Cyber Operator Perspectives on Security Visualization

Anita D'Amico[1], Laurin Buchanan[1], Drew Kirkpatrick[1] and Paul Walczak[2]

[1] Secure Decisions, a division of Applied Visions, Inc., 6 Bayview Avenue, Northport, NY 11768, United States of America
[2] Warrior LLC, Box 1224, Darby, MT 59829
{Anita.Damico, Laurin.Buchanan, Drew Kirkpatrick}@SecureDecisions.com, paul@warriorllc.com

Abstract. In a survey of cyber defense practitioners, we presented 39 assertions about the work cyber operators do, data sources they use, and how they use or could use cyber security visual presentations. The assertions were drawn from prior work in cyber security visualization over 15 years. Our goal was to determine if these assertions are still valid for today's cyber operators. Participants included industry, government and academia experts with real experience in the cyber domain. Results validated the assertions, which will serve as a foundation for follow-on security visualization research. Feedback also indicates that when analyzing a security situation, cyber operators inspect large volumes of data, usually in alpha-numeric format, and try to answer a series of analytic questions, expending considerable cognitive energy. Operators believe security visualizations could support their analysis and communication of findings, as well as training new operators.

Keywords: Cyber operations · Network defense · Human factors · Visualization · Knowledge elicitation · Cognitive work

1 Introduction

Cyber operations have historically been viewed primarily as a technical problem. The speed of cyber attacks has focused research and development on automating the process of attack detection and response. Nevertheless, the human cyber operator remains in the loop to perform many cognitively intense activities, for example, to discover incidents that don't fit the automated attack detection profile, evaluate automated alerts for true and false positives, or assess the operational impact of a cyber incident. The United States Air Force acknowledges the critical position of the human operator, "Computers can keep track of many objects, but humans still remain more capable of higher-level comprehension, reasoning and anticipation", and calls for visualizations that can augment human performance of cyber operations [1].

Designing cyber security visualizations is not easy. Effective visualization design is an extremely complicated process that requires iterative design and evaluation efforts [2]. And there are few evaluation efforts that provide confidence in what visualizations are best to support various cyber security operations. In the small body of work on the

effectiveness of visualizations on cyber operator performance, most have some restriction that reduces the applicability of reported findings, for example, they did not use experienced cyber operators [3], or the data sets were artificially manipulated and are unrepresentative of the size and complexity of data that real cyber operators process [4], or dependent variables were primarily subjective [5]. Furthermore, cyber operators have a variety of roles in network defense, each with its own objectives and sets of activities. Visualizations that may be effective for assessing trends in historical cyber data may not be effective in supporting an operator's rapid assessment of suspicious activity to throw out false positives. More studies are needed to guide the design and selection of visualizations for network defense, and to empirically evaluate the effectiveness of different types of visualizations on the various decisions made by cyber operators.

The survey and results presented in this paper are the initial findings of the first phase of a research project funded by the Air Force Research Laboratory to define visualization objectives and design visualization concepts that have high potential for enhancing cyber operator performance during event detection and preliminary event analysis—the first two stages of the US Department of Defense (DoD) Cyber Incident Handling Life Cycle (CIHLC) (CJCSM 6510.01B) [6]. The second phase of the research will measure the effectiveness of these visualization concepts.

2 Approach

Prior to designing cyber security visualizations, it is necessary to define the operator decisions that the visualizations must support and the information requirements that the operator must satisfy in order to make these decisions. Only after understanding what the operator needs to know to do his or her job can we design visualizations to provide that information in an easily consumable and actionable form.

We chose to focus on the first two stages of the US DoD Cyber Incident Handling Life Cycle (CIHLC) [6] depicted in Figure 1 below. These stages (Detection of Events, and Preliminary Analysis and Identification) require operators to review alert queues of cyber event data to identify, record and report suspicious behavior or cyber events of interest. Examples of the work objectives and operator activities performed during these stages is also included in Figure 1.

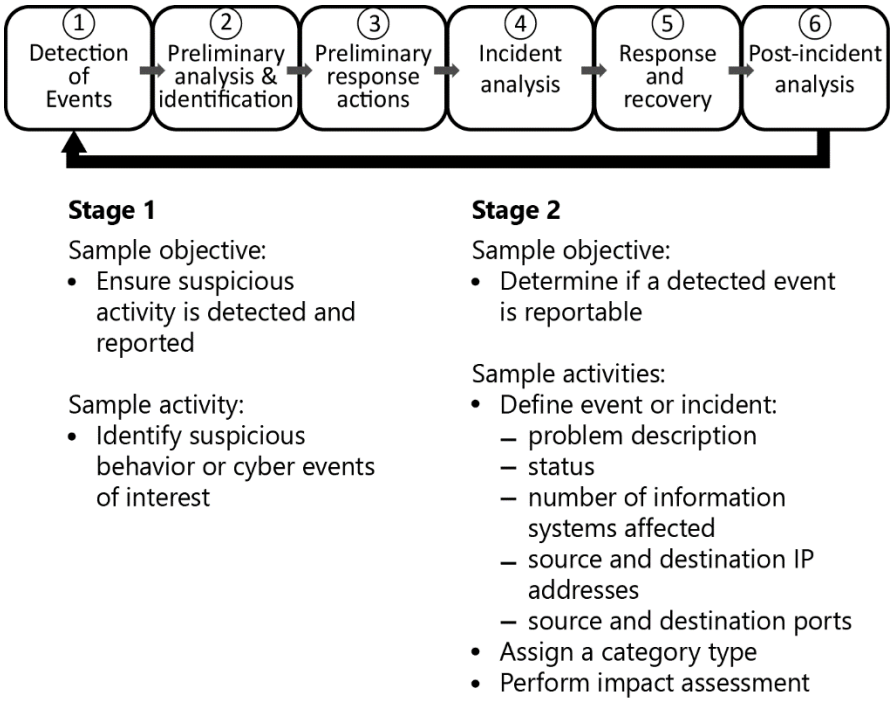

Fig. 1. US DoD's Cyber Incident Handling Life Cycle has 6 stages; our work focused on Stages 1 and 2.

The decisions that Stages 1 and 2 operators make, the cognitive requirements for those decisions, and how they use visualizations in their work have been previously reported [7] [8] [9] [10] [11], observed during Knowledge Elicitations and cyber competitions [12] [13] [14], and the work requirements are referenced in DoD doctrine [3]. However, some of the studies were published more than ten years ago. Prior to using the results of these studies in establishing our visualization objectives and concepts, we wanted to verify that their findings are still valid for today's network defenders operating in a more dynamic cyber environment.

Our approach was to first review the prior research and extract "assertions" about the work that these cyber operators perform, the data sources they use, and their use of visualizations (if any) in their analytic work. We then presented these assertions to fifteen subject matter experts in the form of a survey in which they were asked to rate their level of agreement or disagreement with the assertion. For Assertions 1-1 through 1-7, and 1-13 we also asked the participants to indicate to which stage of the CIHLC the assertion was related. They were permitted to select up to three stages as relevant to the assertion.

Participants. Participants were subject matter experts (SMEs) from industry, the DoD, and academia with a minimum of two years and an average of 25 years of experience in various roles in the cyber domain, including incident response, network operations,

cyber forensics, and cyber counterintelligence. All were male and at least eight had either hands-on experience in conducting incident response or managing incident responders.

List of Assertions. Tables 1, 2 and 3 list the assertions drawn from the prior work. We asked each participant to state their level of agreement or disagreement with each statement on a five-point scale ranging from strongly disagree to strongly agree. Participants were also presented with the option to mark "cannot respond" if they did not have sufficient experience with the issue. The survey provided visualization examples for Assertions 3-14 through 3-16.

Table 1. Assertions about the work of defensive cyber operators

Reference	Assertion Text
1-1	Some operators limit their inspection of data to *no more than a single day's data* to perform their job.
1-2	Some operators search through more than a day's or even a few weeks' worth of data *within their own site* for unusual events or trends.
1-3	Some operators search through more than a day's or even a few weeks' worth of data, *including data from external sites,* for unusual events or trends.
1-4	Cyber operators often *associate several pieces of information together and add a hypothesis* for why these events are all related.
1-5	In many cases, the *attacker-related data is intermingled with a substantial amount of other data*. It can be challenging to find the relevant amidst the irrelevant data.
1-6	When analyzing an event or incident, the operator needs to assess the technical impact of the event or incident on the rest of the network. That is, s/he needs to determine what other resources on the network may have been impacted by the malicious activity.
1-7	When analyzing an event or incident, the operator needs to assess the *operational impact* of the event or incident. That is, to determine what specific operations, missions, or users may have been impacted by the malicious activity.
1-8	Operators often have several monitors on their desks, each depicting different data.
1-9	The information displayed on the operator's monitor(s) is his or her *primary view* into whether there is a suspicious event or cyber incident, and of the activities of the attacker.
1-10	One of the most important cognitive skills that operators leverage is their ability to mentally fuse data from different sources.
1-11	An important feature of the operator's workflow is the series of questions that s/he asks as s/he moves through the analytic process: "Is this legitimate activity?" "How often has this source IP connected to our network?" "Has this destination IP been sending out unusually large payloads?"
1-12	Operators in all roles regularly engage in educating or communicating to others the results of their analyses, via daily briefings at a CERT, on electronic bulletin boards shared by fellow operators, or in training sessions.
1-13	Operators are often required to explain why they formed certain hypotheses or took certain actions; this may require the presentation of knowledge that may not be available to all concerned.

Table 2. General assertions about the state of cyber security visual presentations

Reference	Assertion Text
2-1	Classic security tools, such as firewalls and intrusion detection systems, have over time added reporting capabilities and dashboards that are making use of data visualization techniques like charts and graphics.
2-2	In general, the visual presentations of data in current cyber security tools do not have adequate interactivity to support data exploration.
2-3	When designing visualizations for defensive cyber operators, the designer should assume that *at least two* monitors are available, and use the extra display for depicting different types of information.
2-4	Most cyber security visual displays are fairly basic, such as pie charts or bar graphs.
2-5	Some cyber security visual displays require several hours to learn how to use effectively. But if the operator learns how to use them, their value is worth the investment of time.
2-6	Visualizations are more likely to be added-on to security products later in their design or production, rather than integrated early in the design process.
2-7	Visual data presentation is an effective method for training others. For example, if a new operator is unfamiliar with the network topology, and the topology is a critical component of the operator's decision making, then a visual depiction of parts of the network topology can help the new operator learn the topology more rapidly.
2-8	Visual data presentation is an effective method for communicating findings to colleagues or laypersons, and/or for documenting decisions for review or justification.

Table 3. Specific assertions about the state of cyber security visual presentations

Reference	Assertion Text
3-1	Visualizations should interface to multiple data sources, and provide the operator with a common framework for viewing them.
3-2	The distinct tasks and cognitive requirements of each analysis role and analytic stage indicate a need for *role-based visualization aids*.
3-3	The exploration of voluminous data, and the discovery of patterns within that data, can be enabled through visual data presentation.
3-4	A visualization system designed for defensive cyber operators should be able to draw data from various databases or delimited files, and fuse it into a single visualization.
3-5	The data access and visualization system should provide the operator with the opportunity to save data files, visualization workspaces and any reports created with these files, using the analytic question he is trying to answer as the common reference point.
3-6	In formulating and testing hypotheses to explain suspicious activity, operators look at, reorder, highlight, and filter out data from large datasets, looking for patterns and trends.
3-7	To facilitate examination of data from multiple perspectives, visualization systems should provide multiple, coordinated views of the same dataset. When the operator reorders, highlights, or filters data in one view, the other views should automatically morph to correspond to the changes.

3-8	As operators work their way through data, they apply filters either by specifying criteria for accessing data from the database, or by temporarily filtering data at the display.
3-9	Operators typically apply a series of filters to reduce data — for example, first filter out all connections where bytes returned = 0, then filter data between .mil IP addresses, then temporarily hide any connections to CNN.com. However, if they get interrupted or distracted, as they are likely to do in a noisy environment, they can lose track of where they are in the exploration of the data.
3-10	A simple graphic or table of the filters applied to the data and the displays aids situational awareness by helping operators reorient after distractions.
3-11	Visual data presentation can facilitate the rapid comprehension of a sequence of interconnected events, improving understanding of complex relationships.
3-12	Threat analysis may be facilitated by *animations and visual replay of events across the network*, from which cyber operators can deduce the progression, speed, or direction of an attack.
3-13	By visually depicting the historical activity pattern of a specific attacker, the operator can forecast the next likely action of that attacker.
3-14	Visualizations that *combine several types and dimensions of data* may enhance the operator's ability to see patterns and time trends across multiple data sets.
3-15	A visualization of the *connections between various entities* can help the operator gain insight into the attacker's activities.
3-16	An *animation of a possible path that an attacker could have taken* can help the operator gain insight into the *attacker's activities.*
3-17	A visualization of *the connections between various entities* and an *animation of a possible path* that an attacker could have taken can help the operator *communicate the sequence of the attacker's actions to others*.
3-18	Visual data presentation can be very useful for *ad hoc* types of exploration, as certain patterns are easily comprehended when presented graphically.

3 Results

A complete list of participant responses on their level of agreement with assertions is shown in Table 4. Participants generally agreed or strongly agreed with the assertions presented in the survey. We found that >= 50% of participants were in agreement (either *agree* or *strongly agree*) with 38 of the 39 assertions and >= 75% of participants were in agreement with 33 of the 39 assertions. There were no assertions that had more participants in disagreement (either *disagree* or *strongly disagree*) than in agreement. Only three assertions had less than 10 participants in agreement. Assertion 1-13 had nine participants in agreement, three in disagreement, and three responding *neither*. Assertion 2-3 had seven in agreement, three in disagreement, four responding *neither*, and one selecting *cannot respond*. Assertion 3-13 had seven in agreement, none in disagreement, six responding *neither*, and one selecting *cannot respond*.

Table 4. Count of agreement responses per assertion

Assertion	Strongly Disagree	Disagree	Neither	Agree	Strongly Agree	Cannot Respond
1-1	1	3	0	9	3	1
1-2	0	1	0	7	7	0
1-3	0	1	0	8	6	0
1-4	0	4	2	5	5	0
1-5	0	1	0	3	11	0
1-6	0	0	0	4	11	0
1-7	0	0	0	7	8	0
1-8	0	0	0	5	9	1
1-9	1	0	1	7	7	1
1-10	0	0	1	7	7	0
1-11	0	0	1	5	9	1
1-12	2	2	0	7	5	0
1-13	0	3	3	6	3	0
2-1	0	1	1	7	6	0
2-2	0	2	1	4	6	2
2-3	1	2	4	2	5	1
2-4	0	2	1	7	4	1
2-5	0	2	3	3	7	0
2-6	0	1	2	5	7	0
2-7	0	0	1	2	12	0
2-8	0	1	0	3	11	0
3-1	0	0	1	5	9	0
3-2	1	1	0	5	8	0
3-3	0	0	1	5	9	0
3-4	0	0	0	5	10	0
3-5	0	0	0	4	11	0
3-6	0	0	1	6	8	0
3-7	1	0	1	5	8	0
3-8	0	0	1	6	8	0
3-9	0	1	1	3	9	0
3-10	0	0	3	6	5	0
3-11	0	0	0	6	8	0
3-12	0	0	3	5	6	0
3-13	0	0	6	6	1	1
3-14	0	1	0	5	9	0
3-15	0	0	0	5	10	0
3-16	0	0	2	4	9	0
3-17	0	0	1	5	8	0
3-18	0	0	1	5	9	0

Findings Indicating Incident Handling Processes Vary Significantly. Interpreted strictly by the numbers, there was some disagreement with assertions 1-1, 1-4 and 1-12. In most cases, however, participants who disagreed provided feedback regarding those assertions that indicated a reluctance to agree with the assertion due to the breadth of the assertion. In assertion 1-1 *Some operators limit their inspection of data to no*

more than a single day's data to perform their job, two participants who disagreed actually provided specific job roles as examples of the operators that inspect only a day's worth of data, such as frontline network monitoring staff, help desk or SOC analysts evaluating the most recent anomalies. Two participants who disagreed have experience in cyber counterintelligence and law enforcement, which may provide them with a different perspective.

Assertion 1-4 states *Cyber operators often associate several pieces of information together and add a hypothesis for why these events are all related.* Participant 1 disagreed with this assumption, commenting "Requires a very mature operation," while Participant 6 disagreed and commented, "I think operators would love to do this if they had time. Unfortunately, it seems that most of the work we do today is reactionary after something bad has happened." Participant 5 with a background predominantly in Stages 4-6 in counterintelligence and law enforcement simply stated, "Most do not form a hypothesis." Participant 7 disagreed without comment.

For assertion 1-12, which states *Operators in all roles regularly engage in educating or communicating to others the results of their analyses, via daily briefings at a CERT, on electronic bulletin boards shared by fellow operators, or in training sessions,* participants were not provided the opportunity to write down feedback. The disagreements came from Participant 5 with a background including counterintelligence and law enforcement, and Participants 2, 9 and 12, who each have long histories in DoD network defense and incident response, where sharing results with others may be considered less common than in academia or industry.

For assertion 1-13 that states *Operators are often required to explain why they formed certain hypotheses or took certain actions; this may require the presentation of knowledge that may not be available to all concerned,* Participant 2 commented that this and the previous "couple" of assertions are "COMPLETELY dependent upon the organization they work in", reinforcing the conclusion that incident handling process vary based on organizational maturity, size and workload.

For assertion 1-8 *Operators often have several monitors on their desks, depicting different data,* Participant 2 commented "2-3 most often, but the total depends upon who [sic] many differing tools/systems are being monitored (such as ArcSight, Splunk, an IDS, etc.)".

Findings About Visualizations. We were particularly interested in the responses to Assertion 2-5 which stated: *Some cyber security visual displays require several hours to learn how to use effectively. But if the operator learns to use them, their value is worth the investment of time*. Ten of the fifteen participants indicated agreement with this assertion. Examples provided by the participants of existing security visualizations and tools that they had spent time learning and proved to be valuable include sparklines, Splunk, Websense, WhatsUpGold, SolarWinds, and VizAlert.

Findings about Stages of the CIHLC. Table 5 summarizes the responses from participants when asked to indicate to which stage of the CIHLC the assertion was related. These results provide useful information about what visualizations are needed at every stage. For example, Assertion 1-1 suggests that any visualizations done for Stages 1, 2,

and 3 must be consumed and acted upon in a very short period of time. Our subsequent research on this project indicated that DoD cyber operators may have a timeline of two minutes or less for Stage 1 activity. Assertions 1-2 and 1-3 reveal that no matter where you are in the CIHLC, the operator spends considerable time sifting through data, both from their own enterprise and external data; comments from participants indicated this activity was more common in organizations with more mature incident handling processes. Assertion 1-4 indicates that visualizations that combine different types of data from different sources could assist operators in Stages 2, 3 and 4 hypothesize why events may be related. Comments indicate that this required effort may not regularly happen due to constraints of organizational workload and maturity. Assertion 1-5 tells us that visualizations which highlight attacker-related activity are needed in Stages 1 through 4. Assertions 1-6 and 1-7 clearly indicate that visualizations to show technical and operational impact are needed for both Stages 4 and 5, and may also be useful in Stages 3 and 6. Assertion 1-13 suggests that visualizations which help explain findings are needed across the CIHLC.

Table 5. Number of responses indicating the assertion is most likely to occur during the specific stage of incident handling.

Assertion	Stage 1	Stage 2	Stage 3	Stage 4	Stage 5	Stage 6
1-1	11	9	8	2	1	0
1-2	6	9	6	10	2	6
1-3	7	9	4	9	3	7
1-4	3	9	6	10	2	2
1-5	9	10	6	10	2	3
1-6	2	3	7	12	13	4
1-7	1	1	7	12	12	7
1-13	3	6	5	8	6	5

4 Conclusions

Cyber operations have historically been viewed primarily as a technical problem with a focus on improving technology, as opposed to improving the ability of humans to interact with technology, and with very little regard for the perceptual and cognitive capabilities of the human operators using that technology. It is imperative that the visualizations and decision support systems that these operators use are designed to be compatible with human cognition and the operators' work environment. As in any domain, user-centered and work-centered visualizations need to be developed with an understanding of the operator requirements with consideration for human factors and cognitive challenges.

Cyber security is still a relatively young profession, and as yet, there is not one standardized process or approach to the incident handling aspect of cyber security. As reported by our survey participants, different organizations even within the same industry may vary tremendously by the size of their incident handling organization and the maturity of their cyber security processes. As such, the scope and scale of cyber operations must be considered when identifying visualizations for cyber security operators.

The ability to convey actionable cyber security information in a timely manner remains a significant challenge across all stages of CIHLC. Cyber security operators regularly gather and inspect large volumes of cyber data, largely in alpha-numeric format. In their inspection they seek answers to analytic questions that help them make decisions. Anecdotally we observe that visualizations are not well integrated into this process. Experimental evidence regarding which visualizations would support these cognitive processes is limited.

Responses from our survey suggest that operators see the potential for visualizations: they are interested and willing to use visualizations to obtain actionable information, and they see the value in investing time in learning to use visualizations. However, our interviews with cyber practitioners during a later stage of this research revealed that they lack the technical ability in visual analytics to specify the construction and application of methods that can produce effective visualizations. Thus, it is up to the human factors and information visualization experts to design and develop meaningful visualizations after eliciting an understanding of what questions the cyber operators ask of data and what decisions they make based on that information.

Our research also revealed that the same cognitively intense activity and decisions (e.g. sorting through data and deciding on the most relevant, associating several pieces of data to decide if there is a pattern) may occur across multiple stages, or major tasks, of the CIHLC. And despite the linear depiction of the CIHLC, an operator or team of operators may engage in several stages, or major tasks, simultaneously; for example, response and recovery analyses may commence even before an incident is fully characterized and declared. As a result, an operator, or even multiple operators, may be conducting similar cognitive work at different times in the CIHLC, with similar decision and information requirements. It may therefore be useful to consider the cyber operator's work in terms of the decisions they make, rather than specific stages or tasks, to remove any assumption that a cyber operator has already been exposed to information obtained in prior activity; each decision can stand alone.

Consequently, when designing visualizations to support cyber operators' cognitive work, we should consider re-focusing away from a task or stage orientation and more to a decision orientation. Rather than designing visualizations to support a specific stage or task, we should consider designing visualizations to support specific decisions or information requirements that cut across stages or major tasks in the CIHLC.

To design such visualizations requires further systematic research on not just the type of activity at each stage of incident handling, but also the specific decisions and the information requirements of those decisions, i.e., when facing cyber data to be analyzed, what questions do operators need to answer in order to make decisions? Documenting these decisions and analytic questions within the target work environment would provide visualization designers and developers with the specific problems that the visualizations need to address. In our subsequent research, we identified analytic questions that operators ask themselves in Stages 1 and 2, but substantial work remains to understand and verify the decisions and analytic questions at all stages of the CIHLC.

As we continue our research, we will need to address the absence of an accepted, standardized framework for developing and evaluating cyber security visualizations [15] [16]. We believe such a framework should identify how to specify a visualization's objective, enabling consensus from human factors, information visualization and cyber operations practitioners about the design and initial evaluation of the effectiveness of a

visualization. Such a framework should also support specification of the raw cyber data needed, and, more importantly, how that raw data needs to be transformed to support the specific visualization objective.

We hope that disseminating this work will contribute to the future development of human-centered visualizations for cyber operators by enabling human factors practitioners to better understand the cyber domain, as well as some of the practical requirements for operator performance in a variety of task environments.

Acknowledgments. This material is based on work funded by United States Air Force Research Laboratory under Contract No. FA8650-15-M-6632 with Secure Decisions. The material has been approved for public release and unlimited distribution.

References

1. Cyber Visions 2024, United States Air Force Cyberspace Science and Technology Vision 2012-2025 AF/ST TR 12-01, 28--29. (13 December 2012)
2. Bennett, K. B., & Flach, J. M.: Display and interface design: Subtle science, exact art. Boca Raton, FL: CRC Press. (2011)
3. Sawyer, B. D., Finomore, V. S., Funke, G. J., Mancuso, V. F., Funke, M. E., Matthews, G., & Warm, J. S.: Cyber Vigilance: Effects of Signal Probability and Event Rate. Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 58(1), 1771--1775 (2014)
4. Rasmussen, J., Ehrlich, K., Ross, S., Kirk, S., Gruen, D. and Patterson, J.: Nimble cybersecurity incident management through visualization and defensible recommendations. In: Proceedings of the Seventh International Symposium on Visualization for Cyber Security, ACM, 102--113 (2010)
5. Paul, C. L. K. Whitley, K.: A taxonomy of cyber awareness questions for the user-centered design of cyber situation awareness. In: Human Aspects of Information Security, Privacy, and Trust, (2013)
6. U.S. Department of Defense, Chairman of the Joint Chiefs of Staff Manual, Cyber Incident Handling Program: CJCSM 6510.01B, 10 July 2012 (Directive Current as of 18 December 2014)
7. D'Amico, A., Tesone, D., Whitley, K., O'Brien, B., Smith, M. and Roth, E: "Understanding the Cyber Defender: A Cognitive Task Analysis of Information Assurance Analysts". Report CSA-CTA-1-1 under Contract No. F30602-03-C-0260 issued by USAF, AFMC Air Force Research Laboratory (2005)
8. D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., and Roth, E.: Achieving cyber defense situational awareness: A cognitive task analysis of information assurance analysts. Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting, 229--233 (2005)
9. D'Amico, A. & Kocka, M.: Information assurance visualizations for specific stages of situational awareness and intended uses: Lessons learned. In: Proc of Workshop on Visualization for Computer Security (VizSec), 107--112 (2005)
10. Mahoney, S, et al.: A cognitive task analysis for cyber situational awareness. In: Proceedings of the Human Factors and Ergonomics Society Annual Meeting. Vol. 54. No. 4. SAGE Publications (2010)
11. Erbacher, R. F., et al.: A multi-phase network situational awareness cognitive task analysis. Information Visualization 9.3 204--219 (2010)
12. Buchanan, L., D'Amico, A., Horn, C. and Walczak, P.: NetDemon Final Report. Naval Network Defense Decision Making Model (N2D2M2), under Contract No. N00014-10-C-0374 issued by Office of Naval Research (2011)
13. National Collegiate Cyber Defense Competition (NCCDC), http://www.nationalccdc.org

14. Cyber Security Awareness Week (CSAW), https://csaw.engineering.nyu.edu
15. Langton, J.T., Newey, B.: Evaluation of current visualization tools for cyber security. In: Proc. SPIE 7709, Cyber Security, Situation Management, and Impact Assessment II; and Visual Analytics for Homeland Defense and Security II, 770910 (2010)
16. Staheli, D., et al.: Visualization evaluation for cyber security: Trends and future directions. In: Proceedings of the Eleventh Workshop on Visualization for Cyber Security. ACM, (2014)