2008

Defending Cyber Terrorism - A Game Theoretic Modeling Approach

Tridib Bandyopadhyay
Kennesaw State University, tbandyop@kennesaw.edu

Herbert J. Mattord
Nova Southeastern University, mattord@nova.edu

Defending Cyber Terrorism - A Game Theoretic Modeling Approach

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

Herbert J. Mattord, CISM, CISSP
Nova Southeastern University
mattord@nova.edu

ABSTRACT

In this work we attempt to develop a game theoretic model that can indicate the nuances of strategic investments in the face of possible cyber terrorist attacks. First, we briefly review the literature on terrorism. Second, we identify the ‘cyber’ factors in terrorism, and how this new mode of attack alters the general scenario. Then, beginning with a naïve counter terrorism model, we incrementally incorporate the factors of cyber terrorism to develop our game theoretic model. Our current work is geared towards developing a model that can adequately incorporate the cyber factors of today’s networked economy. In this report, we have also discussed some preliminary insights of (countering) cyber terrorism from the proposed model. This is a research in progress; and we have not yet analyzed the model in its entirety to realize the whole range of conceivable insights.

Keywords

Cyber Terrorism, Counter Terrorism, Cyber terrorist, Cyber attack, Cyber defense, Game

INTRODUCTION

Current understanding of threats of terrorism is different in one significant way. Information systems are central to our infrastructure and business processes, and the networked world makes it possible that a threat could originate from anywhere in the globe. Cyber terrorism is no longer a dooms day prognosis, it is a real possibility. Such possibilities have been appreciated in business, government and media. Because anonymity is easier, and open standard network interconnectivity is seamless over the Internet, cyber terrorism could as well emerge as one of the preferred modus operandi of the terrorists in near future.

Countering cyber-terrorism is an onerous and investment intensive task. That our information risks are now interdependent and that information assets/resources could be accessed from great geographical separations, the challenges for the defender devolve to a whole new dimension. There is scant research in understanding the strategic behaviors (including investments) of countering cyber terrorism. The goal of this research is to model the strategic battle between the attackers and the defenders of cyber terrorism, which can be utilized (analyzed) to understand the effect of the *distributed and interconnected nature of the information assets* of national interest on the attack/defense strategy of the cyber-terrorist/sovereign government, especially under the obfuscating conditions of electorates’ *probability neglect* and broader *macroeconomic* mandate of the government.

Modeling terrorism has been considered in economics and social sciences, and there is considerable research in those streams. In this research we build on the insights from those researches and augment them with cyber specific issues. In order to analyze the strategic behavior of the cyber terrorists and the strategic investment decisions of the defender, we model i) the issue of interconnectivity among information assets/resources (which is central to the efficiency of our economy, infrastructure, and governance), and ii) general lack/absence of observability of countermeasures (which otherwise usher deterrence to attackers, and assurance to the stakeholders). Additionally, for governmental defenders, we also consider the effects of iii) ‘probability neglect’, and iv) multi-period re-election issues.

In what follows, first we introduce the concepts and risks/losses from terrorism in general and cyber terrorism in specific, and then review pertinent literature on terrorism from Economics and Social Sciences, and present their central insights. Second, we identify the novelties of an attack, when terrorism is vectored through the cyber space. Third, through a set of incremental models, we introduce issues of cyber terrorism towards an adequate model for strategic analysis of (countering) cyber terrorism. This we achieve in a conjoined fashion: first we create the front end of the model, and then integrate the supply/provisioning side to it. This is a research in progress, and our analysis of the final model is only in an initial stage, which we do not report here.

TERRORISM

US patriot act, 2001 defines terrorism as "activities that (A) involve acts dangerous to human life that are a violation of the criminal laws of the U.S. or of any state, that (B) appear to be intended (i) to intimidate or coerce a civilian population, (ii) to influence the policy of a government by intimidation or coercion, or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping, and (C) occur primarily within the territorial jurisdiction of the U.S." The high points of this definition include intentional intimidation and coercion of civilians and governments, and mass disruption of business, life and livelihood. UK Terrorism act of 2000 significantly adds purposes of such acts: "… purpose of advancing a political, religious or ideological cause".

Terrorism has been analyzed for its macroeconomic determinants ((Abadie (2004), Blomberg, Hess, and Weerapana (2004), Tavares (2004), Li (2005)) and micro-empirical supports (Krueger and Maleckova (2003), Berrebi (2003)). The economic impact of terrorism is difficult to calculate and estimates could run very high numbers (For example, a nuclear attack on NY could cost our economy 3% of its productive capability), with attendant increase in economic uncertainty and attrition in public confidence (Lenain et al. 2002). Other impacts, including fear triggered/related behavioral and psycho-political effects on our citizens and businesses could be substantial ((Becker and Rubinstein (2004), Sunstein (2003), Viscusi and Zeckhauser (2005), Viscusi and Zeckhauser (2003)). Long term macroeconomic shifts, affecting economic development, investment, employment, and national income are also likely ((Blomberg, Hess and Orphanides (2004), Gupta, Clements, Bhattacharya and Chakravarti (2004), Tavares (2004)).

CYBER TERRORISM

Post 9/11 sentiment in US is characterized by caution, apprehension, and a heightened sense of vulnerability: our physical isolation from the known sources of terrorism now stands shattered. However, physical distance, as such, is already insignificant in one expected scenario of terrorism: terrorism utilizing the cyber space. Terrorists' probable uses of the Internet have been extensively researched before and after 9/11 (Soo Hoo et al. (1997), Furnell and Warren (1999), Cohen (2002), Thomas (2003), and Weimann (2004)): many of which have been corroborated by intelligence findings (Conway, 2005). A superset of the terrorist uses of the Internet indicated by the above studies include propaganda, profiling, Covert/secure communication, generating cyberfear, finance, planning, command and control, mobilization and recruitment, information gathering/sharing, mitigation of risk, theft/manipulation of data, misinformation, and offensive use. Among these, our current work focuses on the *offensive* use of the cyber space, i.e. attacks vectored through the cyber space.

Economic impacts of cyber attacks have been modeled predominantly within business perspectives. Although findings contradict whether 'type of firms' is a determinant in the loss in stock value following a cyber attack, researchers agree that the affected firms' stock values do show downward fall (Cavusoglu et al.(2004), Campbell et al., Ettredge et al., and Garg et al.). Losses to business from the whole range of attacks/frauds have been surveyed, and reported on a yearly basis in considerable detail (CSI/FBI surveys 2002- - 2007). On the other hand, there are numerous detailed prognostic/systemic studies of impact of cyber attacks on critical infrastructure and national assets, especially by the (contracts through) national laboratories in US (www.nist.gov), and (among others) highly technical proposal of genetic algorithm based IDS systems as countermeasures for cyber terrorism (Hansen et al. (2006)) has been argued.

Although there is a large body of game theory modeling of terrorism in the Economics literature[1], there appears to be little modeling effort to include cyber specific factors. On the other hand, researchers in IS have mostly focused on business losses and not on econo-political impacts on the government and its subjects. In this work, we attempt to develop a game theoretic model for countering cyber terrorism: our players in the game are the government, the citizens (agents) and the cyber terrorists. We begin with a naïve model of cyber terrorism with initial cyber factors. Next, we specifically bring in the considerations of a sovereign government as the defender. We also discuss affect based subjective bias among the citizens and how that can translate to subjective decision making processes in a governmental setup. While the analysis of the model is in progress, here we report the incremental development of the model including the insights of attack/defense strategies.

GAME THEORETIC MODELING OF CYBER TERRORISM

Cyber Terrorist versus System Defender: Pure Strategy Equilibrium with Internet Anonymity

We represent this game in strategic form (Figure-1). Player ***D*** is the Defender of the system, which Player ***T*** (the cyber terrorist) attempts to compromise. The defender must decide between the two levels of defense, *High (H)* or *Low (L)*. In practice, a *high* level of defense could include defense in layers (combining preventive, diagnostic as well as mitigation regimes of IT security) which is inherently more expensive than the *low* level (where only a subset of the regimes is

[1] For example, vide http://www.meteck.org/TERRORISM_WP.pdf. We review more research during our model development process.

implemented). In line with cyber systems, we assume that the technical countermeasures are not (readily) observable by the cyber terrorist. *High* level of defense reduces the probability of success of the terrorist, or the damage, or both, depending on the layered regimes. Insofar as the terrorist's goal is to create disruption, *high* level of defense reduces the terrorist's expected payoff. On the other hand, *low* level defense is inexpensive, but the chance that the terrorist will be successful is high, or the damage is high (or both), which translates to an increased expected payoff. For now, assume that the defender acts only defensively. On the other hand, the cyber terrorist's choices are to *Attack (A)* or *not to Attack (NA)* the system. That a successful attack yields zero-sum payoff to ***D*** and ***T*** is another simplification in this model.

The exhaustive set of the strategies of the game is [{*H*, *A*}, {*H*, *NA*}, {*L*, *A*}, and {*L*, *NA*}], and Figure-1 depicts the payoffs when these strategies are played. ***D*** prefers to invest *High* if ***T*** chooses to *Attack*, else invests *Low*. However, irrespective of ***D***'s level of investment, ***T*** has higher payoff for *Attack* than *No-attack*. Thus we have a dominant strategy for ***T***. ***D*** behaves strategically, and foresees this dominant strategy of ***T***. Knowing that an attack is imminent, ***D*** invests *High* in cyber defense mechanisms, where her payoff is higher $(-5 > -10)$. The strategic/rational decisions of both ***T*** and ***D*** leads to the unique strategy/conclusion that ***D*** will implement strict controls and ***T*** will attack to breach such controls. One noteworthy aspect of this game is this unique pure-strategy equilibrium. Also note that this outcome/expectation is echoed in popular press, although expectations of cyber terrorism and their effects do differ in imminence and/or magnitude of impact. Such belief is also bolstered by the ***anonymity*** that the Internet offers to the cyber terrorist in general.

Cyber Terrorist versus System Defender: Perturbed Internet Anonymity, and Mixed Strategy Equilibrium

That *anonymity* is important in the cyber terrorism game in defining a unique equilibrium is credible and interesting. Assume that ***D*** now strategizes to create capability to alter the issue of *anonymity* in the game that works in favor of the cyber terrorist. ***D*** can additionally invest in cyber forensic technologies to achieve capability to pursue and track ***T*** after the attack. Note that the strategy of *pursuit* (***P***) does not per se reduce the losses of an actually realized attack; although it creates a strategic deterrence for ***T*** by increasing the implicit cost of her attack. Addressing the issue of *anonymity* in cyber terrorism changes the game substantially (Figure-2) in terms of the equilibrium.

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

Figure-1

D \ T	A	N/A
P	-100 -5 Q- I	0 -10 Q- II
N/P	+10 -15 Q- IV	0 0 Q- III

Figure-2

That ***D*** now has the capability to counter the systemic advantage of (Internet) anonymity of ***T*** is reflected in the redesigned pay-off structure of the game (Figure-2):

1. A cyber terrorist apprehended and punished by law likely brings much confidence to the citizens (-5 > -15). It also sends a strong message of deterrence to other scheming cyber terrorists. However, on the other hand, if no attack is realized from ***T***, then the additional investments to achieve the capability to pursue ***T*** is uncompensated (-10 < -5).
2. In order to signify high penalty (possibly including capital punishments) in the eventuality of being caught and punished, the expected payoff of ***T*** is now much lower when the defender has invested in cyber forensics, and developed capability to pursue[2] (-100 < +10).

D's newly available option of investment in pursuance capabilities devoid the game of a dominant strategy for ***T*** (figure-3):

1. If ***T*** decides to attack, investment in *pursuit* is better than otherwise (-5 > -15). The game begins at quadrant ***Q-I***.

[2] We simplistically assume that the capability to pursue is perfect

2. Foreseeing that facing an *attack* strategy from ***T***, ***D*** could rationally invest in pursuit capability, ***T*** rationally opts *not to attack* (0 > -100). The game moves to quadrant ***Q-II***.
3. However, if ***T*** decides not to attack ***D***, then ***D*** has no reason to invest in pursuit capabilities (0 > -10), and the game moves to quadrant ***Q-III***.
4. However, in absence of ***D***'s capability to pursuit, ***T*** is now better off *Attacking* ***D*** than otherwise (+10 > 0), and the game proceeds to quadrant ***Q-IV***.
5. By the first argument, the game now makes a transition back to quadrant ***Q-I***.

Clearly, the above cycle continues indefinitely, and there is no pure strategy equilibrium. An attempt to achieve equilibrium through pessimistic/worst case approach (*minimizing the maximum losses*) is not decisive either:

1. On one hand, the worst payoff for ***D*** is (-15) if ***T*** attacks, else (-10). Thus the *Min-Max* strategy for ***D*** is to always invest in pursuit capabilities (-10 > -15).
2. On the other hand, for *pursuit* strategy of ***D***, the worst payoff for ***T*** is (-100), else (0). Thus the *Min-Max* strategy for ***T*** is *No-Attack* (0 > -100).

However, it is easy to see that the *Min-Max* strategies of the players are not in Nash Equilibrium. Irrespective of which player (***T*** or ***D***) implements the *Min-Max* strategy, the other player rationally deviates. Thus, Anonymity through the Internet, once preempted, leaves us without a predictable outcome in pure strategy.

However, reasonable expectation leads us to the possibility of the players mixing (randomizing) their strategies. Because we consider a one shot finite game, a mixed strategy Nash Equilibrium is plausible. A *mixed strategy* of ***D*** in this game is to *Pursue* (i.e. invest to build such capability) but only with a certain probability**.** Randomizing is a cost effective approach in this context: although pursuit is not certain, a sufficiently high probability of identification can effectively deter ***T***. Mixed strategy of ***T*** here refers to the randomized decision to attack a certain resource or a certain part of information network.

T (***D***) randomize between strategies of *attack* and *no attack* (*pursuit* and *no-pursuit*) in such a fashion that ensures equal expected payoffs, i.e. ***T*** (***D***) is *indifferent* between available strategies. We calculate the indifferences of ***T*** (***D***) from the mixed strategies of ***D*** (***T***):

1. If ***D*** randomizes *pursue* with probability x, and *no pursue* with probability $(1-x)$, the 'indifference' between strategies of ***T*** occurs at the solution of $\left(x.-100+(1-x).\,10=0\right)$, or $x \approx 9.1\%$.
2. If ***T*** randomizes *attack* with a probability *y*, and *no attack* with probability $(1-y)$, then 'indifference' between the strategies of ***D*** occurs at the solution of $\left(y.-5+(1-y).-10=y.-15+0\right)$, or $y=50\%$.

The solution above suggests that ***D*** should invest to achieve capability to pursue 9.1% of all attacks (or any attack on designated 9.1% of the critical and protected resources), and the cyber could randomly decide to attack an arbitrary target. Unlike the *Min-Max* strategy before, we do have a mixed-strategy Nash Equilibrium here: so long one player randomizes at her level of indifference, the other player never deviates.

1. The strategy of randomized pursuit by ***D*** changes the earlier dominant strategy of *attack* from ***T***. This is a definite improvement from the first case: facing possible apprehension, ***T*** now randomizes between *attack* and *no-attack.*
2. The expected payoff to ***D*** and ***T*** are -7.5 and 0 respectively[3]. But beyond the 'expected return', the game now captures the risk preferences of the players. A cyber terrorist is unlikely to settle for a confirmed payoff of *0* with a pure strategy of *no attack* (by definition, a terrorist is a risk seeker) and thus ***T*** prefers to randomize between its strategies even with unchanged payoff of *0*. The game is also rational for risk averse ***D***, who ends up with a net negative payoff of *-7.5* (buying security/insurance!).

Cyber Terrorist versus System Defender: Networked Resources and Preempted Anonymity

In spite of its ability to lend intuitive explanations, one major disadvantage of representing the above games in strategic form is that the temporal considerations are not integrated. For example, although provisions for building up pursuit capability may occur at an earlier date, the action of pursuit must follow a realized attack, and this temporal ordering is not apparent in the strategic form of representation. More so, with numerous strategies/options in game, the strategic form of representation

[3] $0.5.-5+0.5.-10=0.5.-15=-7.5 \quad and \quad 0.091.-100+0.909.10=0.091.0+0.909.0=0$

increasingly complicates the design of the pay-off structure (which is instrumental in offering intuitive explanations). In this subsection, we present a more realistic abstraction of the reality in an extended game-tree framework: here the resources are internetworked, and the cyber terrorist can progressively breach more resources exploiting the networked interconnectivity between them. In particular, here we provide the strategic interplay between ***D*** and ***T*** in an extensive imperfect-information game tree framework (Figure-3). The scenario of this front end game between ***T*** and ***D*** is explained below:

1. ***D*** has 2 resources[4] to protect, and these resources share a common connectivity. Because this interconnectivity works solely for the bidirectional 'trusted' communication, assume that there is a fixed probability of cross propagation of breach (***q***, dependent on organizational policies and control measures in place) from one resource to the other. In other words, if the cyber terrorist attacks and breaches one resource, with a subsequent probability ***q***, it can then breach the other resource, utilizing the interconnecting link between the resources. ***D***, for its part, could (invest to) protect both/either/none of these resources (cost rises proportionally), which we now represent in 3 discrete levels (*H*, *M*, *L*). ***D*** further invests to acquire capability to *pursue* a cyber terrorist who attacks one or more of the resources (we incorporate this as a mandatory investment required for preempting anonymity of ***T***). In reality, such deterrence is a required strategy for a sovereign defender, which we further discuss in the following section.
2. A scheming cyber terrorist does not know which of the resources/targets is/are protected (no observability). Thus ***T***'s information set is coarse (depicted in the superimposed oval) - in bolstering our earlier insight that ***T*** may employ a randomizing strategy herself. If a resource is protected (unprotected), ***T*** fails (succeeds) with a certain probability (***p***). Assume, for simplicity, that ***T*** has enough resource to attack only one resource at a time. However, if ***T*** succeeds to breach one resource, for sure he could progressively attempt to breach the other resource utilizing the interconnecting link, wherein ***T*** succeeds with a fixed probability of success (***q***).

We do not provide hard numbers or present elaborate pay-off structure in this game tree because our current effort is focused towards development of the cyber terrorism game framework in a minimally sufficient manner, and also because we do not carry out any analysis of the model here. Although we do not provide any risk preference structure in designing the model here, it is instructive to note that so long we maintain a relative difference of risk preferences between ***T*** and ***D*** in the right direction, the model likely provides comparable insights. Although we do not provide any sketches/outlines for solution, it is also important for us to clarify that the nature of *imperfect information* in the game precludes a backward induction strategy for solution.

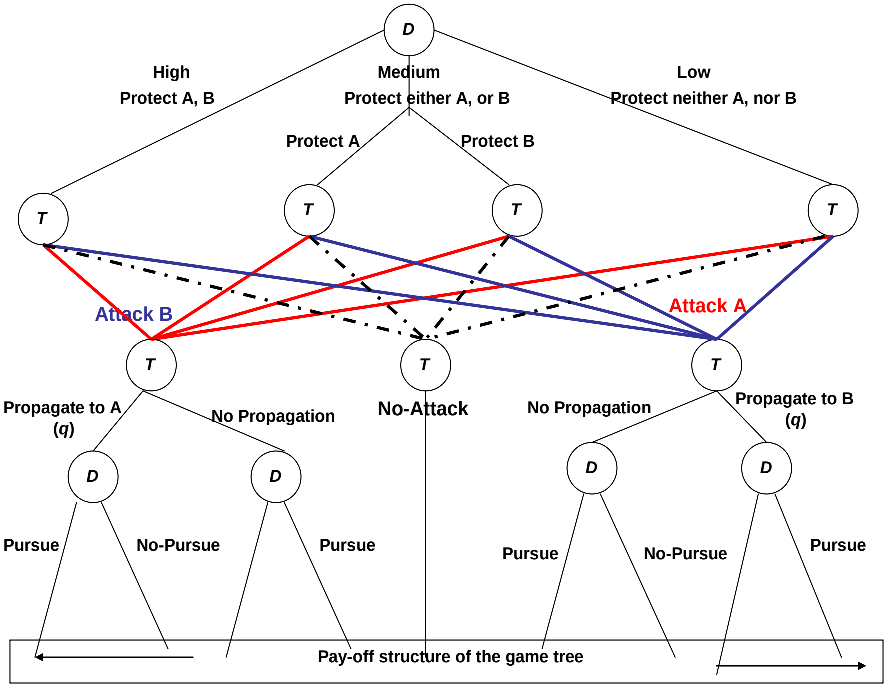


Figure-3

[4] multiplicity of resources to gain insight, yet simplified in number to ensure some tractability

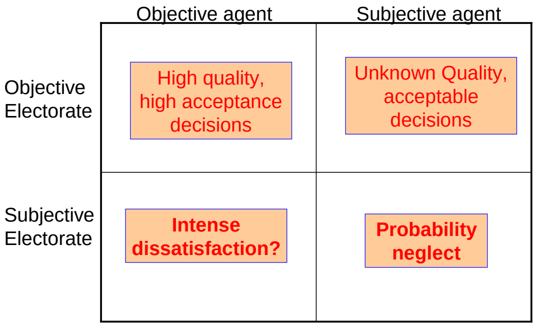
The Government as the Defender

We now consider the more specific case where the defender is the (elected) federal government (***G***) of a country. In this subsection we discuss the supply side of the game as against our earlier focus on the front end of the counter-terrorism game.

G employs knowledgeable agents to strategize counter-terrorism initiatives. Utilizing our earlier framework (Figure-3), agents could objectively estimate the randomizing strategies of the cyber terrorist, and also estimate the concomitant losses that could result. However, one major disconnect appears important in this context: G may be mandated to represent the electorates' sentiments, which may be subject to affective bias (***probability neglect***, discussed in the next paragraph). This disconnect appears at the level of the agents and their selection/election process. Agents immune from the election processes are likely to initiate counter terrorism strategies in an objective fashion. However, the same may not be true for agents who are nominated by the government, or are elected representatives. The game takes an interesting turn here.

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[5]. 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 realization of such acts of terrorism - higher than what pure economic rationality could justify. Social researchers call this phenomenon '***probability neglect***'. This is likely to be apparent when we think about cyber terrorism - when cyber terrorists could hack into our interconnected information/infrastructure systems, and wreak havoc in basic life and livelihood of the citizens. Dooms day prognostics, media hype, science fiction, and ultra advocates have vividly painted many possible events[6]. Such probability neglect, in mass scale, can have far reaching effects. For example, among others, this could give rise to a general need for higher protection from ***G*** to obviate such events. Such needs in turn, translate to demand for stricter regulation and/or higher government/corporate spending to mitigate such risks of terrorism. Finally, through elected officials or government-nominated agent, popular *probability neglect* could eventually cause higher (?) than optimal investment/regulation in the prevention and mitigation of cyber terrorism. This is beyond the economic rationality of ***G***: we will differentiate this by identifying the fact the ***G*** may as well *subjectively* strategize her counter terrorism measures, which is likely to be higher than the *objective* strategy of ***G***. The possibilities of resultant decisional quality and acceptability are represented in figure-4[7].

Decisional Disconnects between Electorates and G's Agents



	Objective agent	Subjective agent
Objective Electorate	High quality, high acceptance decisions	Unknown Quality, acceptable decisions
Subjective Electorate	**Intense dissatisfaction?**	**Probability neglect**

Figure-4

Given the changed scenario, the issues of objectivity/subjectivity and observability/unobservability are important:

1. The level of objectively decided investment is to counter attacks from ***T***, an *uncertain future event*. The subjectively decided investment takes care of

[5] "… 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.**

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

[7] Adopted from Simon Luchinger's comment on 'Precaution against Terrorism' by Wiener et. al (2006) in 'Managing Strategic Surprises: Lessons from Risk Management and Risk Assessment', editors Bracken et al. at Workshop and Lecture Series in "Law and Economics" at University of Zurich, Winter Term, 2005/06

  a. ***G***’s allegiance to the electorate (and indirectly their ‘level of need’ to be protected from ***T***) and
  b. ***G’***s desire to succeed in the next electoral process, a *certain event with uncertain outcomes*.

2. The counter measures (the extent of which is decided subjectively or objectively) taken by the agents of ***G*** may or may not be observable to ***E***.

  a. If ***E*** cannot observe counter measures, unfavorable apathetic attitude of ***G*** may be inferred,
  b. If ***E*** observes counter measures, and ***T*** attacks but fails to succeed, a very favorable impression for ***G*** may be expected,
  c. If ***E*** 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.

- Counter-terrorism is a security product that the elected government must provide to its electorate. This is justifiable because a climate of protection against cyber terrorist attacks is important to ensure that productive opportunities are fully exploited towards higher income/consumption of the electorate in general. However, such protection is costly and the resources are draws from the same tax coffer which also provides for creation of productive opportunities.
  - Investment in counter-terrorism measures reduces productive opportunity in the economy - affecting real Income of ***E*** in the next period, and possibly reducing consumption in the current period.
  - Given a level of investment,
    - Realized cyber attack affects real income that could bear inverse relationship with the level.
    - No realization of attack keeps productive opportunity unaffected at the security level, but cost of security good is uncompensated.

We have modeled the aggregate game in an extensive form. Note that the insights of the cyber terrorist’s strategies are integral to the tree diagram, and so also is the tension between the political and economic decisions of the sovereign government (figure-5). Our motivation here is limited to developing a model which could capture the neo-threat of cyber terrorism, and we have presented a framework that is consistent with the IS domain observations and macroeconomic ramifications. We have not provided any specific pay-off structure, which could remain fairly generic in the modeling scenario.

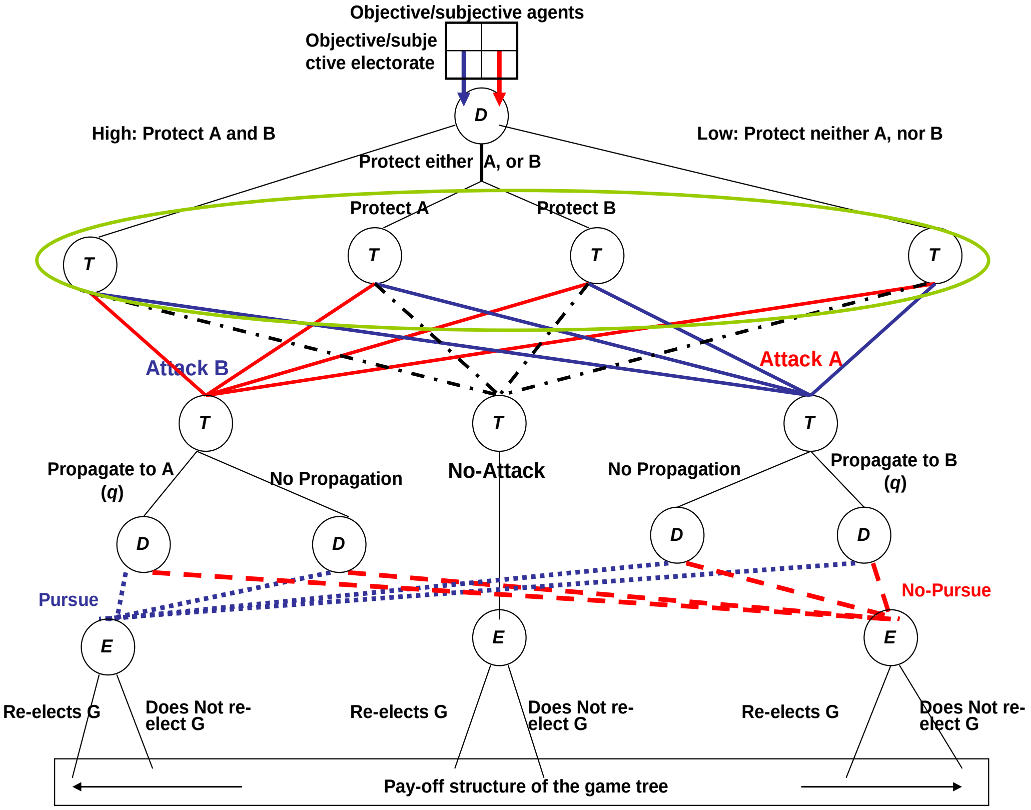


Figure-5

Conclusion and Future Work:

In this work, we have progressively enriched a naïve game theoretic model from the front-end as well from the supply side.

In the supply side, the sovereign defender acquires its budget and provisioning opportunities from the tax coffer, leaving macroeconomic ramifications in the productive opportunities of the country. Provisioning apart, the elected government may also remain encumbered in a decision scenario where subjective elements (stemming from the process/mandate of popular election to reflect electorate sentiments, including *probability neglect*) may impair purely objective measures. At this cross road, quality of decision could be weighed against acceptability/likability of decisions.
In the front end, pursuance appears to be a very effective strategy, forcing the cyber terrorist to relinquish the dominant strategy of attack. A layered defense is effective but costs dearly. Given that we would like to have pursuance capabilities, this may translate to very high outlay in countering cyber terrorism. Having preventive measures observable for the cyber terrorist usher unknown effects, thus deterrence by observability does not appear to be a much supported idea. Further complicating the scenario is the distributed and/or interconnected nature of our information assets which are of interest to the cyber terrorist. That our information risks are so interdependent, the front end game becomes substantially involved.

Finally, we have brought together the insights and modalities of both the front and back end to present an aggregate model that adequately capture the scenario of cyber terrorism. We do not provide any solution of the model, which is currently in an ongoing stage.

REFERENCES

1. Abadie, A.: 2004, Poverty, political freedom, and the roots of terrorism, NBER Working Papers, 10859, National Bureau of Economic Research, Cambridge, Mass.
2. Becker, G. S. and Rubinstein, Y. 2004, Fear and the response to terrorism: An economic analysis, mimeo, http://www.ilr.cornell.edu/international/events/upload/BeckerrubinsteinPaper.pdf.
3. Berrebi, C.: 2003, Evidence about the link between education, poverty and terrorism among Palestinians, Princeton University Industrial Relations Section Working Paper 477, Princeton University.
4. Blomberg, S. B., Hess, G. D. and Orphanides, A. 2004, The macroeconomic consequences of terrorism, Journal of Monetary Economics 51(5), 1007–1032.
5. Blomberg, S. B., Hess, G. D., and Weerapana, A. 2004, Economic conditions and terrorism, European Journal of Political Economy 20(2), 463–478.
6. Campbell, K., Gordon, L. A., Loeb, M. P., and Zhou, L. 2003. The Economic cost of Publicly Announced Information Security breaches: Empirical Evidence from the Stock Market. Journal of Computer Security. Vol. 11(3)
7. Cavusoglu, H**.**, Mishra, B. Raghunathan, S. (2004). The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reaction for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce 9(1), 69-105.
8. Cohen, F. 2002. Terrorism and Cyberspace. Network Security Vol. 5.
9. Ettredge, M., and Richardson, V. J. 2002. Assessing the Risk in E-Commerce. Proceedings of the 35th. HICCS.
10. Furnell, S. and Warren, M. 1999. Computer Hacking and Cyber Terrorism: the Real Threats in the New Millennium. Computers and Security 18(1).
11. Garg, A., Curtis, J., and Halper, H. 2004. Quantifying the Financial Impact of IT Security Breaches. Information Management and Computer Security Vol. 11(2).
12. 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.
13. Gupta, S., Clements, B. J., Bhattacharya, R. and Chakravarti, S.: 2004, Fiscal consequences of armed conflict and terrorism in low- and middle-income countries, European Journal of Political Economy 20(2), 403–421.
14. Hansen, J. V., Lowry B. P., Meservy, R. D., and McDonald, D. M. 2006. Genetic programming for prevention of cyberterrorism through dynamic and evolving intrusion detection. Decision Support Systems 43(4).
15. Krueger, A. B. and Maleckova, J.: 2003, Education, poverty and terrorism: Is there a causal connection?, Journal of Economic Perspectives 17(4), 119–144.
16. Lenain P., Bonturi M., and Koen V. (2002). The Economic Consequences of Terrorism. OECD Working Paper No. 334. JT 00129726
17. Li, Q.: 2005, Does democracy promote or reduce transnational terrorist incidents? Journal of Conflict Resolution 49(2), 278–297.
18. Rasmussen E. (1989) Games and Information – An Introduction to Game Theory. Second Edition. Blackwell Press, USA.
19. Soo Hoo, K., Goodman, S., and Greenberg L. 1997. Information Technology and Terrorism Threat. Survival 39(3).
20. Sunstein, C. R.: 2003, Terrorism and probability neglect, Journal of Risk and Uncertainty 26(2- 3), 121–136.

21. Tavares, J.: 2004, The open society assesses its enemies: Shocks, disasters and terrorist attacks, Journal of Monetary Economics 51(5), 1039–1070.
22. Varian, H. (2002) System Reliability and Free Riding. Working Paper. The University of California at Los Angeles.
23. Viscusi, W. K. and Zeckhauser, R. J.: 2003, Sacrificing civil liberties to reduce terrorism risks, Journal of Risk and Uncertainty 26(2-3), 99–120.
24. Viscusi, W. K. and Zeckhauser, R. J.: 2005, Recollection bias and the combat of terrorism, Journal of Legal Studies 34(1), 27–55.
25. Weimann, G. 2004. How Modern Terrorism uses the Internet. United States Institute of Peace, Washington, DC. (http://www.usip.org/pubs/specialreports/sr116.pdf)
26. Wenzlaff K. (2004) Terrorism: Game Theory and Other Explanations. Universitat Bayreuth Working Student Paper