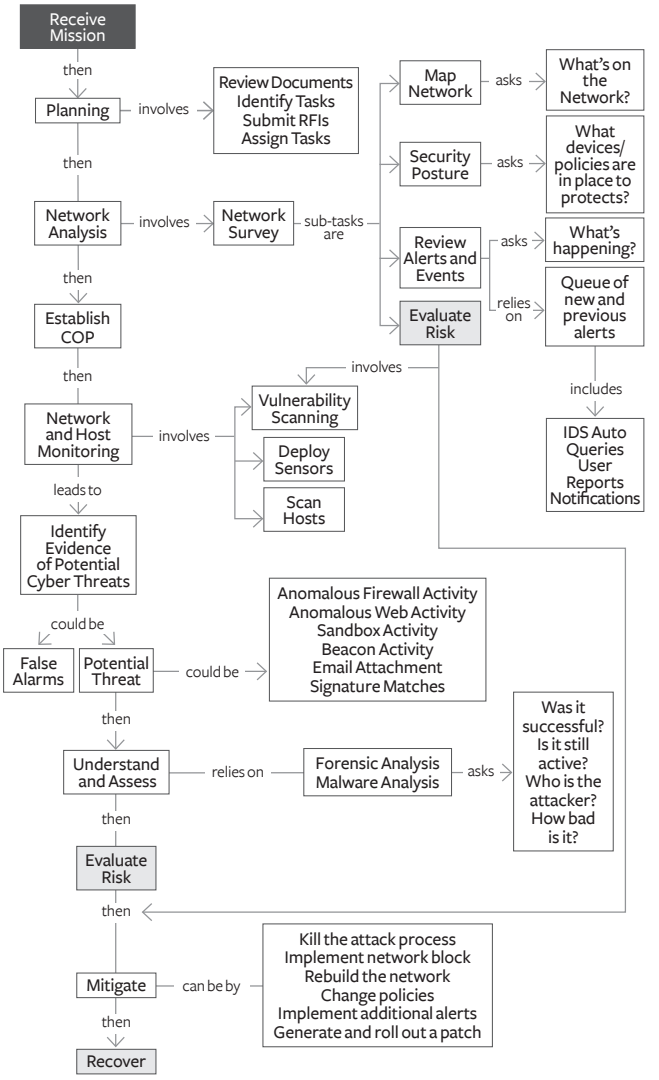

Figure 1. Initial Workflow model

On the other hand, some entered the CPT community with little to no computer science background. Embracing such diversity was necessary for the interview results and for the refined work model to reflect the variability of experience in actual practice.

In the interviews, the participants were shown a diagrammatic model of the work. As the participants

Sarah Smith is a Capability Analyst at U.S. Cyber Command, who supports experimental activities designed to understand operations and inform technical solutions. Prior to her assignment at U.S. Cyber Command, Sarah served as a Cyber Network Defense (CND) Manager for a Cyber Protection Team (CPT).

recounted their experiences, they referenced the diagram and provided annotations and suggestions for how it could be corrected, improved, and refined. The first interviews began with the model presented in Figure 1. Interviews were conducted over two months, at multiple locations, and the workflow model was successively iterated and refined. As the interviewing continued, fewer and fewer modifications were proposed. The diagram converged on a consensus model, acknowledged by multiple independent CPT members as being a good depiction of their workflow, regardless of CPT Service or Mission alignment.

Notice that the left-hand side of Figure 1 is a sequence of events or activities. Many work models assume that work can, and should, be represented as a series of clear-cut steps or stages. As our research continued to refine the model, however, it was discovered that the work of CPTs needs to be described in terms of parallel tasks and feedback loops, not as a series of steps or stages. Figure 2 presents a "high-level" overview of the workflow model. The purpose of this high-level overview is to offer critical work task elements without the potentially overwhelming details about the sub-tasks. (In comparison to planning models for full missions, the diagrams created for CPT modeling are elementary.

At the top and bottom of Figure 2 are two continuous horizontal lines. The line at the top highlights the fact that CPT interaction with intelligence, and with the supported organization (circles at the left side of the Figure) are continuous processes that occur at many points throughout a mission. The line at the bottom serves as a reminder that CPT members remain cognizant of potential vulnerabilities or threats and the evaluation of risks. The full model expands on the concepts and activities that are involved for each of the major nodes that are highlighted in green

in Figure 2: Planning and Logistics, Monitoring and Collecting, Sensemaking, and Closure. The full model is presented in Figure 3.

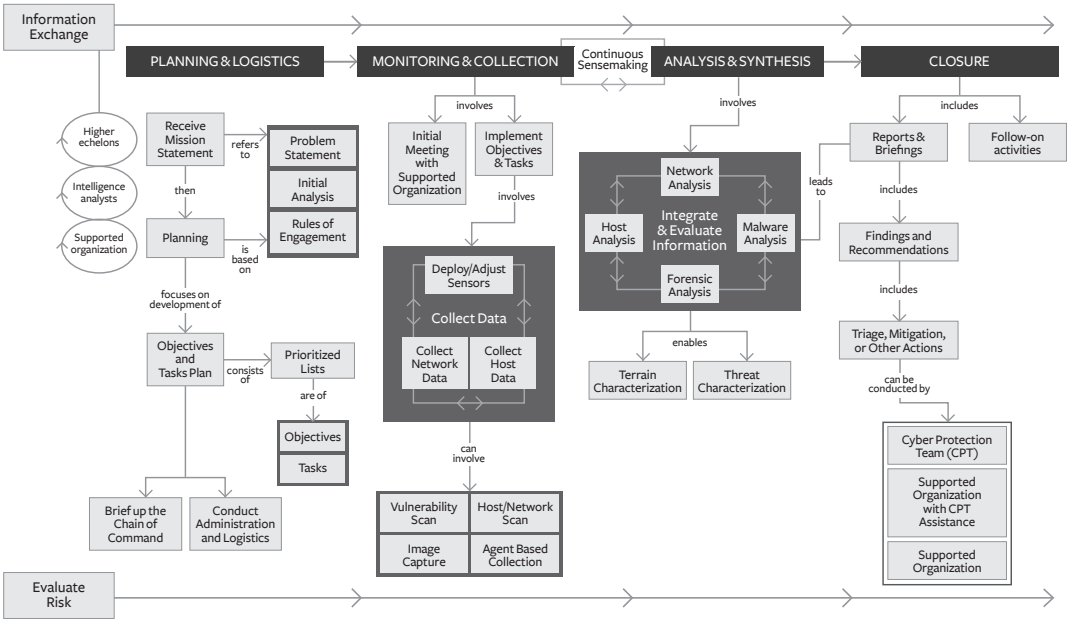

Figure 2. Abstract view of CPT workflow

From the standpoint of cognitive work analysis, a few features of the model are noteworthy. First, the model does not match the current doctrine in all respects. The primary tasks described in earlier models and in CPT CONOPS involve stages of Survey, Secure, Protect, and Recover. This and other aspects of CPT doctrine are still evolving. The field study interviews revealed that there is much more to CPT mission-related activity. Specifically, the primary activity categories are perhaps better described as Planning, Collection, Analysis and Synthesis, and Closure. Within each of these are many sub-tasks and activities.

Second, while CPT work can be understood as having stage-like primary activities, it is not possible to capture the range and details of CPT mission-related activities in a step-wise, sequential or linear chain model. The initial model was built upon a sequential "backbone," as pointed out above (Figure 1). Some CPT activities are sequential, and a high-level sequence can be discerned in a retrospective study of any given cyber mission, but from the field study interviews, we learned that most CPT activities are interdependent (note the cross-links in Figure 3). Some activities are cyclical, some are continuous, and others are parallel. For example, the process of creating an accurate logical-physical map of the cyber-terrain involves waves of iteration and refinement as different subtasks are conducted (e.g. passive scan, active scan, host monitoring, etc.). Thus, sub-tasks that occur in cycles were represented as cycles in the diagram, and some of these are nested. For example, high-level sensemaking

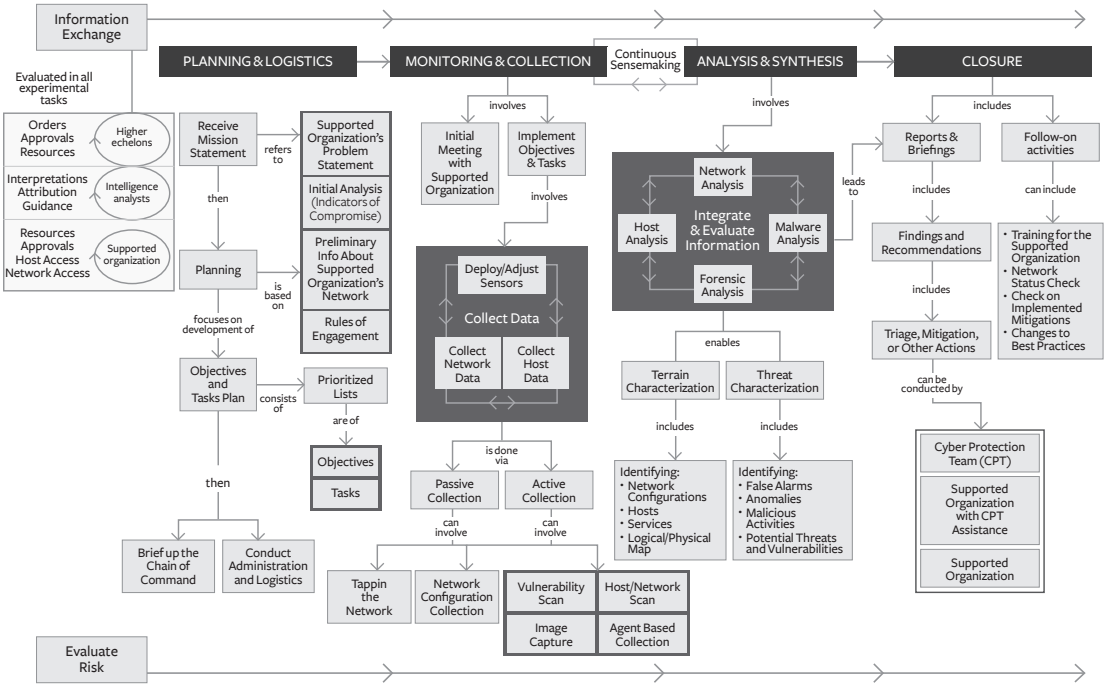

Figure 3. Detailed CPT work model

is represented by the cycle between Monitoring/Collection and Analysis/Synthesis. Within Monitoring/Collection is an embedded cycle of Sensor Deployment, Traffic Monitoring, and Host Monitoring.

It is important to note that this model represents the collection of tasks that may be considered ideally rigorous. As such, this model represents how an experienced team would perform a mission without time constraints. In fact, no team performs all these tasks for all missions. Instead, teams leverage their understanding of the situation to adapt their work to suit the constraints and intent of the mission and taking into account the mission of the network owner (i.e. mission essential elements of the network). As a model of ideally rigorous CPT work, it illustrates the breadth of work that CPTs must be able to perform and therefore helps to describe technology support requirements.

Putting the model to work

An important reason for including all the fine grain detail (Figure 3), rather than reducing the complexity to a simpler representation, is that in expressing the full range of the tasks that CPTs conduct, one can create "layers" that represent different Mission types, or Services differences. This contextualizes the differences by expressing them within the broader context. Figure 4 presents a layer (green coloration) of what is involved in the Network Mapping

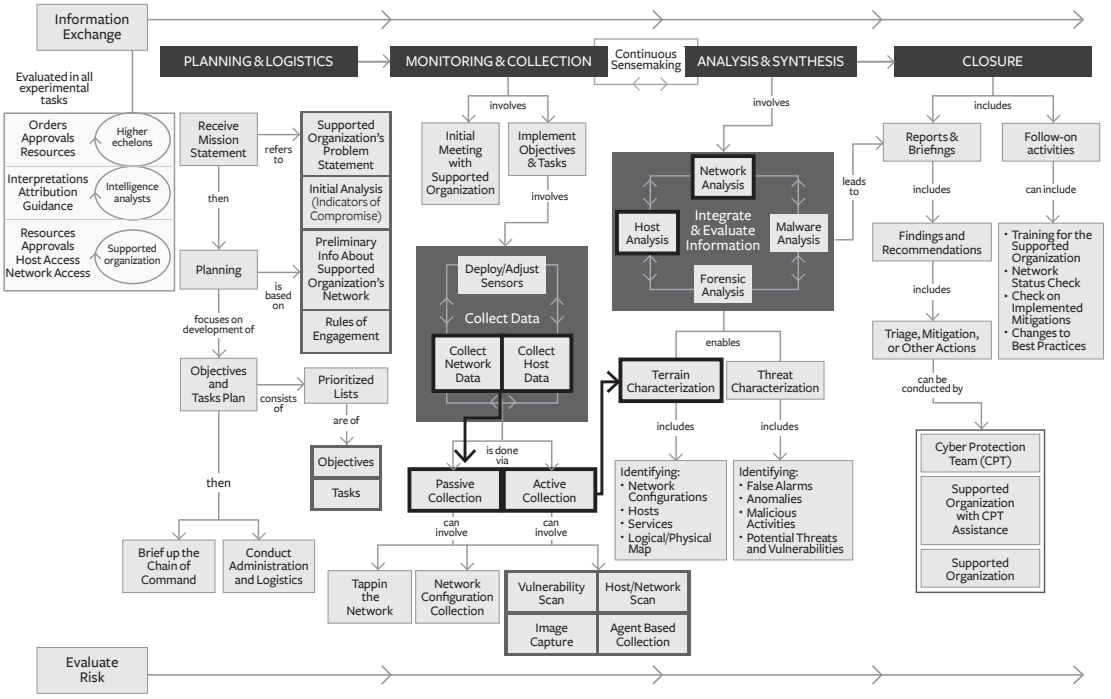

Figure 4. CPT work model overlaid with network mapping task

Task. Figure 5 shows a layer (orange coloration) that depicts what is involved in the Malware Identification task.

Workflow models of this kind have several immediate uses, described above, but going forward, they have additional applications that can be of value to the Cyber Mission Force and researchers who are developing technologies for the Force.

- Such a task decomposition can be reviewed to identify aspects of CPT performance that can be readily observed and measured.
- Because CPT work is distributed across many work roles, this work model can be used to document which roles are involved with which particular tasks.
- Workflow models can be used in a "checklist" mode to track performance and CPT qualifications.
- Workflow models can be used in training and can allow individuals who are less familiar with CPT work to come to an understanding at levels of detail.
- While CPT work is heavily dependent on computational technology, it is fundamentally cognitive work. Workflow Models can be used to highlight CPT activities and functions that can only be conducted by human decision makers. This highlights the importance of training to high levels of proficiency and expertise.

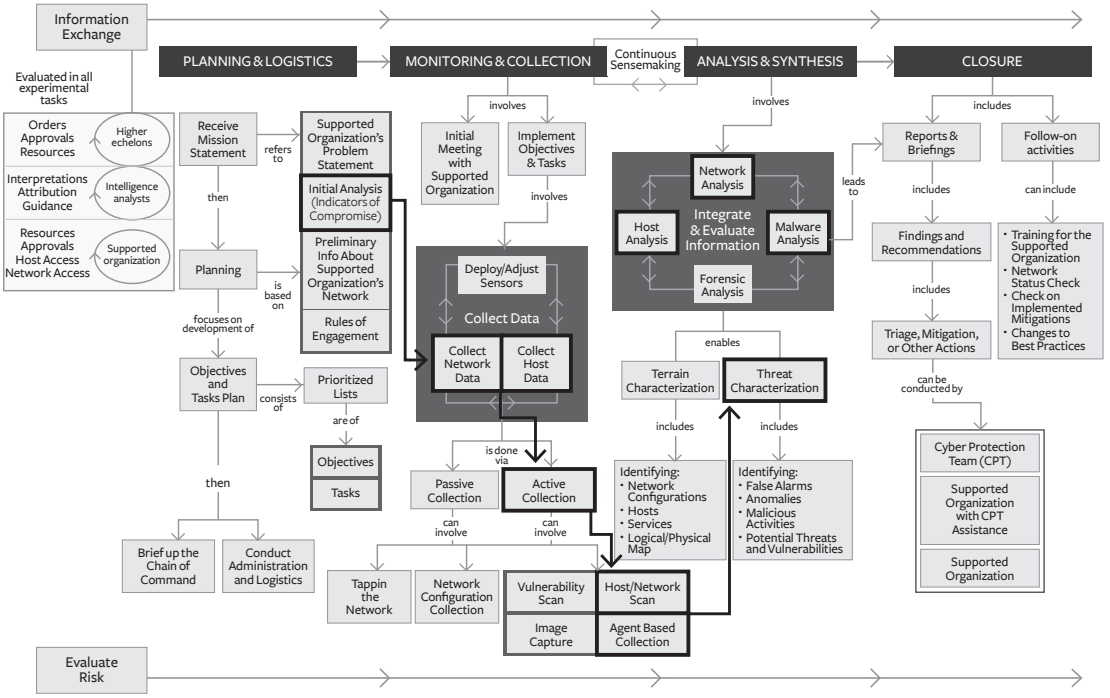

Figure 5. CPT work model overlaid with sensor deployment task

- Workflow models reveal work design issues, such as bottlenecks and capability gaps.
- Workflow models provide a focus for discussion of work methods, desired tool functionalities, and best (and sub-optimal) practices.
- Workflow models allow representation and comparison of mission differences, Service differences, down to the level of individual CPTs.
- Workflow models can be used to identify aspects of the work that demand additional or better technical support.
- Workflow models inform CONOPS and allow tracking of changes in CONOPS. At an even higher level, workflow models provide a window on the current work that can inform and contextualize the design of entire campaigns of experimentation.

Currently, CPT work methods are evolving, and technology support requirements are continuing to emerge. Thus, the workflow model presented here represents the state of CPT work methods as they currently exist within the CMF. Cyber work methods and technologies are evolving at a pace which demands continual curating of this "as-is" model. Furthermore, this project demonstrates the need for models of work for the other types of cyber teams (i.e. Mission and Support) in the CMF. Although our research team used methods that are typical

for field studies in other work domains, the research team found that automated instrumentation might provide data for mathematical models of cyber teamwork. Such mathematical models should prove invaluable for simulations to aid with operational and strategic planning. Our current research is pursuing this notion.

DISCLAIMER

This paper reflects the views of the authors. It does not represent the official policy or position of Department of Defense, U.S. Cyber Command or any agency of the U.S. Government. Any appearance of DoD visual information or reference to its entities herein does not imply or constitute DoD endorsement of this authored work, means of delivery, publication, transmission or broadcast.

ACKNOWLEDGMENT

The authors would like to acknowledge the contributions to the research reported here by the Applied Physics Laboratory, Johns Hopkins University.

NOTES

1. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
2. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
3. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
4. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
5. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
6. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.
7. U.S. Department of Defense, The Department of Defense Cyber Strategy, (2015), Washington, DC, https://www.defense.gov/News/Special-Reports/0415_Cyber-Strategy.