# DECISION SUPPORT METHODS IN CYBERSECURITY EDUCATION*

TOMASZ M. KOMOROWSKI[1] AND TOMASZ KLASA[2]

[1] *Institute of IT in Management*
*Faculty of Economics and Management, University of Szczecin*
*Mickiewicza 64, 71–101 Szczecin, Poland*

[2] *Faculty of Economy and Information Technology*
*West Pomeranian Business School in Szczecin*
*Żołnierska 53, 71–210 Szczecin, Poland*

(received: 6 February 2019; revised: 28 February 2019;
accepted: 12 March 2019; published online: 28 March 2019)

**Abstract:** Even the best technology will be ineffective if not used appropriately, therefore education and training about cybersecurity principles and programs are essential components of any cybersecurity strategy. This article presents selected models of the decision support theory from the point of view of cybersecurity education. The analysis of scientific literature and the available research results serve as a base to characterize approaches to raise the awareness of decision-makers about potential cyber threats and the development of appropriate attitudes and the conscious use of information systems and digital resources. The main part of the article is devoted to the issue of the use of teaching methods to increase the involvement of learners. It also describes examples of selected models of the game theory used in IT security education, including examples of simulation games dedicated to decision-making in the domain of IT security.

**Keywords:** smart manufacturing systems, Industry 4.0, information technology, operational technology, industrial automation and control system, functional safety, cybersecurity, risk evaluation

**DOI: https://doi.org/10.17466/tq2019/23.2/f**

## 1. Foundations of Cybersecurity

Education and awareness about the cybersecurity risk is one of the elements of constructing solid legal foundations [1] – a legal and policy framework for a national cybersecurity strategy. All countries in the EU are obligated to enact and keep up-to-date the cybersecurity strategy. It is not a simple mission, but

* This paper was presented during the MEDEA symposium on Art-Science-Technology, 3–10 September 2016, Zakynthos, Greece.

there are many alliances cooperating to achieve this goal. BSA – the Business Software Alliance (www.bsa.org) is the leading organization representing the interests of software companies in dealing with governments and in the worldwide international market. The BSA, in a published document called *The Building Blocks of a Strong Legal Cybersecurity Framework* [1] established a comprehensive legal and policy framework that can be built in each country. It relies on the following key principles:

- risk-based and prioritized;
- technology-neutral;
- practicable;
- flexible;
- respectful of privacy and civil liberties.

Cyber-threats come in many variants. An objective assessment of risk allows establishing a hierarchy of priorities or critical sectors. Policy makers need to be confident that cyber protections are focused on those areas, where the potential for harm is the most significant. Examples of risk assessment and prioritizing methods are described using, *inter alia*, the Survivability System Analysis (SSA) with the Probability Risk Assessment (PRA) [2], or Bayesian Defense Graphs and Architectural Models [3]. Some methods are widely used and adapted, such as MEHARI or CRAMM, others are recent proposals – *e.g.* FoMRA [4]. A technology-neutral approach to cybersecurity protection is very important to ensure access to the effective solutions created and tested by many experts and communities [5]. The factor „practicable" is measured by the effectiveness of the strategy, but any strategy is only as effective as it is adoptable for the largest possible group of critical assets and implementable across the broadest range of critical actors [1]. Flexibility is revealed as managing the cyber risk by a cross-disciplinary function and not a one-size-fits-all approach. Each economic activity concerned with the processing, system and business faces distinct challenges, and the range of actors and must have the flexibility to address their unique needs [6]. Security requirements should be balanced with the need for protection of privacy and civil liberties. To ensure that requirements and obligations are proportional, a declaration intended to provide the confidence of fundamental rights is strictly necessary. People, processes and technology are equally important to ensure cybersecurity and even the best technology will be ineffective if not used appropriately [1].

Any cybersecurity strategy consists of the four essential components:

- raising awareness;
- education and training;
- principles and policies;
- processes and programs.

A distal portion of this article will present selected methods of the game theory and decision support systems which can be helpful in the implementation of the above mentioned components.

## 2. Game theory and Cybersecurity

Many people of the whole world think about how to find a most effective way to teach cybersecurity. Game theory can be one of the solutions of this problem. Game theory is used as a framework for modeling situations with more than one decision maker, named „player". This approach is often used in many disciplines [7].

In games, as in the real world, there is no universally optimal decision, as both parties take independent decisions that influence the effects obtained by the other party. Research in the area of game theory has developed many reasoning algorithms for choosing a strategy that will result in the best possible effect [8].

Usually, a game model includes at least three obligatory and two optional elements (Figure 1). The first element is a player or players, who participate in the game. The second obligatory element are strategies (each player has many move options – strategies). The third element is called „payoffs" and consists (related to each player) of a combination of strategy choice results (outcome). The fourth (optional) element is information about sequences of moves made by the players. The fifth element is knowledge about all facts that are important to the players when making their moves.

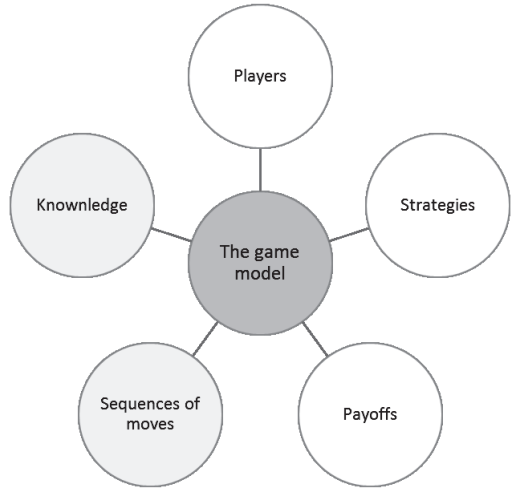


**Figure 1.** Game model elements
Source: Author's own work based on [8]

In some cases, it is necessary to rely the decisions taken on the probability distribution over pure, simple strategies. This approach is called mixed strategies and is intended to prevent the opponent from an easy prediction of the planned steps.

For instance, in the case of the *Rock, Paper, Scissors* game, if further actions of the opponent are predictable, they can be easily countered and the opponent can be defeated. Thus, it is important to take actions in as an unpredictable way

as possible, to hide the chosen strategy. Action randomization based on mixed strategies is one of the ways to obtain such a goal.

There are different ways of game analysis. Usually, the goal is either to predict future steps that are likely to happen during the game or to find a strategy for a chosen player that will provide the highest payoff. To achieve the second goal, it might be necessary to predict a number of future moves of the opponent.

### *2.1. Nash Equilibrium Concept*

Different approaches to games analysis are also known as solution concepts. One of the well-known examples is the Nash equilibrium concept, where all players take the optimum strategy (see Figure 2. and Figure 3). This means that each of the players has predicted properly the strategy of the other players and has chosen the best (optimal) response to that strategy.

The Nash equilibrium, in the version with zero sum games, is where one player loses what the other player wins, or vice versa. The game presented in Figure 2 has the Nash equilibrium in the element [a3; b1] in the payoff matrix, which is the highest in the column and also the lowest in the row (payoff minimization rule).

| | | Player 2 | | |
|---|---|---|---|---|
| | | b1 | b2 | b3 |
| Player 1 | a1 | 2 | 3 | 6 |
| | a2 | 1 | 7 | 4 |
| | a3 | 3 | 5 | 4 |

**Figure 2.** Nash equilibrium with zero sum games
Source: [9]

The Nash equilibrium (version with non-zero sum games), where players try to maximize their own profit, is in this case (Figure 3) also in the element [a3; b1]. Player 1 and Player 2 try to maximize their profit based on the second player's choice.

| | | Player 2 | | |
|---|---|---|---|---|
| | | b1 | b2 | b3 |
| Player 1 | a1 | 3;5 | 4;8 | 2;6 |
| | a2 | 1;3 | 2;4 | 6;1 |
| | a3 | 8;5 | 7;2 | 3;3 |

**Figure 3.** Nash equilibrium with non zero sum games
Source: [9]

## 3. Game Theory and Classes of Games

There are three classes of games that are related to cybersecurity problems:

- security games;
- deception games;
- simple educational games.

Decision making in the area of security is usually based on opposite interests of the attacker and the defender. For this reason, the game theory has been recently adapted in homeland security and critical infrastructure protection, to introduce randomization and harden prediction of a chosen strategy in this way. It is important especially because attackers can follow any changes in the resource allocation and build the defender's strategy patterns on that basis.

### *3.1. Simple example of a security game*

The example in Figure 4 is a very simple case of a security game with species, a set of possible targets (*e.g.*, data base, web server, mail server...).

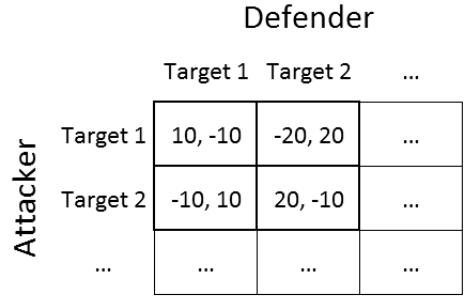


**Figure 4.** Simple example of a security game
Source: Author's own work based on [8]

While the attacker can focus on a chosen target, the defender wants to counter the attack, although it is not known which field is the target. Of course, the defender's resources are limited and protecting the whole area in a sufficient way is impossible, so it is necessary to choose which areas to protect, and which to leave unprotected.

There are four payoff values for each of the targets. The attacker gets a higher value if the target was not protected, while the defender gets a higher value if the target was protected. For example, the decision maker (Defender) has only one resource (firewall license) to protect two targets (two web servers in different localizations). The Hacker (Attacker) can harm one of these resources. If the decision maker protects the wrong resource, then the „payoff" for the attacker will be higher (the Hacker will be the winner).

### 3.2. Common rules of security games

Usually the attacker is modeled as capable of observing and learning the defender's strategy before committing the attack. The defender, at the same time, is usually forced to decide where to allocate limited countermeasures, to strengthen protection against the attacker, who can react to the defense strategy.

Strategic decision-making in virtual warfare is very similar to protection of the physical infrastructure:

- resources are limited;
- it is necessary to manipulate the information that is accessible to the attacker;
- it is necessary to learn the attacker's strategy.

Since the game theory can handle many of these problems, security games become more and more popular.

### 3.3. Deception games

It is often based on utilization of randomized strategies to bluff. Such randomization of actions is intended to make prediction of the current resource allocation harder – when acting in the same way, no matter how well the defense is prepared, it is harder for the attacker to notice that the target is actually unprotected, *e.g.*:

- for physical security: dummy/fake cameras;
- for information security: various documents (politics) which have defined fake rules with restrictions (for example for scanning all digital documents sent via LAN).

Dummy cameras are those that look as real as the actual thing but are fake. They come in a variety of shapes and sizes. People can choose depending on what works best for them. While most cameras have basic features, the more advanced ones also come with zoom, pan, and tilt features.

The effects of deception can be valuable educationally and rich in experience, but often have following implications:

- they are easily identifiable;
- they cannot prove anything;
- they create a false sense of security.

Moreover, using elements of fake security could lead to legal issues (*e.g.* several home and business owners have been sued for using fake security cameras).

### 3.4. Honeypot as an example of deception game

The game theory with the deception perspective can be explored as creating and deploying honeypots. In this case game theory is used to optimize the information learned about the attacker's strategies by modeling the progress of the attack [8].

Some honeypot options use the game theory to optimize the probability that the attacker will attack an artificial and specially prepared server (honeypot) but not a real system. The attacker cannot distinguish between real servers and

honeypots, but at the same time not all computers in the network are identical to the attacker.

The alternative of a honeypot model gives the attacker the option of probing servers before the attack. The probe results are only useful, if the defender voluntarily discloses some information to the attacker.

### *3.5. Simple educational cybersecurity games*

Games of this class are very simple and similar to many other digital activities like „fun and learn". They are designed to help people to learn about cybersecurity rules and security behavior in the digital world. There appears to be a close association between play and learning. Computer games enhance learning through visualization, experimentation and creativity of play, and often include problems that develop critical thinking [10]. The simple educational cybersecurity games are focused on achieving common goals, *e.g.*:

- explain the basic terms and notions related to the cybersecurity knowledge;
- teach the rules of security behavior in the digital world;
- explain what will happen when the behavior is not correct;
- present cyberthreats and methods of cyberprotection.

## 4. Implementation of DSM in solutions for cybersecurity education – practice examples

Implementation of Decision Support Methods can be often seen as a popular type of games. One of the popular open source advanced cyber games was created by the Digital Forensics and Cyber Security Center at the University of Rhode Island and was sponsored by the U. S. National Science Foundation through the Open Cyber Challenge Platform[**]. The general OCCP concept is based on the Virtual Scenario Network (VSN) – a network of virtual machines representing an organization's IT infrastructure (network, servers, workstations, data stores, IT tools, *etc.*). Each virtual machine (the number of machines depends on the chosen scenario) can be imported to the game administrator's PC host (see Figure 5). Free software and scenarios with documentation are ready to use for classroom or competition purposes.

This platform can be explored also by contributors. An existing scenario can be modified or a new scenario can be created and uploaded to the community.

The base concept of an OCCP game implies cooperation of four teams. The Gray Team is represented by scripts that generate a „normal" use of the VSN services. The Red Team can be people or scripts that attack the VSN to deny or corrupt services, steal data, *etc.* People or scripts that represent the IT staff for the VSN – are called the Blue Team. The last is the White Team – people and scripts that monitor/support the system, and officiate/score the instance of challenge.

[**] Open Cyber Challenge Platform `https://opencyberchallenge.net/`

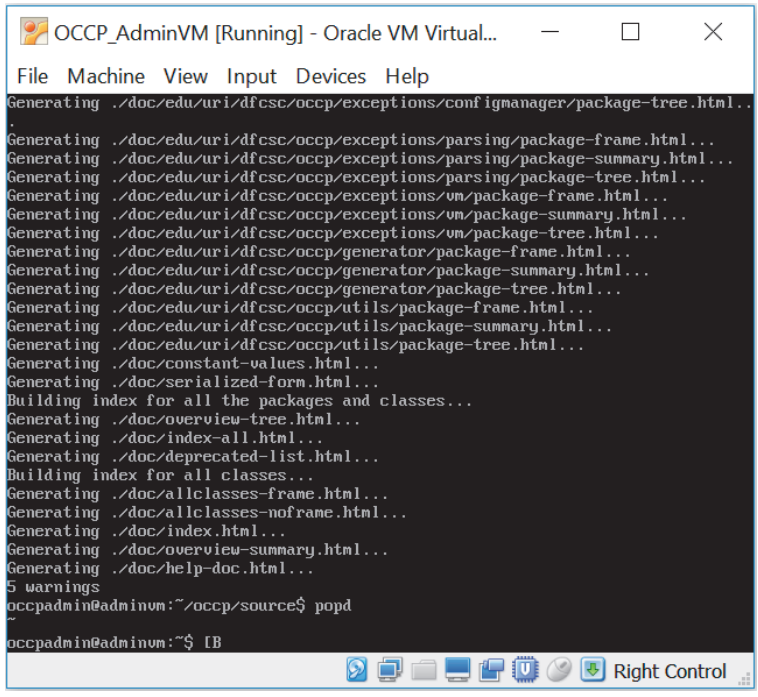


**Figure 5.** OCCP Admin Virtual Machine
Source: Author's own work

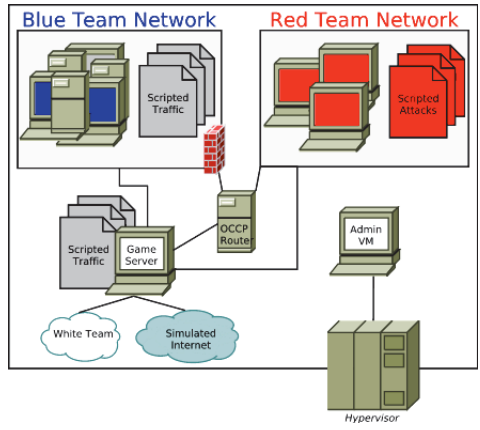


**Figure 6.** Teams in OCCP game
Source: `https://opencyberchallenge.net/`

The scenarios allow the implementation of at least three types of game: network deference, secure programming or penetration testing, digital forensics and malware analysis games.

The first scenario teaches how to protect a network. The Blue Team are students and Red Team are scripted attacks. During the game positive points are assigned to the Blue Team for services kept active, and negative points are

assigned to the Blue Team for data stolen and services denied. In other scenarios also negative or positive points can be assigned for data stolen and services denied (score visualization in Figure 7). Sometimes students must find what data has been stolen and who has done it.

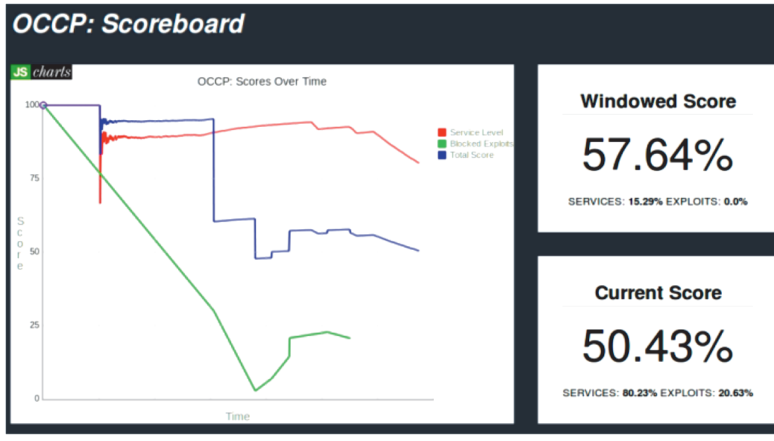


**Figure 7.** OCCP scoreboard visualization
Source: `https://opencyberchallenge.net`


**Figure 8.** Control-Alt-Hack tabletop game
Source: `http://www.controlalthack.com/`

Another example of a cybersecurity game (a tabletop card game this time) is Control-Alt-Hack™ (Figure 8). This game is dedicated to 14+ year olds, and can be played by 3–6 players. During approximately one hour players can improve their network skills and knowledge by identify Internet threats and make good or bad decisions in the cybersecurity area. Carefully selected questions and specific roles help educate social engineering and management skills. Control-Alt-Hack is an

example of a typical security game with implementation of the Nash equilibrium theory.

### *4.1. Examples of simple educational cybersecurity games*

*Are you cybersafe?* is a Polish simple board game for testing the player's cybersecurity knowledge. The game layout and the question formula make this solution a perfect choice for school kids and for those who are at the beginning of their „cyber life").

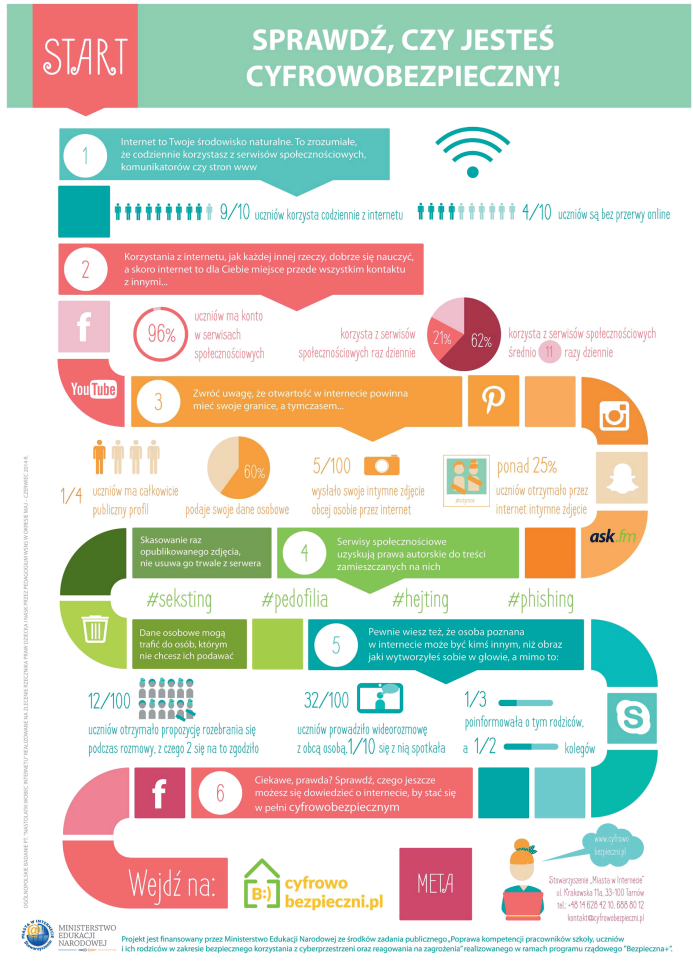


**Figure 9.** Board game *Are you cybersafe?*

This proposal has not implemented an advanced game theory or decision making algorithms but in this case it is not necessary. The simple game is a rapid entrance to more complex issues and exercises conducted by a professional teacher.

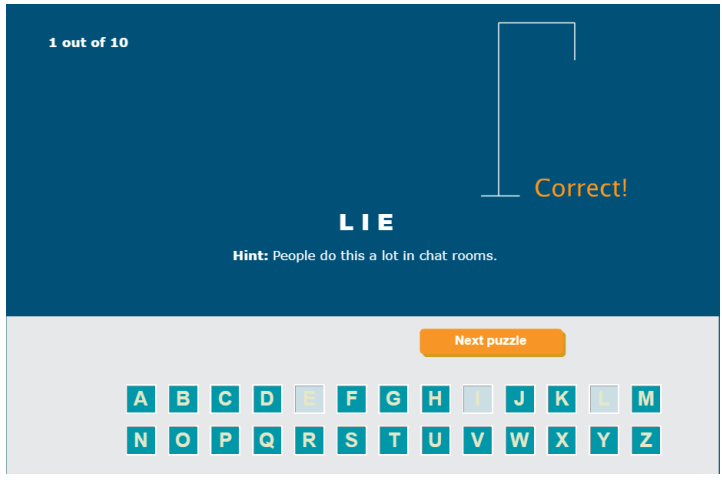


**Figure 10.** Internet Safety Hangman online game
Source: `https://www.quia.com/hm/40647.html`

## *4.2. Hangman and Webonauts*

*Internet Safety Hangman* is an online game where kids can learn words or sentences related to the safety rules. A simple method implementing a classic game can be extended and used in more sophisticated applications [11].

The Webonauts Internet Academy (Figure 11) is an online game witch allows kids to learn all about the web safety and digital citizenship rules. Taking on the role of 'webonauts', children have to complete a series of missions in order to graduate from the Webonauts Internet Academy. The lessons follow the motto – Observe, Respect, and Contribute.

The game teaches children how to keep passwords secure or how to build web profiles.

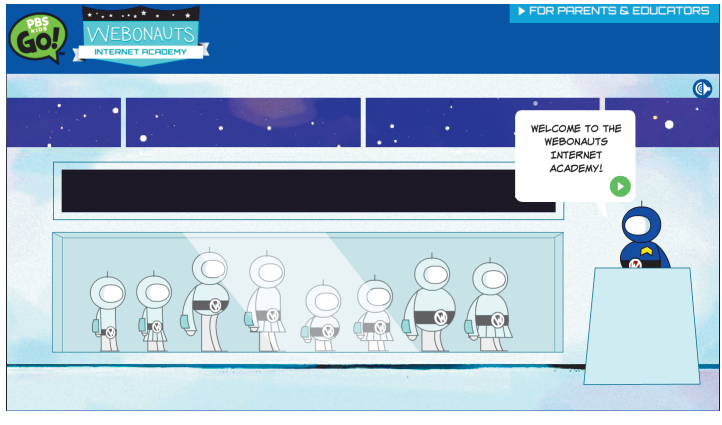


**Figure 11.** Webonauts Internet Academy game
Source: `http://pbskids.org/webonauts/`

## 5. Conclusions

The importance of cybersecurity education is steadily growing. Almost all of the teaching approaches used in practice are based on traditional methods: speech, text + photo presentations, simple project methods. Decision Support Methods in teaching Cybersecurity can:

- improve involvement;
- give fast feedback and interaction between education participants (players);
- provide more realistic conditions and cases than traditional education.

Games that teach decision-making and their consequences contribute to improving the cybersecurity.

Why games? Games can be fun which makes people involved and can give permission to explore ideas and ask questions. This type of learner involvement is intended to have an entertainment value. Practically, there are no security games dedicated to the Polish user on the Polish market. Security objectives and this way of teaching the rules of safety can be also achieved by playing traditional games. Physical games may appeal to people who do not enjoy computer games and generally do not require an extensive setup or have resource dependencies. The potential of educational security games is huge.

### *References*

[1] EU Cybersecurity Dashboard *A Path to a Secure European Cyberspace* [online] http://cybersecurity.bsa.org/assets/PDFs/study_eucybersecurity_en.pdf

[2] Taylor C, Krings A and Alves-Foss J *Risk Analysis and Probabilistic Survivability Assessment (RAPSA): An Assessment Approach for Power Substation Hardening* [online] https://www.researchgate.net/profile/Jim_Alves-Foss/publication/228861020_Risk_analysis_and_probabilistic_survivability_assessment_RAPSA_An_assessment_approach_for_power_substation_hardening/links/0046352127e8cc3e24000000.pdf, Computer Science Department University of Idaho

[3] Sommestad T, Ekstedt M and Johnson P 2009 *System Sciences, HICSS '09*

[4] El Fray I A 2012 *Lecture Notes in Computer Science* **7564**

[5] Delaney D G, Welch V and Starzynski C A 2015 *Annual Report and Strategic Plan (2015–2020)* [online] http://hdl.handle.net/2022/20412, Center for Applied Cybersecurity Research

[6] Roberson E P 2015 *Adequate Cybersecurity: Flexibility and Balance for a Proposed Standard of Care and Liability for Government Contractors*, 25 Fed. Cir. B. J. 641 (2015–2016)

[7] Jajodia S, Shakarian P, Subrahmanian VS, Swarup V and Wang C (Eds.) 2015 *Cyber Warfare: Building the Scientific Foundation*, Springer, USA

[8] Kiekintveld Ch, Lisy V and Pibil P *Game-theoretic Foundations for the Strategic Use of Honeypots in Network Security* [online] http://www.cs.utep.edu/kiekintveld/papers/2014/klp_game_theoretic_foundations.pdf

[9] William A 2008 *International encyclopedia of the social sciences* [online] http://www.columbia.edu/~rs328/NashEquilibrium.pdf

[10] Amory A, Naicker K, Jacky V and Adams C 1999 *British Journal of Educational Technology* **30** (4) 311

[11] Battigalli P and Dufwenberg M 2005 *Dynamic Psychological Games*, UCLA Department of Economics