Association for Information Systems
AIS Electronic Library (AISeL)

SAIS 2008 Proceedings

Southern (SAIS)

3-1-2008

Countering Cyber Terrorism: Investment Models Under Decision and Game Theoretic Frameworks

Tridib Bandyopadhyay
Kennesaw state university, tbandyop@kennesaw.edu

Reda Sebalia
Kennesaw state university, rsebalia@students.kennesaw.edu

COUNTERING CYBER TERRORISM: INVESTMENT MODELS UNDER DECISION AND GAME THEORETIC FRAMEWORKS

Tridib Bandyopadhyay
Kennesaw state university
tbandyop@kennesaw.edu

Reda Sebalia
Kennesaw state university
rsebalia@students.kennesaw.edu

ABSTRACT

In this work we attempt to develop models that can suggest requisite levels of investment, and/or indicate the strategic nuances of such investments in the face of possible cyber terrorist attacks. Beginning with one naïve model each under the two broad conceptual frameworks of Decision Theoretic and Game Theoretic frameworks, we have incrementally introduced pertinent backgrounds, investment criteria and economic dynamics to achieve (what we call) adequate investment models for countering cyber terrorism related attacks. This initial work is geared towards a broad based understanding of the issues surrounding the threat of cyber terrorism, and an adequate investment propensity of the defender.

Keywords

Cyber Terrorism, Counter Terrorism, Investment, Cyber terrorist, Attack, Defense, Game, Decision

INTRODUCTION

Post 9/11 understanding of terrorism is significantly different from what it used to be before. The apparent inaccessibility of our resources, assets and lives separated by thousands of miles and large bodies of waters from known centers of terrorism has been proven wrong in a sorry yet reverberating manner. As such, the physical separations are also becoming increasingly inconsequential in view of the intensity of information resources and assets in our economy and basic lives in general, and the interconnected nature of these assets (given the pervasive nature of the Internet and the trend of web based services which essentially join these resources and assets) in particular. As a result, the threats of terrorism now equally emanate from cyber spaces as from physical modes and spaces. Although such dawning was evident even before we realized the 9/11 attack[1], the possibilities of cyber terrorism and the effects are more likely, and certainly more debilitating in nature now than ever.

Countering cyber terrorism is a daunting task which is immensely investment intensive. Such investments are not only required to create a preventive/detective pre-breach regime (intelligence, prevention and detection technologies, pursuance of cyber terrorists and required legal provisions), huge investments are also required to plan and provide for incident response and other mitigation and damage reduction/control measures. Although there are contradicting opinions about the real possibilities of worst case scenarios, our need to understand the economics of countering cyber terrorism is real, appropriate, and pending.

In this work we investigate models/frameworks to assess and understand investment dynamics of countering cyber terrorism. In particular, we investigate models under 1) Decision Theoretic Framework (where investment towards countering cyber terrorism is optimized given the probabilities of such acts and the magnitude of attendant losses), and 2) Game Theoretic Framework (where the investor is strategic and considers temporal, societal, behavioral and political environments along with economic considerations). This is a research in progress and we do not provide any conclusive evidence or conjecture about suitability of any particular model/s. Instead, our focus in this report is to highlight the intricacies and subtleties of the dynamics of investment in countering cyber terrorism.

In what follows, first we provide a brief comparison (of the approaches) between decision and game theoretic concepts. Second, we develop one adequate investment model each under the decision and game theoretic frameworks, and discuss our broad understandings from this effort. Lastly, we provide future directions of this research and our concluding thoughts.

[1] "The FBI believes cyber-terrorism, the use of cyber-tools to shut down, degrade, or deny critical national infrastructures, such as energy, transportation, communications, or government services, for the purpose of coercing or intimidating a government or civilian population, is clearly an emerging threat for which it must develop prevention, deterrence, and response capabilities." - Former FBI Director Lois Freeh, Statement before the United States Senate Committee on Appropriations, Armed Services, and Select Committee on Intelligence, May 10, 2001.

COMPARISON OF THE MODELING FRAMEWORKS

Decision and Game theoretic models have their own strengths and weaknesses. *Decision theory* could be viewed as a theory of one player game, against nature (chance happenings). The focus in decision theory is on rational preferences (risk integrated utility characterization, and the expected utility maximization paradigm), and formation and revision of beliefs (e.g. Baye's updates for prior and posterior probabilities). Decision theory is also used to understand how information may be acquired before an informed decision could be made[2].

G*ame theory*, on the other hand, explicitly identifies the strategic players in its modeling efforts. Concept of equilibrium is paramount in game theory in bolstering the fact that the strategies of the players lead to expected payoffs (whose maximization is the rational choice of the strategic players), and that any off-equilibrium strategy employed by a player must initiate a counter strategy for the other player such that at the end, neither of the players is interested to move from the equilibrium in the first place (Nash Equilibrium). The game settings and pay-off structures are tools to ensure and refine equilibrium/s that may ensue from the game modeled. Game theory allows modeling under complete and incomplete information availability (to players) as well as temporal staggering of the strategies, which make such modeling insightful.

MODELING INVESTMENT AGAINST CYBER TERRORISM UNDER DECISION THEORETIC FRAMEWORK

Naïve model in pre-breach regime

We begin with a naïve model which assumes that all information assets are lumped together in a single location, (a simplification), and that the investor ***D*** (defender) is interested to protect this asset (fixed value: ***L***) against a cyber terrorist ***T***. The pre-breach measures (firewall, IDS systems, Honey Pots, etc.) employed by the investor in the information network reduces the probability $p(c_p)$ of the success of a cyber terrorist, where c_p is the investment in such measures[3]. Assuming that the utility of the defender is linear in investment, the investor solves $\underset{c_p}{Max}\ \{c_p - p(c_p)L$ to arrive at the optimal investment to counter cyber terrorism $c_p * = p'^{-1}\left(\frac{-1}{L}\right)$. Thus ***D*** increases investment as the value of the information asset (at risk) increases (an intuitive result). Knowing the exact loss from the asset, the investor can calculate its optimal investment level.

Model incorporating pre-breach and mitigation regimes

However, Preventive measures could be augmented by incidence response and mitigation measures (evacuation plans and provisions, building flash capacity in hospitals and other facilities, back-up redundancies, etc.), which potentially reduce the real loss when an attack is actually realized. Essentially, given an attack, the loss of the value of asset is no longer fixed now; it is responsive to the investment in the mitigation measures. Assuming that the post investment loss is $l(c_m)$, where c_m is the investment in such measures[3], the investor now solves $\underset{c_p,\, c_m}{Max}\ \{c_p - c_m - p(c_p)l(c_m)$ to arrive at its simultaneous optimal investments in the preventive and mitigation regimes, given by the concurrent solutions for $c_p *$ and $c_m *$ from the equations: $c_p * = p'^{-1}\left(\frac{-1}{l(c_m^*)}\right)$ *and* $c_m * = l'^{-1}\left(\frac{-1}{p(c_p^*)}\right)$. Because such simultaneous solutions are not amenable to much insight without employing specific functional forms, a brief functional analysis of the investments is imperative here. We have analyzed with two different functional forms to test for the efficacy of the investments in the joint optimization, one of which yields symmetric investment in either of the regimes, while the other indicates an either/or investment scenario between the regimes. We have omitted the details here for paucity of space except a depiction of the investment and the reduced expected loss in the shaded rectangle in figure-1.

Model incorporating pre-breach and mitigation regimes with exogenous budget constraint

It is unlikely that ***D*** will have all the funding readily available for such counter terrorism endeavors. It is rather practicable to assume that ***D*** would be constrained under some budget considerations ***B***. Whether such budget is arrived utilizing an objective or subjective framework/estimation is beyond consideration here (this has been considered, in part, in the game theoretic model development section). For example, in figure-1, the budget can be interpreted as the *x* axis of the diagram, meaning $B = c_p^* + c_m^*$.

[2] http://levine.sscnet.ucla.edu/general/whatis.htm

[3] Standard assumption of decreasing marginal utility of investment applies in both preventive as well as mitigation measures.

Model incorporating multiplicative regimes with exogenous budget constraint and distributed targets

Without any loss in generality we may also assume that the information assets are now distributed in more than one different location, yet interconnected (signifying current trends in Internet based and web-faced applications) with some non-zero probability of cross propagation of breach between these assets. The problem is substantially involved now, assuming that the cyber terrorist can attack either or both of the locations, and given a success in one of the locations, may exploit the interconnection to reach the other location. While we identify this as an *adequate model* in the decision theoretic framework, a complete solution of this problem, although plausible, has not been investigated by us yet.

.

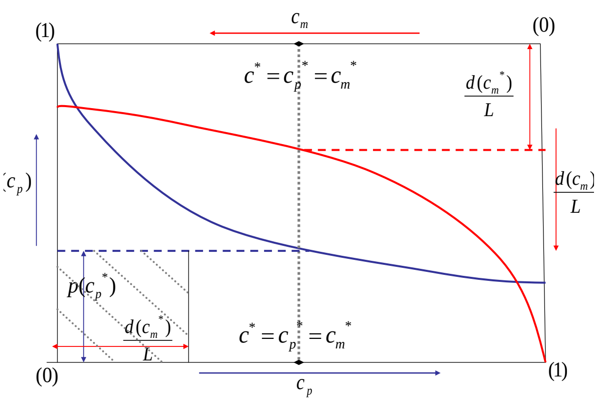
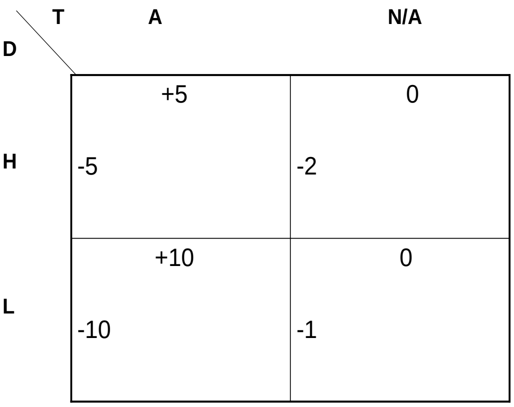


Figure-1



D \ T	A	N/A
H	+5 -5	0 -2
L	+10 -10	0 -1

Figure-2

MODELING INVESTMENT AGAINST CYBER TERRORISM UNDER GAME THEORETIC FRAMEWORK

Games that a cyber terrorist plays with the defender of the system

Our first model is depicted in strategic form (Figure-2). Player ***D*** is the investor (Defender) and Player ***T*** is the cyber terrorist (Attacker). The defender has options to decide between two levels of defense, *High (H)* or *Low (L)*, which is however not observable by the cyber terrorist. High-level defense is more costly to provide, but reduces the probability of success of the terrorist or the damage, (or both) and likewise reduces the terrorist's expected payoff. Low-level defense is inexpensive, but the chance that the terrorist will be successful is high or the damage is high (or both), which is reflected in the terrorist's increased payoff. The defender plays a solely defensive strategy (does not pursue the terrorist - a simplification). On the other hand, the cyber terrorist's choices are to *Attack (A)* or *not to Attack (NA)* the critical information assets of national interest.

Figure-2 gives possible payoffs that describe the above situation. ***D*** prefers to invest *High* if ***T*** chooses to attack, else could invest *Low*. However, regardless of whether the level of counter-terrorism investment is high or low, ***T*** has higher payoff for *Attack* than *No-attack*. Therefore, the strategy *Attack* strictly **dominates** the strategy *No-attack* for ***T***. Since ***D*** believes that ***T*** is rational and will strategize for higher payoff, she realizes that ***T*** will attack. Given this anticipation, she invests *High* in counter terrorism measures where her payoff is higher ($-5 > -10$, given an attack). In essence, the rationality of both ***T*** and ***D*** leads to the conclusion that ***D*** will implement strict counter terrorism controls and ***T*** will attack to breach such controls[4].

In practice however, the defender's investments could also include cyber forensic technologies and training personnel to achieve capability to pursue and track a scheming/perpetrating cyber terrorist. Such added costs of *pursuit* (*P*) capability do not reduce the losses of an actually realized attack, although intuition suggests that this action may be able to deter the cyber terrorists: we model this enhanced game separately (figure-3).

Note that the payoff structure has been modified to reflect the facts that:

- A terrorist identified and booked improves the image of the defender than otherwise (-5 > -15), however, if there is no attack from a cyber terrorist, then the added cost to achieve the capability to pursue remains uncompensated (-10 < -5)
- The expected payoff of the cyber terrorist is now much lower when the defender has invested in forensics (-100 < +10), signifying extremely high penalty in the eventuality that the cyber terrorist is caught and punished by the legal machinery.

Unlike the earlier case, this game now lacks a dominant strategy for either of the players as explained below (vide figure-3):

[4] Note that (by design) this game yields pure strategy equilibrium between the players ***D*** and ***T***.

- Assume that ***T*** decides to *Attack*. Under such conditions, investment in *pursuit* is better than otherwise (-5 > -15). The game thus begins at the NW quadrant.
- Knowing that facing an *attack* strategy ***D*** would rationally invest in pursuit capability, ***T*** now opts *not to attack* (0 > -100). The game moves to NE quadrant.
- However, if ***T*** opts not to attack then the defender has no reason to invest (0 > -10), and the game makes a transition to the SE quadrant.
- In absence of ***D***'s capability to pursuit, ***T*** is now better of *Attacking* (+10 > 0), and the game moves to SW quadrant. This by the first argument moves the game to NW quadrant again.

D \ T	A	N/A
P	-100 -5	0 -10
N/P	+10 -15	0 0

Figure-3

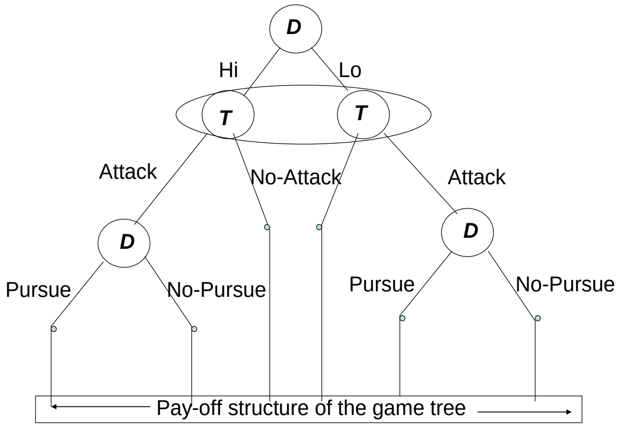


Figure-4

The cycle above continues indefinitely, and there is no pure strategy equilibrium. One way to break the impasse could be to consider that the players prepare them for the worst case scenarios, i.e. they could adopt a *Max-Min* strategy. For *attack* strategy of ***T***, the worst payoff for ***D*** is (-15), and for *no-attack* strategy of ***T***, the worst payoff for ***D*** is (-10). Thus the *Max-Min* strategy for ***D*** is to always invest in pursuit capabilities (-10 > -15). On the other hand, for *pursuit* strategy of ***D***, the worst payoff for ***T*** is (-100), and for *no-pursuit* strategy of ***D***, the worst payoff for ***T*** is (0). Thus the *Max-Min* strategy for ***T*** is *no-attack* (0 > -100). However, note that the *Max-Min* strategies of the players are not in Nash Equilibrium, if one of the players implements its *Max-Min* strategy, the other player will certainly deviate.

However, a mixed strategy Nash Equilibrium is plausible for this *finite* game: A *mixed strategy* of ***D*** in this game is to *Pursue* (invest in such capability) only with a certain probability[5] because randomizing is a cost effective approach in the context of pursuit. Although pursuit is not certain, a high probability of identification can effectively deter ***T***. On the other hand, mixed strategy of ***T*** refers to a randomized decision to attack a certain resource or a certain part of information network.

It is easy to see that ***T*** (***D***) would randomize between strategies of *attack* and *no attack* (*pursuit* and *no-pursuit*) in such a fashion that ensures equal payoffs, or in other words, when ***T*** (***D***) is *indifferent* between available strategies. However, we calculate the indifferences of ***T*** (***D***) from the mixed strategies of ***D*** (***T***):

- Suppose that ***D*** randomizes *pursue* with probability x, and *no pursue* with probability $(1-x)$, then the payoff-indifferent strategies of ***T*** occurs at the solution of $\left(x.-100+(1-x).10=0\right)$, or $x\approx 9.1\%$.
- Similarly, if ***T*** randomizes *attack* with a probability *y*, and *no attack* with a probability of $(1-y)$, then the payoff-indifferent strategies of ***D*** occurs at the solution of $\left(y.-5+(1-y).-10=y.-15+0\right)$, or $y=50\%$.

D invests to achieve capability to pursue 9.1% of attacks (or all attacks on 9.1% of the critical and protected resources), and the cyber terrorist flips a coin and randomly decides whether a target would be attacked or not. Most importantly, so long one player randomizes with this prescription, the other never deviates: and the mixed strategy Nash Equilibrium of the game is stable. The expected payoff to ***D*** and ***T*** are -7.5 and 0 respectively[6]. There are several outcomes and insights from this changed game structure:

[5] It is more practical to think in terms of a revolutionary game concept, where only a random portion of the networks / resources is made amenable for trace back and pursuit capabilities, while the others are not. Same applies for the choices of the cyber terrorist given myriad targets that may exist in a network connecting the critical infrastructure of the defender.

[6] $0.5.-5+0.5.-10=0.5.-15=-7.5 \quad and \quad 0.091.-100+0.909.10=0.091.0+0.909.0=0$

- The strategy of randomized pursuit (investment thereof) of ***D*** has successfully changed the earlier dominant strategy of *attack* by ***T***. Facing the possibility of being caught; ***T*** now randomizes between her choices of *attack* and *no-attack*.
- The game introduces the risk preference and risk aversion of the players in the game. A cyber terrorist is unlikely to settle for a confirmed payoff of *0* with a pure strategy of *no attack* and thus ***T*** prefers to randomize even with unchanged payoff of *0*. The game is also rational for ***D***, who is risk averse, and ends up with a net negative payoff of *-7.5*.

One major disadvantage of the above games (represented in strategic forms) is the fact that temporal considerations are not integrated. We conclude our discussion of the strategic interplay between ***D*** and ***T*** in an extensive imperfect-information game tree framework. Note that in the game, a scheming cyber terrorist does not really know whether the defender is highly or lowly invested in the counter terrorism measures and controls (figure-4). Thus his information set is coarse (depicted in the superimposed oval) emphasizing our insight that ***T*** may employ a randomizing strategy. Although provisions for building up pursuit capability may occur at an earlier time, the actions must follow a realized attack, and this temporal ordering is maintained in the game tree. We do not provide hard numbers for the pay-off structure because we do not carry out any further analysis. However, it is instructive to note that because of the imperfect information nature of the game here, a backward induction strategy is inappropriate and may not be employed.

The Government as the defender

Now consider the more specific (and likely) case: the defender is the (elected) federal government (***G***) of a country. Assume that ***G*** has a set of knowledgeable professionals who can objectively estimate the randomizing strategies of the terrorist, and the losses that could result. Utilizing a decision theoretic framework (section-1), or by the use of the games discussed earlier in this section, ***G*** may *objectively* strategize her levels of investment in counter terrorism measures against ***T***. However, representatives of the electorate (who may have oversight responsibilities and/or overriding decisional prerogatives) may require echoing the desires, beliefs and sentiments of the citizens (***C***) of the country. It is here that the set up of this cyber terrorist game takes an interesting turn when the defender is a sovereign government.

Research in social sciences suggests when outcomes of a disaster or attack on public life and property are vivid, gory, or evoke memory that is strong in terms of affect, human mind is prone to assign higher than actual probability for the realization of a catastrophic event[7]. For example, a terrorist attack leading to mindless bloodbath, loss of life and property (like that of 9/11) causes us to ascribe higher probability of such acts of terrorism - higher than what pure economic rationality could justify. Social researchers call this phenomenon '**probability neglect**'. The same affect can be expected to be in the background when we think about cyber terrorism - when cyber terrorists could hack into our interconnected information systems, and wreak havoc in basic life and livelihood of the citizens. Dooms day prognostics, media hype, science fiction, and ultra advocates vividly paint these possible events[8]. Such probability neglect, in mass scale, can have far reaching effects. For example, among others, this gives rise to a general need for higher protection to obviate such events. Such needs in turn, translate to demand for stricter regulation and/or higher government/corporate spending to control and mitigate such risks. Finally, through elected representatives, popular probability neglect could eventually cause higher than optimal investment/regulation in the area (prevention and mitigation) of cyber terrorism. This is beyond the economic rationality of ***G***: we will differentiate this by identifying the fact the ***G*** could *subjectively* strategize her levels of investment in counter terrorism measures, which is likely to be higher than that from the *objective* strategy of ***G***.

An attempt to model this game in strategic form is inherently fallacious because a player in background (***C***) must be somehow considered between ***G*** and ***T***, temporal settings are not concurrent, observability[9] issues are critical, and especially for a sophisticated analysis, macroeconomic issues are unavoidable:

- The level of objectively decided investment is to counter attack from ***T***, an *uncertain future event*.
- The subjectively decided investment takes care of
  - ***G***'s allegiance to the electorate (and indirectly their need to be protected from ***T***) and
  - ***G'***s desire to succeed in the next electoral process, a *certain future event with uncertain outcomes*.

[7] "… First, differences in probability will often affect behavior far less than they should or than conventional theory would predict. Second, private behavior, even when real dollars are involved, can display insensitivity to the issue of probability, especially when emotions are intensely engaged. Third, and most important, the demand for legal intervention can be greatly affected by probability neglect, so that government may end up engaging in extensive regulation precisely because intense emotional reactions are making people relatively insensitive to the (low) probability that the relevant dangers will ever come to fruition". ***Probability Neglect: Emotions, Worst Cases, and Law, Cass R. Sunstein, Chicago Law School Working Paper.***

[8] While these events could happen in reality, the chances of their happening, especially in a large scale, could be extremely rare.

[9] Observability and personal experiences are critical in creating impression about security and sense of protection: having seen TSA staff thorough checking every airline passenger, and having gone through the process themselves, airline passengers are more likely to be satisfied by the security level of the airports and their flights than otherwise.

- The counter measures (the extent of which could be decided subjectively or objectively) by ***G*** may or may not be observable to ***T*** or ***C***.
    - If ***C*** cannot observe counter measures, unfavorable '*less caring*' attitude of ***G*** may be inferred,
    - If ***C*** observes counter measures, and ***T*** attacks but fails to succeed, a favorable impression for ***G*** may be expected,
    - If ***C*** observes counter measures, and ***T*** attacks and succeeds to wreak havoc, not only a sense of helplessness, anger, wastage of effort and resource is likely, a very unfavorable impression of incompetence of ***G*** may ensue.
- A climate of protection against cyber terrorist attacks is important to ensure that productive opportunities are fully exploited towards general good of the society. However, such protection is costly and draws from the same coffer which also provides for creation of productive opportunities.
    - Investment in counter measures reduces productive opportunity in the economy - affecting real Income of ***C*** in the next period, and
    - Given a level of investment in counter measures, a *realized* cyber attack affects real income more than otherwise.

The above alludes to an involved game which can only be modeled in an extensive form (figure-5). As before, insofar as our motivation is limited towards identifying an adequate investment model, we refrain from specifying pay-off structure in this extensive imperfect-information game. Note that the insights of the cyber terrorist's strategies (figure-4) are now integral to the tree diagram (figure-5), and that all macroeconomic factors which may lead to ***G***'s electoral success in the next period is integral to the design of the pay-off structure in the *adequate model* of the game (figure-5).

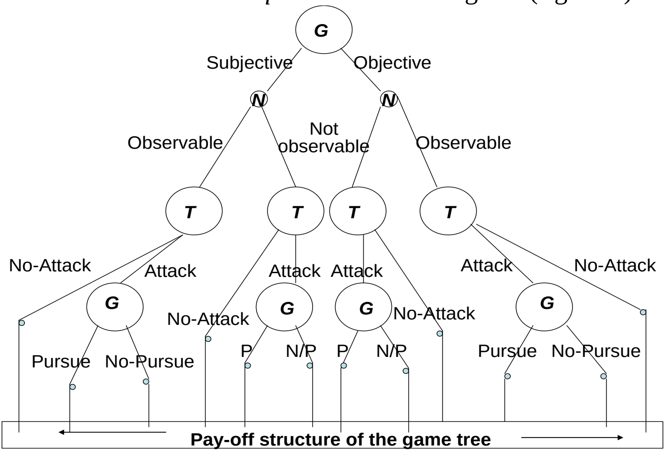


Figure-5

Conclusion and Future Work:

In this work we have developed a simple model (each under decision and game theoretic concepts) that attempts to capture the dynamics of cyber terrorism, and then we have progressively enriched the model to capture the said dynamics in more intimate and realistic fashions. Our focus in this work has been to highlight the factors of influence and the backdrops, such that economic nuances of counter-terrorism investment become clearer. Although our game theoretic model is far more enriching in terms of developing investment insights and equilibrium understandings, the decision theoretic model appears to be more sophisticated in providing quantitative prescription for counter terrorism investments. This is a research in progress, and it is too early to conjecture superiority of one model over the other. However, at this point, it does appear that a hybrid model can be more suitable than either of the models alone. In such a hybrid model, equilibrium strategies could be arrived with the help of game theoretic insights, which could then be integrated in a decision theoretic framework in the pay-off structure; where the utility of the players is maximized given the risk preferences that they exhibit in the cyber terrorism backdrop. This also happens to be our direction in which we propose to continue our future efforts.

REFERENCES

1. Gordon L. A., and Loeb M. P. (2002). The economics of information security investment. ACM Transactions on Information and System Security, 5(4), 438-457.
2. Lenain P., Bonturi M., and Koen V. (2002). The Economic Consequences of Terrorism. OECD Paper. JT 00129726.
3. Rasmussen E. (1989). Games and Information – An introduction to game theory. Second Edition. Blackwell Press, USA.
4. Sunstein, C. R. (2006). Probability Neglect: Emotions, Worst Cases and Law. Chicago Law School Working Paper.
5. Varian, H. (2002) System Reliability and Free Riding. Working Paper. The University of California at Los Angeles.
6. Wenzlaff K. (2004) Terrorism: Game Theory and Other Explanations. Universitat Bayreuth Student Paper.