A review methods for predicting adversarial cyber operations

Abstract. Abstract. Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract Abstract

# Introduction

The cyber domain is a dynamic and conditions of importance to cyber security frequently change. For example, new types of internet services are offered, software systems are updated, vulnerabilities are made public, and new forms of attacks are developed. In a dynamic environment as this, situational awareness both difficult and important to achieve. Consequently, a considerable number of papers can be found on the topic of cyber situational awareness. For instance, Franke and Brynielsson (2014) found 102 papers explicitly labeled as research on the cyber situational awareness and Shiravi et al. (2012) describes 38 solutions for visualising cyber security events.

According to the definition of Endsley (1995a, 1995b), situational awareness concerns the ability to perceive relevant elements, comprehend what they mean, and make projections about the future. These projections serve as input to decisions. Cyber security decisions mainly concerns ways to manage threats posed by adversaries. Thus, decision makers in the cyber security domain need to perceive what the adversaries do, comprehend what their actions mean, and predicting future cyber attacks. This paper concerns the last of these, i.e. predicting adversaries’ future actions, intentions, or plans. Only 15 papers the review by Franke and Brynielsson (2014) were classified as to deal with projections of the future. Thus, despite the apparent value of predictive analytics related to cyber security, there are relatively few ideas on how to approach the issue.

There are a large body of literature on methods for assessing and analyzing ways that attackers can attack a system. These typically assume a generic threat model and aim at finding possible attacks rather than likely attacks. For example, a large number of attack graph tools has been presented (Hong et al., 2017). These make no predictions about what adversaries will attempt to do, but rather what they could do. However, the accuracy of such models appears questionable when their output is compared to attackers actions (Sommestad and Sandström, 2015). In addition, attackers seldom not try all possible attacks, e.g. because they have certain favorite tools or try to avoid detection. For that reason, some have developed mathematical models over how adversaries and penetration testers behave in a network (Sarraute, 2012)(Sarraute et al., 2013)(Hoffmann, 2015) (Backes et al., 2017). While the aim of this research is to plan attacks that realistically simulate human attackers, this work is focused on simulating a generic attacker and do not acknowledge adversaries have different talents or incentives. Thus, they do not make predictions of attacks based on the dynamic or variable threat model that organizations are exposed to. In addition, the analyses do not take observed events, e.g. intrusion detection alerts, into account when they.

There are plenty of general methods for performing event processing and predicting future events (e.g. software failures) from the current situation, typically by applying sophisticated methods such as machine learning on historical data (Fülöp et al., 2010). However, not all of these are applicable to the dynamic and adversarial nature of cyber security. There are also approaches (e.g., (Bell et al., 2002) (Kott and McEneaney, 2006)) specifically related to the predictive analysis of adversarial courses of action in non-cyber domains, although the efficacy and robustness of these approaches remain debatable. Nevertheless, there are threat intelligence with the potential of supporting predictions. For example, it is known that a spike in attacks occurs a while after a vulnerability or an exploit code is publically released (Ramirez-Silva and Dacier, 2007). Thus, predictions of cyber operations should be possible to some extent.

This paper is a product of member of the research task group IST-129 of NATO, specifically focusing on predictive analysis of adversarial cyber operations. It presents the main output of the groups work: an analysis of issues related to the predicting adversarial cyber operations and a review of approaches presented in the extant literature.

The paper is structured as follows. Section 2 describes the prediction problem and some issues associated with it; Section 3 describes the method used in the literature review; Section 4 continues with an overview of methods proposed in the literature, with a particular focus on the elements they use as input and the elements they make predictions about; Section 5 discusses limitations with the available approaches and potential avenues for future research.

# The problem of predicting adversarial actions and intentions

To make accurate predictions is an aim of most scientific theories and predictions are integral in many domains. However, the problem of predicting predict adversarial cyber operations is associated with a number of issues: intelligent agents, the tempo of the decision making, data availability, and the absence of general laws. None of them is unique to the cyber security domain, but together they create a complicated and difficulty problem.

## Intelligent agents

The problem involves predicting actions or intention involves prediction of what an intelligent agent. The adversary can change plans, be irrational, and employ tools tactics and procedures that are unknown. Other domains largely occupied with predictions, e.g. weather forecasting and meteorology, does not involve intelligent adversaries of this type. In other domains predictions are made in a situation that can involve intelligent agents behaving as adversaries, but can also rely on the law of great numbers and rely on overall risk assessments. For instance, insurance companies needs to deal with the risk of frauds and moral hazards. However, insurance companies can typically estimate the overall risk for all insured clients and cover it with higher premiums [REF]. Thus, the adversarial dimension cannot be ignored, but they do not have to single out individuals with bad intentions or predict which individuals that will act maliciously the next day. In other domains, such as chess playing, military warfare, the role of adversarial agents is as essential as it is in the cyber security domain. In chess computers search use the minimax algorithm to assess the best course of action given the options the computer and the opponent have for different courses of actions[REF], i.e. a highly intelligent opponent is assumed. In the military domain, maneuver warfare aims at doing tactile maneuvers that shock and disrupt an intelligent opponent [REF], e.g. by deceiving and surprising the opponent.

The involvement of (intelligent) adversaries makes the problem more dynamic and thereby influence the types of predictions that are useful. For example, a solution which can be easily manipulated to make incorrect predictions will be of limited use to anyone facing an intelligent adversary. It could even hamper a defence to rely on such a solution.

## Decision making tempo

Not all decisions and predictions of relevance to the cyber security domain needs to be super-fast. Some incidents play out over the course of months and other play out during seconds; some useful predictions concern adversarial campaigns over the course of the following year and some useful predictions concern anticipation of which machine data access the adversary will gain with the commands arriving within a second. The cases when decisions needs to be made within seconds makes prediction of adversarial cyber security operations problematic, and very different from the cases for weather forecasts and actuarial predictions. Such cyber security decisions have a situation more like that of automated trading systems for stocks or control systems in electrical power systems.

The decisions that needs to be taken at an incredibly high speed typically involves actions to thwart scripted attacks embedded in software, e.g. as antivirus software does to prevent known computer viruses and computer worms. However, [DSB] points out that cyber automation is not being applied at the rate it should, and contemporary antivirus software is not at predicting previously unknown attacks [REF]. To thwart known attacks that are scripted, a defender needs to make decisions as fast as the attacker (or its code) does. This can be expected to require some degree of automation, and thereby require computational models identifying reasonable defensive action.

## Archival data

Despite being data-intensive, the cyber security domain suffers from a lack of data to base decisions on. First, confidentiality and privacy issues hinders organizations from effectively sharing threat intelligence and raw data related to known incidents with each other. This results in simulating or creating data stream which are not representative of the “real world”. Second, when data is available, the ground truth is rarely known in any detail. The limitations of intrusion detection systems and forensic methods mean that some adversarial operation will be go unnoticed and that many details related to them are uncertain or missed. For instance, it is possible that some actions are taken just to misguide analysts analyzing logs. Third, the field is under constant development, with a constant stream of new technologies, system changes and usage patterns. Attacks are also adapted to circumvent new security technologies. When security systems effectively predicts an attack and can thwart it, the attackers can be expected to invent a new variant that is more difficult to predict. Thus, event data which is a couple of years old may be useful when models on car insurances or financial processes, but have limited value to cyber operations.

These data problems more or less prohibit straightforward data-intensive solutions such as machine learning. The confidentiality issues, the ability to model and simulate large, complex systems and the lack of a ground truth in operational systems also make it difficult to test the merits of a predictive solution. This can be compared to the case for robot trading, where it is straightforward to assess the performance of solution. In the cyber security domain, where success against a deceptive adversary is difficult to observe, that that type of straightforward feedback is rarely available.

## Fundamental laws

Another issue that, in most cases, the current state in a cyber system and the fundamental laws it operates according to in only partly known by a system administrator. In most cyber systems, the systems are just too complex for an operator to keep track of everything. Tools such as network vulnerability scanners also have limitations, and report on approximately half of the vulnerabilities in a system (Holm et al., 2011). Thus, while it is theoretically possible to know exactly how a computer system is constructed and the rules that users obey to, it is often practically impossible. In fact, it is sometimes stated that the adversary knows more about your network than you do [REF and quote needed]. Furthermore, many cyber security attacks are specifically about breaking the “laws” a system administrator try to enforce and/or believe exist. For example, a buffer overflow vulnerability allows attackers to take control over a machine’s the execution flow in when they should be allowed to merely input data into the machine. It is therefore difficult to accurately reason about what an adversary can do.

The fact that an administrator only have a partial understanding of the cyber system’s present state and only have a partial understanding of the actions that are possible leads to obvious problems for predictive methods. The situation is completely different from the situation on a chess, where the rules of the game are clear; more similar to the case for trading robots, where information about the situation can differ between different actors; and closely related to the situation in warfare, where “information superiority” is considered a critical determinant of mission success (Lamaa et al., 2014).

## Summary

The four characteristics listed above make the problem tough. On the other hand, the utility of a good prediction is high, because in theory, a system administrator or tool with full rights in the system can thwart any attack predicted in time. Consequently, some of the more basic and practically useful cyber security technology involve an element of prediction and direct (automated) intervention. For example, antivirus systems are able to predict that software is malicious because they use signatures of such software and a firewall can anticipate an attack by recognizing external IP-addresses known to be malicious.

Trivial cases like this, where known attacks codes and known adversaries are involved, are not the focus of the contemporary research on this problem. Nor is the focus of the contemporary research on prediction of adversarial cyber operations the anticipation of completely new forms of attacks performed by resourceful adversaries such as nation states. Most solutions are in-between these two extremes and make probabilistic statements based on explicit assumptions on the attacks the adversary is capable of. In terms of the six levels of threat defined by the US Defence Science Board describes six levels of threats [Defense Science Board] most of the research on predicting adversarial cyber is focused on threat level three and four, which discover previously unknown vulnerabilities and develop exploit code for these. Hence, the present review will primarily deal with such research.

# Review procedure

This section describes the inclusion criterions for the review, the method used to identify the relevant literature, the elements extracted from the literature and process of extracting this information.

## Inclusion criterion

As noted above, the issue predicting adversarial cyber operations involves both straightforward cases were a known threat is to be recognized and more or less impossible cases where previously unknown attacks performed by professionals should be predicted. The panel and the literature search aimed at focusing on research in-between these two extremes. It was also recognized that much of the extant research on cyber security have some relation to prediction. For example, when the relationship between cyber variables are investigated in terms of statistical relationships this offers potential input to prediction models. However, as this review is mostly concerned with existing prediction models, and not surveying potential building blocks of new ones, such research was excluded. Thus, the primary inclusion criteria was that the papers should describe a model *explicitly developed* for predicting adversarial cyber operations.

In addition, the predictions produced by the model should be able to support a decision maker within an organization to secure their cyber environment. This meant that papers listing attacks that were possible to perform against the cyber environment were excluded they did not make statements about the likelihood that the attacks would be performed within a certain time frame. For instance, most papers on attack graphs, which rarely state how likely attacks are to happen, were excluded. Similarly, papers on models producing generic predictions, such as “*more attacks of type X will happen next year*”, were excluded unless it was possible to tune the predictions based on information related to a specific organization or cyber environment. Finally, some papers were excluded because they were too abstract and superficial. For example, papers stating basic ideas about how threat intelligence could foster prediction, without detailing what this threat intelligence comprise of, were excluded.

## Literature search

Some initial attempt with the definition of search terms that could be used to target literature related to predicting adversarial cyber operations. However, it was soon acknowledged that this literature was too diverse and scattered to be identified by a straightforward search in literature databases. Fortunately, the panel members participating in the review process was diverse set of researchers, with backgrounds in cyber security, mathematics, forensics, combat assessments, visualisation, and military intelligence. This diversity helped to identify a fifteen topics that were related. These topics included, among others, “the cyber OODA-loop”, “cyber attack profiling”, “data fusion approaches”, “risk and incident management”, “situation description methods”, “the relationship between capabilities and actions”, “unknown vulnerability detection”, “attack probability indicators”, and “multi-step attack models”.

Panel members were assigned to topics they had previous knowledge of and searched for literature within this topic that could match the search criterion. These searches typically started with searches in scholarly databases to identify research papers and internet searches to find “grey literature” (e.g. technical reports). Such searches were complemented by inspection of references used in papers considered relevant. The search process hardly can be described as structured. However, the range of competences and background among the panel members ensured that it covered a wide range of topics related to cyber security. A database of 36 papers had been identified and passed the inclusion criterion after the group screened the paper’s title and abstract. After review of the full text XX papers were found to meet the inclusion criterion. These XX can not be said to represent an all available papers related to prediction of adversarial cyber operations, but it is the group’s opinion that they are likely to indicate the state of research in this area.

## Information extraction

The literature addressed the prediction problem from a number of different angles, and at different levels of abstraction. At first, an input-output-perspective attempted to broadly characterize the data the models used. The model of STIX [REF] was used for this purpose. However, the analysis soon showed that it was that most of the models used more or less the same data objects in STIX, namely: vulnerability-information, attack patterns, indicators, intrusion sets, and other observed data. In addition, it turned out to be non-trivial to classify the data used in a reliable manner, partly because of the different levels of abstraction used in the papers. Instead, the following information was extracted to characterize the models:

1. If a particular formalism was used or proposed.
2. Data used as input for the prediction model.
3. The data produced as output by the prediction model.
4. The scalability of the solution or implementation.

To further characterize the models it was extracted how they handled the following issues:

1. Adversaries attempting to tampering with/fooling the prediction method.
2. The time it takes to make the prediction and timing issues.
3. Availability of data needed for analysis or model construction.
4. Assumptions concerning knowledge of system vulnerabilities and attacks.

Furthermore, information was extracted to characterize the maturity of the research in terms by assessing:

1. If the model had been implemented in prototype and what Technology Readiness Level the model was on.
2. If the model’s its usefulness for was demonstrated, e.g. in a case study.
3. Tests or other evaluations of accuracy of the prediction model.

These nine information elements was extracted as quotes and descriptive summaries of descriptions provided in the reviewed papers.

# Results

## model characteristics

Descriptive text and listing of the papers that are included.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reference** | **Proposed formalism** | **Input data** | **Output data** | **Scalability** |
| (Lei and Li, 2008) |  |  |  |  |
| (Cheng et al., 2011) |  |  |  |  |
| (Santos Jr., 2003) |  |  |  |  |
| (Colbaugh and Glass, 2012) |  |  |  |  |
| (Sarabi and Bailey, 2015) |  |  |  |  |
| (Yang et al., 2009) |  |  |  |  |
| (Qin and Lee, 2004) |  |  |  |  |
| (Shen et al., 2007) |  |  |  |  |
| (Greitzer and Frincke, 2010) |  |  |  |  |
| (Yang et al., 2008) |  |  |  |  |
| (Lee et al., 2006) |  |  |  |  |

## Management of Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reference** | **Adversaries** | **Timing issues** | **Data availability** | **Knowledge assumptions** |
| (Lei and Li, 2008) |  |  |  |  |
| (Cheng et al., 2011) |  |  |  |  |
| (Santos Jr., 2003) |  |  |  |  |
| (Colbaugh and Glass, 2012) |  |  |  |  |
| (Sarabi and Bailey, 2015) |  |  |  |  |
| (Yang et al., 2009) |  |  |  |  |
| (Qin and Lee, 2004) |  |  |  |  |
| (Shen et al., 2007) |  |  |  |  |
| (Greitzer and Frincke, 2010) |  |  |  |  |
| (Yang et al., 2008) |  |  |  |  |
| (Lee et al., 2006) |  |  |  |  |

## Model maturity

|  |  |  |  |
| --- | --- | --- | --- |
| **Reference** | **Technology readiness level** | **Usefulness demonstrated** | **Accuracy demonstrated** |
| (Lei and Li, 2008) |  |  |  |
| (Cheng et al., 2011) |  |  |  |
| (Santos Jr., 2003) |  |  |  |
| (Colbaugh and Glass, 2012) |  |  |  |
| (Sarabi and Bailey, 2015) |  |  |  |
| (Yang et al., 2009) |  |  |  |
| (Qin and Lee, 2004) |  |  |  |
| (Shen et al., 2007) |  |  |  |
| (Greitzer and Frincke, 2010) |  |  |  |
| (Yang et al., 2008) |  |  |  |
| (Lee et al., 2006) |  |  |  |

# Discussion

## Research maturity, trl discussion, what is the impact of doing this on strategic/operational/tactical levels etc.

* There are few papers many of which had poor citation records suggesting that there is a lack of knowledge in this area.

## Prospect for predictive analysis of adversarial cyber operations

* Some discussions about what one could expect in the future. How to deal with the issues etc.

## Suggestions for future work (initial list)

* Prediction may be enhanced or streamlined if feedback is included earlier and in multiple areas of the OODA loop (topic for future research). For instance, Kalman filters could be used to improve predictions if real-time results are not a requirement.
* Analyse event relationships across different TTPs
* Low Observables - There may be components of an attack beyond observable components … how do we identify unobservable attacks (what do we have to do to make them observable)
* Given the point in conclusions below on TRLs, could be research in this area also
* If we get a prediction in real time, how does this impact potential COAs?
* How can we define and prove metrics on predictability?
* How can we create and validate models of predictability?
* Perform similar evaluation using latest STiX revisions to see if impact on conclusions

## Conclusion (initial potential list)

1. What is the benefit of this research…..should answer this as a conclusion/finding/position
   1. Lexicon for what is a prediction vs. an identification(?) is , in some of the papers, blurry
   2. We were able find very little in the way of directly applicable research into prediction (as opposed to identification) ….
      1. poses a risk to cyber defenders
      2. Continues to keep cyber defense at a temporal disadvantage
2. Open area for experimentation guided by user requirements and architecture
3. Less on this area than we originally thought. Doing the research in plenary was a good way to uncover this (we should take credit for *how* we did this….)….group setting / cross checking / etc.
4. The only case of a single analytic “prediction” approach is the known, known and that is identification / pattern matching / deterministic. (could claim it is prediction with 100% certainty)
5. For the known, unknown appears that multiple paths are needed a conditional predication analytic (i.e., dynamically creating/spawning a dedicated/specific (possibly biased or “tuned” towards an outcome) process with only 1 result in mind) and then integrate the results across the analytics spawned;
   1. The next event you predict isn’t necessarily dependent on the previous events. May not follow a TTP….but cannot ignore historical information on either incidents or events
   2. Analytic tuned to being part of a known TTP/actor
   3. Analytic tuned to being part of a unknown TTP/known actor
   4. Analytic tuned to being part of a unknown TTP/unknown actor
   5. Analytic tuned to being part of a spoofed TTP
   6. Can we divide this ala statistics into certainty and uncertainty?
   7. If we see something, it is a primary attack of possibly a result of an attack elsewhere (secondary impact)
6. Is it possible that there is a strong prediction pattern that follows a theory that to break into a given system, an attacker will try for the path of least resistance…..lowest common vulnerability exposed? Can there be a “common” TTP?
7. Is the current state of the art real time enough to impact this? Our analysis that puts a relative Technology Readiness Level on the papers will frame this position. Notionally supported by some of the responses to the cfp…and if this is true, it notionally supports the argument on CSOC or cyber defence maturity
   1. K, K = about 8 or 9 since not full automation
   2. K,U = 5 or 6?
   3. U, U = maybe 1 or 2?
   4. Do we need to have definitions of TRL for this activity or are the general accepted definitions good enough…our interpretation of TRL for this could also be a good contribution

# References

Backes, M., Hoffmann, J., Künnemann, R., Speicher, P., Steinmetz, M., 2017. Simulated Penetration Testing and Mitigation Analysis. Saarland.

Bell, B., Santos Jr, E., Brown, S.M., 2002. Making adversary decision modeling tractable with intent inference and information fusion. Proc. 11th Conf. Comput. Gener. Forces Behav. Represent. 535–542.

Cheng, B.C., Liao, G.T., Huang, C.C., Yu, M.T., 2011. A novel probabilistic matching algorithm for multi-stage attack forecasts. IEEE J. Sel. Areas Commun. 29, 1438–1448.

Colbaugh, R., Glass, K., 2012. Predictive defense against evolving adversaries. ISI 2012 - 2012 IEEE Int. Conf. Intell. Secur. Informatics Cyberspace, Border, Immigr. Secur. 18–23.

Endsley, M.R., 1995a. Toward a Theory of Situation Awareness in Dynamic Systems. Hum. Factors 37, 32–64.

Endsley, M.R., 1995b. Measurement of Situation Awareness in Dynamic Systems. Hum. Factors J. Hum. Factors Ergon. Soc. 37, 65–84.

Franke, U., Brynielsson, J., 2014. Cyber situational awareness – A systematic review of the literature. Comput. Secur. 46, 18–31.

Fülöp, L.J., Tóth, G., Rácz, R., Pánczél, J., Gergely, T., Beszédes, Á., Farkas, L., 2010. Survey on Complex Event Processing and Predictive Analytics. Proc. Fifth Balk. Conf. Informatics 26–31.

Greitzer, F.L., Frincke, D.A., 2010. Combining Traditional Cyber Security Audit Data with Psychosocial Data: Towards Predictive Modeling for Insider Threat Mitigation. In: Advances in Information Security. pp. 85–113.

Hoffmann, J., 2015. Simulated Penetration Testing: From“ Dijkstra” to“ Turing Test++.” ICAPS 364–372.

Holm, H., Sommestad, T., Almroth, J., Persson, M., 2011. A quantitative evaluation of vulnerability scanning. Inf. Manag. Comput. Secur. 19, 231–247.

Hong, J.B., Kim, D.S., Chung, C.-J., Huang, D., 2017. A survey on the usability and practical applications of Graphical Security Models. Comput. Sci. Rev. 26, 1–16.

Kott, A., McEneaney, W.M., 2006. Adversarial reasoning: computational approaches to reading the opponent’s mind. CRC Press.

Lamaa, A., Jansen, M., Trepant, H., Suddards, A., 2014. Achieving information superiority Five imperatives for military transformation.

Lee, S., Lee, D.H., Kim, K.J., 2006. A conceptual design of knowledge-based real-time cyber-threat early warning system. Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics) 4331 LNCS, 1006–1017.

Lei, J., Li, Z.T., 2008. Using network attack graph to predict the future attacks. Proc. Second Int. Conf. Commun. Netw. China, ChinaCom 2007 403–407.

Qin, X., Lee, W., 2004. Attack plan recognition and prediction using causal networks. Proc. - Annu. Comput. Secur. Appl. Conf. ACSAC 370–379.

Ramirez-Silva, E., Dacier, M., 2007. Empirical Study of the Impact of Metasploit-Related Attacks in 4 Years of Attack Traces. Adv. Comput. Sci. – ASIAN 2007. Comput. Netw. Secur. 4846, 198–211.

Santos Jr., E., 2003. A Cognitive Architecture for Adversary Intent Inferencing: Knowledge Structure and Computation. Proc SPIE 17th Annu. Int. Symp. Aerospace/Defense Sens. Control. Vol 5091 182–193.

Sarabi, A., Bailey, M., 2015. Predicting Cyber Security Incidents Using Feature-Based Characterization of Network-Level Malicious Activities Categories and Subject Descriptors. Int. Work. Secur. Priv. Anal. (SPA ’15) 3–9.

Sarraute, C., 2012. POMDPs Make Better Hackers : Accounting for Uncertainty in Penetration Testing. In: AAAI’12 Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence. Toronto, Ontario, Canada, pp. 1816–1824.

Sarraute, C., Buffet, O., Hoffmann, J., 2013. Penetration Testing == POMDP Solving? 66–73.

Shen, D., Chen, G., Cruz, J.. J.B., Haynes, L., Kruger, M., Blasch, E., 2007. A Markov game theoretic data fusion approach for cyber situational awareness. Proc. SPIE 3, 65710F–65710F–12.

Shiravi, H., Shiravi, A., Ghorbani, A., 2012. A Survey of Visualization Systems for Network Security. IEEE Trans. Vis. Comput. Graph. 18, 1313–1329.

Sommestad, T., Sandström, F., 2015. An empirical test of the accuracy of an attack graph analysis tool, Information and Computer Security.

Yang, S.J., Byers, S., Holsopple, J., Argauer, B., Fava, D., 2008. Intrusion activity projection for cyber situational awareness. IEEE Int. Conf. Intell. Secur. Informatics, 2008, IEEE ISI 2008 167–172.

Yang, S.J., Stotz, A., Holsopple, J., Sudit, M., Kuhl, M., 2009. High level information fusion for tracking and projection of multistage cyber attacks. Inf. Fusion 10, 107–121.