Cross Impact Security Analysis using the HACKING Game

Arthur H. Hendela
New Jersey Institute of Technology
art.hendela@hendela.com

Murray Turoff
New Jersey Institute of Technology
murray.turoff@gmail.com

Starr Roxanne Hiltz
New Jersey Institute of Technology
roxanne.hiltz@gmail.com

ABSTRACT

Security of network assets is a high priority with little traditional return on investment. Increasingly, cyber attacks are being used by both terrorist and unfriendly government organizations. The HACKING Game, a Cross Impact Analysis planning tool, can be used to plan security resource allocation in computer networks. Cross Impact Analysis provides a mathematical basis to determine the interrelationships of one event with a set of other events. Output from the HACKING Game's Cross Impact Analysis model can be used to help justify security expenditures, with an added benefit of being a training tool for employees learning to protect networks. This paper presents details of the Hacking Game's design and its capabilities. Cross impact modeling can be used to develop games for any situation characterized by a set of offense and defense events to produce an individual or collaborative model for such things as natural and man-made disasters.

Keywords

Gaming, planning tools, Cross Impact Analysis, modeling

INTRODUCTION

Consider these reports from among many that can be found about cyber attacks, based on a PBS interview with Richard Clark, former White House adviser on cyberspace security, and a BBC story. They show that both terrorists and "unfriendly" governments are engaging in cyber attacks, and that both governmental and non-governmental organizations are their targets. They demonstrate that any organization concerned with preparing for "man made" disasters needs to be concerned with the security of their computer resources. Clark said, on March 18, 2003:

> "What we found on Al Qaeda computers were two things. One, the kind of simple hacking tools that are available to anyone who goes out on the Internet looking for them, tools such as LOphtCrack that allows you to get into almost anyone's password if they've used a simple eight-digit password. That kind of tool frightens most people when they learn that if they're using only an eight-digit password, hackers can easily obtain their data. But we also found indications that members of Al Qaeda were from outside the United States doing reconnaissance in the United States on our critical infrastructure. Where were the railroad crossings? Where were the big natural gas depositories? Where were the bridges over rivers that also carried the fiber for the backbone of the Internet?" (http://www.pbs.org/wgbh/pages/frontline/shows/cyberwar/vulnerable/alqaeda.html)

The BBC reported on Thursday, July 9, 2009:

> South Korea is experiencing a third wave of suspected cyber-attacks - coordinated attempts to paralyze a number of major websites. One of the country's biggest banks, a leading national newspaper and the South Korean spy agency appear to have been targeted. Some reports suggest the attacks might be the work of North Korea. (http://news.bbc.co.uk/2/hi/asia-pacific/8142282.stm)

Budget conscious organizations need a cost-effective planning method in order to protect their computer

Reviewing Statement: This paper has been fully double blind peer reviewed.

networks and the intellectual property that resides there. Without traditional return on investment to help justify security expenditures, an approach must be found that can help allocate the limited resources in a way that maximizes the system's protection, while providing the greatest probability of protection. The HACKING Game uses a mathematical model based on the Fermi-Dirac probability distribution that can help estimate the probability of success in defending networks against harmful attacks. The HACKING Game uses a cross impact model (Turoff 1972a; Dalkey 1975) which allows approximation methods to examine the interaction and likely occurrence of a set of future events. The model utilizes subjective probabilities of causality of the event set as developed by one or more subject matter experts in the domain to which it is applied. Once the judgments of at least one expert or the collective judgments of a group of experts (Linstone 2002) are determined, one may construct a structural model (Lendaris 1980) that can be used to drive the game calculation. When the experts each develop a model with which they are satisfied, their group estimations can be pooled into a collective model using the linearized C factors which show the influence of one event on another as developed in the Turoff model (Turoff 1972a).

A complete classical probability transitions model between all future states of ten events occurring or not occurring as described in (Turoff 1972a) is given by the equation $\sum_{j=1}^{N} j!\binom{N}{j} \cong eN!$ while $N \to \infty$. This equates to approximately 10 million subjective estimations. The cross impact estimation only needs n^2 estimates for n events. For the 10 event model the number of supplied estimates is reduced to only 100. This approximation approach is similar to other matrix estimation models such as using subjective measures of association. With subjective measures (Karni 2009) of associations, the relationship between items is estimated by summing all possible combinations of 2, 3, 4, … n-1 items at a time. Cross impact analysis is specific to using probabilities with the boundary conditions for never occurring, occurring half the time, and always occurring set to 0.0, 0.5, and 1.0, respectively. The output of the model is a scale of cross impact factors that relate the relative impact relationship between any two events on an interval scale. Additionally, a composite linear measure is created that estimates the impact of events not explicitly included in the model.

The remainder of this paper first describes what type of game the HACKING game is, and then describes the technical details of the cross impact model that serves as one of its foundations. Covered next are the design of the program and how the game is actually played. We conclude with a discussion of some potential uses of the game in emergency planning and preparation for cyber attacks, as well as other possible applications.

TYPES OF GAMES

Von Neumann and Morgenstern introduced the idea of the Zero Sum game during the 1940's, where the gain by one player must be offset by a corresponding loss by another player (Von Neumann 1953). From this work, games are classified in two broad categories, cooperative games and non-cooperative games. Cooperative games have many players that may or may not collude with one another during the course of the game. For example, a game developed for businesses cooperating in a joint venture showcases the cooperation of two corporations for mutual gain. The size of the respective companies influences the cooperation during the joint venture. When two companies are the same size, joint ventures are an optimal strategy (Aloysius 2002). Non-cooperative games are those where the participants are solely competitive and do not share information (Garcia 2003). One such example of a non-cooperative game pits managers against one another, each with limited resources. As resources become scarcer, the malevolence of the players towards one another increases (Wayne 1992).

The HACKING Game combines aspects of zero sum and cooperative/non-cooperative games. Planners for both the offense and defense teams discuss the strategies before producing success probabilities. Strategies known by one side are kept from being known by the opposing side. Although strictly not a zero sum game, players pitted against one another should reach a point where neither can improve their probability of succeeding against one another. This is because the probability of both sides succeeding must add to one. This optimum result is a type of Nash equilibrium where the product of the probabilities reaches a maximum value (Nash 1951). It is also very possible that the players would reach a local optimum where it is difficult for either side to improve the outcome probabilities with any incremental changes to their defense or attack postures.

THE HACKING GAME CROSS IMPACT MODEL

The purpose of cross impact modeling is to examine fairly unique events in a given future time frame that do not have a known frequency of occurrence to determine a true probabilistic value. Examples where this type of modeling might be used are in the launch of a new product to understand the potential interaction occurring in the marketplace. This section reviews the mathematical foundations of the model we are using. The cross impact theory we are using (Turoff 1972a) uses a Fermi-Dirac probability distribution (Figure 1) from quantum physics that describes electron excitation states events as having an actual value of one or zero but a probability of the transition expressed by this continuous distribution. In our computer model we constrain the probability estimates to between 0.01 and 0.99 to be in a reasonable range for humans and to avoid dealing with zeros and infinities in the calculations. Taking the shape of a logistic sigmoid function (Figure 1), we can make the simplifying assumption that the interaction between elements varies asymptotically towards 0 when there is no correlation between two events impacting the likelihood of occurrence and asymptotically towards 1 when there is an almost certainty that the two events strongly impact the likelihood of each other's occurrence. In order to transfer this distribution into a gaming structure of N events, we define three event types.

1. The inclusion or incorporation of a given defense event option in the system.
2. The inclusion or incorporation of a given offense event option in the system.
3. The inclusion of one or more event options that represents the success or failure of an attack. In each case the sum of the success and failure probability of each event = 1. That is Σ P(i) = 1.0 for i = 1 to N and the probability of failure, Σ(1- P(i)) = 1.0 for i = 1 to N.

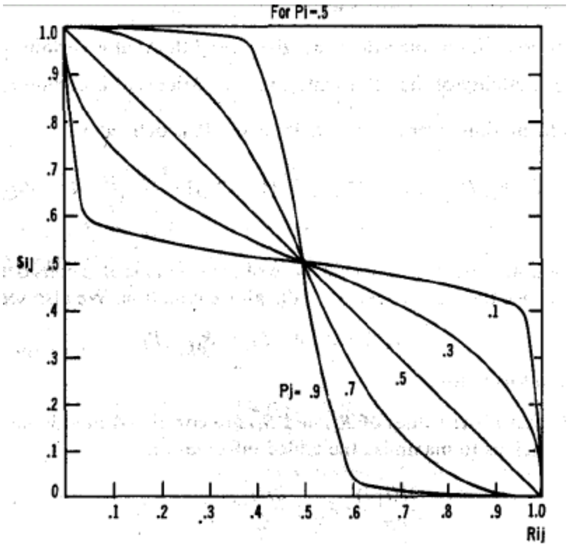

Figure 1. Example Fermi-Dirac Distribution of cross impact factors S(i,j) versus R(i,j) for P(i) = 0.5 (Turoff 1972a).

We set all the initial probabilities of occurrence, P(i), to 0.5. The inflection point in the middle of the X scale represents where an event is no more likely to occur than any other. The following probability notation corresponds to the 1972 paper by Turoff:

P(i) = the probability of the i-th event.

R(i,j) = the probability of the i-th event given the j-th event is certain to occur.

S(i,j) = The probability of the i-th event given the j-th event is certain to not occur.

C(i,j) = The influence of the occurrence of the j-th event upon the i-th event.

Gamma(i) = The influence on the occurrence of the i-th event by the unspecified events.

P(i) is calculated from the other variables by the equation:

P(i) = 1/(1+e**(-Gamma(i)-Σ(C(i,j)*P(j)))) for all j <> i (Figure 2).

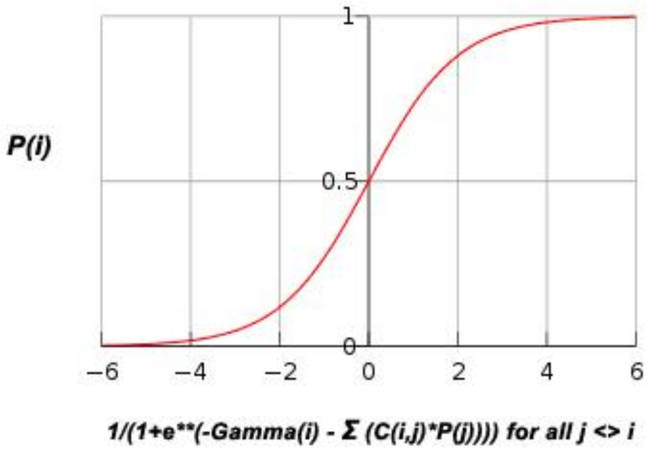

Figure 2. Example plot of P(i) versus the function of gamma, C(I,j) and P(j) for all j not equal to i

In this solution, the Gamma(i) factors are calculated by normalizing the P(i) equation once the C(i,j) influence factors are known. C(i,j) is calculated given the probability inputs P and S, or P and R (Turoff 1972a). Exact details of the calculaton of C(I,j) and Gamma(i) may be found in Turoff's "An alternative approach to Cross Impact Analysis" on pages 350-358. The actual calculations in the software run approximately 3500 lines in Visual Basic.

P(i) asymptotically approaches zero as the exponent function approaches minus infinity and tends towards one as the exponent function tends towards plus infinity. The exponent function value is zero when the interaction between events is considered neutral at P(i) equals 0.5.

This model uses a subjective estimate of the probabilities, which are non-linear in nature, to compute the cross impact factors (C(i,j)) which are a linear interval scale of the amount of impact the j-th event has on the i-th event in the range of plus to minus infinity. A positive C(i,j) value indicates that a positive influence exists from the j-th event on the i-th event while a negative value indicates the opposite impact. This linear influence factor is why the C(i,j) values can be used to cluster the events into scenarios (Banuls 2007) for a different type of analysis. A large event set can be reduced to a set of more independent mini scenarios therefore reducing the overall complexity which human planners have to overcome.

Table 1 describes the questions that are asked to create the subjective estimates of the conditional/causal probabilities given that a chosen event has an impact on another chosen event. The questions also help to determine if an event is included in the model at all. These estimates are referred to as P(i,j) where the j-th item (column) has an impact on the i-th item (row).

In the initial version of this game we will use one result variable, Q, defined as the resulting measure of success for the overall model. In order to build a beginning learning model, we will use only one success measure, that is, Q=1. The success probability, P(success) for one player is equal to 1-P(success) for the other player. It is possible that future versions will have alternative measures of success or failure. For example, a success may not only be that an event has occurred, but how long an event outcome, such as a denial of service attack, lasts. Note that the Q probabilities do not have any impact on the P(i)'s for either the inclusion of particular defense or offense items as the variables are considered consequence variables.

The assumptions in Table 1 treat the success/failure events as end points known as sinks in a transition process where they do not influence the strategic events for defense or offense. This significantly reduces the number of subjective estimates needed to create the model. Once a model has been designed, a defense and offense team takes the budget they have been given and uses it on the events they can afford to execute. They do this by changing the probability from its default value of 0.5, representing no influence, to something closer to a value of one or zero. The amount of change from 0.5 depends on their intended investment for each event. When both teams have completed their changes to the probabilities, the model is run and the probabilities of success or failure are calculated and shared by both teams. Players can then do a new round to try to improve their outcome. They will also be told which attack or defense items are being used, but not the investment made in

Option Types I row impacted by J column	Defensive Event Options	Offensive Event Options	Results Event Options
Defense N Event Options P(i) for i = 1 to N	Estimate the probability that the i-th defense option is part of the system if the j-th defense item is definitely included. R(i,j) notation.	Estimate the probability that the i-th defense option will be included in the system if the j-th offense item is definitely included. R(i,j) notation.	No change in any P(i) for any of the modification of a success or failure event option.
Offensive M Event Options P(i) for i = 1 to M	Estimate the probability that the i-th offense option is included if the j-th defensive items is definitely included. R(i,j) notation.	Estimate the probability that the i-th offensive option is part of the system if the j-th offensive item is definitely included. R(i,j) notation.	Same as above.
Results Q Success Options P(i) for i=1 to Q P(success)= 1- P(failure)	Estimate the probability of any attack succeeding if this defensive option is definitely part of the system S(i,j) for i=1 to N, and j=1 to Q. S(i,j) notation.	Estimate the probability of any attack failing if this offensive option is part of the system S(i,j) for i=1 to M and j=1 to Q. S(i,j) notation.	The Gamma(i) for each result P(i) or other P(i)'s indicates the potential impact of unspecified options. This serves as a measure of the incompleteness of the model.

Table 1. Description of questions to discern subjective estimates.

each. In principle the Nash equilibrium is reached when both sides return the value of the success variables to 0.5. They may also reach a situation where neither is able to improve their outcomes as measured by the respective probabilities of success.

HACKING GAME PROGRAM DESIGN

The HACKING Game is a prototype system developed as part of a corporate initiative and PhD research project. Its purpose is to help security planners develop probabilistic estimates of computer network attack and defense under budget constraint. As an online game, the participants do not have to meet face-to-face in order to provide input to the planning process. The HACKING Game is flexible as there is no pre-determined scenario. Starting points in the form of event libraries are provided to help the planner choose events that commonly occur. They are then asked for estimates of the interactions among the chosen events.

The categorization of the hardware, software, and events for attack and defense are developed from a detailed literature review. Each of the hardware, software, and attack/defense events is assigned a relative cost to consume limited budgets and assess relative loss. Each offense/defense event is given an initial default probability of 0.50 as this is the zero point where any event has an equal probability to occur or not to occur. Leaving these probabilities as defaults yields no information in terms of determining aspects of the attack scenario. Budgets are consumed as a function of event price and probability chosen.

The game contains a set of starting points that contain various aspects of the network topology and the type of attacks and defenses that can be used against the network. The starting points are contained in two types of data catalogs. Master catalogs are standard across all games. Game catalogs are copies of data from Master catalogs with modifications for the individual game. The catalogs hold data regarding the objects comprising the network and the events that interact on that network. For example, the component catalog contains entries such as types of servers, PCs, routers, hubs, and switches. The event catalog contains offense and defense events that can take place to attack or defend the components of the network. Example offenses are Altering Log Files, IP Address spoofing, and kernel level root kits. Example defenses are the application of anti-spoof filters, closing unused IP ports, and disabling the ActiveX Auto run setting in the browser. Not all defense events are appropriate to thwart a particular offense event. The Offense/Defense interaction library contains data on appropriate defenses for a particular offense. For example, to thwart the altering of log files, you may encrypt the logs or limit access privileges. To prevent IP Address Spoofing, you may apply anti-spoof filters at the network gateway. To defend against kernel level root kits, you may install a file scanner to monitor activity that may alter key files (Skoudis 2002).

Categories and the list of hardware and software components are currently being developed via a detailed literature review. The current breakdown of hardware component categories is shown in Table 2. The component category library is used as a reference table and contains three pieces of information. The three pieces are: 1) the name of the component category, 2) the description of the item, and 3) a URL where more information can be found.

Name	Description	More information URL
File Server	A computer on a network intended to provide shared storage of files and programs.	http://en.wikipedia.org/wiki/File_server
Network Hubs	A hardware device for connecting Ethernet equipment together, making it act as a single network segment.	http://en.wikipedia.org/wiki/Network_hub
Ethernet Switch	A computer networking device that connects network segments.	http://en.wikipedia.org/wiki/Network_switch
Desktop PC	An independent Personal Computer.	http://tinyurl.com/yz8w577
Monitor	A computer display device.	http://en.wikipedia.org/wiki/Monitor
Notebook PC	A small mobile computer.	http://www.pcworld.com/ic/laptops
Router	A device whose software and hardware are usually tailored to the tasks of routing network traffic to a specific PC, printer or other IP device.	http://en.wikipedia.org/wiki/Router
Modem	A device to transmit data over a telephone or cable line.	http://tinyurl.com/ylyhxbr

Table 2. Component Type Categories

Once the category types are established for the physical network, specific hardware components are entered into the category table. Each component is given six pieces of information as shown in Table 3. The costs of the components are used against the allotted budgets given to the players at the start of the game. The components are not used in the actual data model, but only guide the types of attacks that are appropriate for defending.

Item	Description	Example
Name	Identifying name for the component.	Server – 80 GB
Description	Technical specification for the component.	1.86 Intel Dual-Core Xeon Processor, 1GB RAM, 80GB Hard Drive, CD,

		10/100/1000 Ethernet, 4U
More information link	URL to a deeper explanation of what the component is.	http://en.wikipedia.org/wiki/File_server
Component Type	Category type of the component as shown in Table 1.	File Server
Cost	Current or relative price of the component in generic units.	713
Photo File Name	Photograph of the item.	Server80Gb.jpg

Table 3. Component Table Example

Event types are the high level categories under which security attacks and defenses fall. For each named event type there are entries in the detailed event table for both attacks and defenses. The Event Type table provides a reference list for these category types. The table contains three main pieces of information: Name, Description/Example, and a URL with more information. The event types are listed in Table 4.

Name	Description/Example	More information URL
Reconnaissance	Investigate a target using publically available information via web reconnaissance or social networking.	**http://tinyurl.com/648mmw**
Scanning	The process of looking for security vulnerabilities via password attacks or war dialing.	**http://tinyurl.com/yfnu6le**
Application Attacks	Attacks on programs viewable over the internet via session tracking attacks and forcing bad SQL.	**http://tinyurl.com/dbobvb**
Network Attacks	Maliciously compromising the security of a computer network via IP address spoofing or session hijacking.	**http://tinyurl.com/yzflyca**
NETCAT attacks	A utility used to write directly to network connections such as an open port.	en.wikipedia.org/wiki/Netcat
Denial of Service	An attack which prevents legitimate users from accessing a system via process killing or system overloading.	**http://tinyurl.com/jzn67**
Stop Services	A denial of service attack that does not require a local user account to implement such as spoofing.	**http://tinyurl.com/e8f4a**
Exhaust Services	An attack outside a network to tie up specific resources such as with a SYN Flood attack.	**http://tinyurl.com/2p75nz**
Covering tracks	An attacker remains hidden and in control of a system for extended periods of time such as altering log files.	www.nsisecure.com/logmon.htm
Covert Channels	A communication method that hides data from detection as it moves through a system such as with Covert TCP.	**http://tinyurl.com/ygxtc4g**
Rootkits	A program used to gain high authority access to a system such as kernel level and traditional rootkits.	en.wikipedia.org/wiki/Rootkits
Exhaust Resources	A technique to stop or overload resources from inside the network such as extensive logging and logic bombs.	**http://tinyurl.com/ylre2ve**
Back Doors	An attack where a “good” program causes destruction such as the AntiSpyWare 2009 program.	**http://tinyurl.com/bbu3y**

Table 4. Event type categories

Once the event types are established, specific network attacks and defenses are entered into the event table. Each event is given seven pieces of information as shown in Table 5. The costs to perform the event are used against the allotted budgets given to the players at the start of the game.

Item	Description	Example
Event Name	Identifying name for the event.	Account Harvesting
Description	A brief definition of the event.	The attacking technique or activity involved with obtaining legitimate user IDs and passwords to gain access to target systems for illegal or malicious purposes
More information link	URL to a deeper explanation of what the event is.	**http://tinyurl.com/yzl6af7**
Event Type	Event type of the event as shown in Table 4.	Scanning
Cost	Relative cost of the event.	100
Event Role	Whether the event is an offense, a defense, or both.	Offense
Event Importance Factor	Relative expert opinion as to the likelihood of this attack or defense.	On a scale of 1 to 100 where 1 represents low importance and 100 represents high importance.

Table 5. Event table example

During play of the game, expert judgment plays an important role in the determination of a particular event's importance. Those learning to create security plans can give their opinions as to the relative importance of offense and defense events before and after playing the game. We hypothesize that after they have played the game for a while, their rankings will become closer to those expressed by experts.

PLAYING THE HACKING GAME

Games begin with an Administrator defining a game record in the database. This data consists of a Game Name and description, the username of the person with administrative responsibility for the running of the game, known as the Overall Game Director, OGD, the budget for the team or individual that will play the game, and whether the game is being played by a single person or by a team of people. For the current prototype, games may only be played in single user mode. Game players are divided into two teams, offense and defense. The offense team chooses events that are of an attack nature. The defense team chooses events to thwart the attacks. In single user mode, the player participates as both teams. In single user mode the player can learn the effects first hand on how changes in offense and defense tactics affect the overall outcome. Once past this initial prototype stage, when a team mode is developed, the two separate teams will no longer have the ability to see the effects during play. Each side will work blindly and then only see the outcome when the final result is revealed.

Each player is given a budget for network configuration and to execute the protection and attack events. This budget is set prior to the start of the game by the OGD. As a network event is chosen, a network component added, and a probability entered, the budget is partially consumed. Protection or destruction of the network is limited by the available funding.

Input to the Cross Impact model is keyed into a series of forms and then reviewed. We assume an initial probability, P(i), of using any offense or defense as 0.50, entered as 50, to show the event is equally likely to occur or not occur. The probabilities are adjusted in the range of 1 to 99. Once the input is finalized, the Cross Impact Model results are calculated and shown online as reports. The model can be revised and rerun until a player is satisfied with the results.

Each player is assigned a username and a role. The role limits access to various aspects of the game system. Administrators are permitted to work with any and all aspects of the data and access all system screens. An Overall Game Director, OGD, for an individual game is permitted to work with all screens and data for an individually assigned game. A player may only access the data input features used by the probability model.

Programming was done using Visual Studio 2005 with Visual Basic. The runtime environment was ASP.NET 2.0 with an SQL Server 2000 database. Report functions are implemented using Crystal Reports 10.2.3600.0.

FUTURE WORK AND GENERALIZATIONS

The HACKING Game needs evaluation of its strengths and weaknesses as a planning and learning tool. The current plan is to let gamers play and then determine the quality of the plan compared to traditional security checklist methods. Additionally, the HACKING Game is to be evaluated for effectiveness in aiding those learning to prepare security plans. It is also possible that the factors that are used in the play of the game will have a second use in the determination of items used to create mini scenarios. These items should be treated in combination because they are tightly coupled through relationship factors. The coupling could then be applied to reduce the number of game options for actual organizational security planning (Banuls 2007).

Longer term it is envisioned that the HACKING Game can be used to supplement planning activities in a host of environments, not just network security. For example, the HACKING Game's catalogs could be modified to create other types of plans. The attack – defense structure of opposing options and expert subjective judgments could be used to ultimately build threat models for other types of situations such as terrorist threats against specific types of facilities such as chemical or nuclear plants. For business planning, the tool could be used to assess the viability of launching a new product against a competitor.

The building of the resulting model is only as good as the expertise of those making the estimates. However, this approach offers an excellent way of allowing multiple experts to collectively develop the structure of the model. This approach to building a model for gaming and training using the relative importance of defense options is quite general and can be applied to natural and man-made disasters as well. In natural disasters the offense is "mother nature" and stressing the plans of the defense becomes the objective.

The problem of creating a good event step is an important pre-effort and not easy to accomplish collectively. There is related work in the "dynamic Delphi" effort (White 2009) which allows an easy process to collectively rate the importance of event candidates for use in the model by a large number of knowledgeable individuals. Associated with the system is a database to allow a group to prepare a set of events for use in alternative scenarios and to create detailed plans (Yao 2009). Since both systems are asynchronous and online they can lead to events that might be useful to model for training purposes for many types of response roles. If the individuals playing the games are able to learn the influence relationships between the events, then the game would be a very useful learning tool. Another related tool is recent work to be able to take the linear scale factors and to cluster the atomic events into micro scenarios which could formally reduce the complexity of the situation (Banuls and Turoff, 2010). This method would also allow the compaction of the events in the cross impact analysis into a less complex model.

The integration of these tools into a single planning system would allow a continuous planning process by large groups of individuals that represent all the different organizations involved in planning and responding to a crisis or disaster. Having such a system online would allow everyone to spend a small amount of time each week to contribute their knowledge to an evolving process that can handle the discovery of problems and mistakes that have evolved from prior experience. Such a system is currently missing from the toolset of local, regional, state, and national planning efforts. Current systems do not really integrate over the actual team that is needed in most disaster situations or handle any unexpected problems. Our stated approach to a planning system was proposed in 1971 (Turoff 1971). It was shown at that time to be a highly efficient and cost effective approach to the use of teams of individuals compared to bringing the teams together for face-to-face meetings (Turoff 1972).

CONCLUSION

Today's security planners are faced with the daunting task of finding useful, yet cost effective methods to stretch security budgets while providing adequate protection of organizational networks and intellectual property. The HACKING Game has the potential to provide a planning tool that is a cost effective supplement to traditional planning methods. Additionally, it is hoped that the HACKING Game can aid those new to the security area to shorten the time to learn how best to protect a network.

REFERENCES

1. Aloysius, J. A. (2002). "Research Joint Ventures: A Cooperative Game for Competitors." European Journal of Operational Research **136**(3): 591-602.
2. Banuls, V. a. M. Turoff. (2007). Scenario Construction via Cross Impact. The Network Nation and Beyond. New Jersey Institute of Technology. **1:** 22.

3. Dalkey, N. (1975). An Elementary Cross-impact Model. The Delphi Method: Techniques and Applications. H. A. a. M. T. Linstone.
4. Garcia, D. D., David Ganet, Peter Henderson (2003). "Everything you Always Wanted to Know about Game Theory (But were Afraid to Ask)." SIGCSE 2003 **35**(1): 96-97.
5. Karni, E. (2009). Subjective Probabilities on a State Space. Seminar 208, Microeconomic Theory, Johns Hopkins**:** 40.
6. Lendaris, G. G. (1980). "Structural Modeling - A Tutorial Guide." IEEE Transactions on Systems, Man, and Cybernetics **SMC-10**(12): 34.
7. Linstone, H. A. a. M. T. (2002). The Delphi Method: Techniques and Applications.
8. Nash, J. F. (1951). "Non-Cooperative Games." Annals of Mathematics Journal **54**(1951): 286-295.
9. Skoudis, E. (2002). Counter hack. Upper Saddle River, NJ, Prentice Hall.
10. Turoff, M. (1971). "Delphi and its Potential Impact on Information Systems." AFIPS Conference Proceedings **39**.
11. Turoff, M. (1972). "Party-Line and Discussion: Computerized Conferencing Systems." Proceedings of the First International Conference on Computers and Communications **October, IEEE**.
12. Turoff, M. (1972a). "An alternative approach to Cross Impact Analysis." Technology Forecasting and Social Change **3**: 338-368, reprinted in "the Delphi Method".
13. Von Neumann, J. a. O. M. (1953). Theory of Games and Economic Behavior. Princeton, Princeton University Press.
14. Wayne, S. J. a. D. R. (1992). "Extending Game Theoretic Propositions About Slack and Scarcity in Managerial Decision Making." Journal of Human Relations **45**(5): 525-536.
15. White, C., Plotnick, L., Kushma, J., Hiltz, S.R., and Turoff, M. (2009). An Online Social Network for Emergency Management. ISCRAM 2009, Gothenberg, Sweden.
16. Yao, X., Turoff, M., and Chumer, M. J. (2009). Designing Collario for continuous reviewing and practicing of emergency plans to ensure complex system safety. ISCRAM 2009, Gothenberg, Sweden.