Understanding Optimal Investment in Cyber Terrorism: A Decision Theoretic Approach

Tridib Bandyopadhyay, Kennesaw State University, USA

ABSTRACT

In this work, the author develops and explains a set of economic models under the decision theoretic framework to conceptualize the requisite levels of investment in the defense against cyber terrorism. This paper begins with a naïve model of cyber defense, on which the author progressively implements aspects of layered defense and domain conditionality to investigate practicable investment levels for countering cyber terrorism related risks. The proposed model characterizes the minimum budget below which a defending nation cannot feasibly contemplate to deploy more than one layer of defense against cyber terrorism. Beyond budgetary considerations, the paper also calculates the relative technological capabilities that the defending nation must possess to deploy a detection regime behind the first layer of protection regime. Finally, the author calculates and presents the optimal bifurcation of budget between the prevention and detection regimes should the defending nation possesses adequate funds to deploy layered defense in cyber terrorism.

Keywords: Cyber Defense, Cyber Terrorism, Domain Conditionality, Layered Defense, Technology Investment Decisions

INTRODUCTION

Our understanding of terrorism has significantly changed from what it was before 9/11. The lives and assets of one of the mightiest nations in the world - separated from most of the known terrorism threat centers of the post second world order – was violated by a sub national or dissident group in the most blatant fashion. Concerns, measures and readiness against terrorism have taken a whole new dimension in the post 9/11 world.

Further, an important variant of the terrorism problem has emerged in view of the modern networked economy, in which all forms of business and governance must thrive. As information systems and information assets become integral to all business processes, and information and network assets get increasingly internetworked with the help of Internet based technologies, assaults on a nation’s assets no longer require physical means, medium or presence like that of 9/11. Subversive elements can create and dispatch threat vectors over the Internet from far flung areas and cause devastating blows on our economy or public life. For example, our banking and financial systems could be brought to a halt with the help of a fast propagating computer worm, or critical infrastructures like power grids could be shut down after overpowering supervisory controls.
like automated relays in switchgears with the help of computer bugs.

Cyber terrorism has been defined in different lights by the experts in the field (e.g., Politt, 1997; Denning, 2000). However, there are some generally agreed commonalities: Cyber terrorism is (a) perpetrated by groups having foreign allegiance or sub national agenda for political reasons, which (b) targets the property and life of nations, and (c) utilizes modern ICT (Information and Communication Technologies) and cyber space in the way the threat vectors are conceived, dispatched and activated in order to (d) create huge, visible and psychologically impactful outcomes of catastrophic proportions.

Although such possibilities of electronically driven terrorism threats was not widely appreciated by the stakeholders of the networked infrastructure and systems before the 9/11 attack, active deliberations on such possibilities in the intelligence circles has been documented. Former FBI Director Lois Freeh, in a statement on May 10, 2001 before the United States Senate Committee on Appropriations, Armed Services, and Select Committee on Intelligence deposited, “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.”

As we increasingly embrace the ICT and cyber space in the way we conduct business, monitor and manage infrastructural services and interact in our social circles, and especially in view of the current trend in electronically mediated governance, the impacts of cyber terrorism are far reaching than before. Further, the distributed nature of the interconnected systems ensure that the attacks could be seeded and initiated from any point on the network and can be executed at any other point of the network - emphasizing further gravity of the eventuality and difficulty of defense. The risks of cyber terrorism also exhibit interdependency between the defenders of the systems owing to the propagatory nature of threats, adding further difficulty in the way adequate defense could be ensured. It is thus imperative that the defense against cyber terrorism threats be fundamentally understood by the stakeholders of today’s globally interconnected information systems.

As such, countering cyber terrorism is onerous. Investments are required to place prevention and detection technology controls on the network and information assets and also keep aside provisions for exigencies towards incidence response, incidence containment, and business and governance continuity. Funds are also needed for developing pre-attack defense capabilities and proactive measures in terms of intelligence and deterrence as well for creating and managing post detection capabilities like legal frameworks and enforcement capabilities. This further underscores the need to understand the dynamics of multifaceted investments in defense against cyber terrorism.

In this work, we focus on the economic fundamentals of cyber defense and demonstrate the investment dynamics of countering cyber terrorism. In particular, we present a series of progressively mature models under the framework of decision theory - where the adversaries are implicitly modeled in the way the threats are realized - and against which the defender must establish optimal level of defense to combat the probabilistic attacks of cyber terrorism. The article is organized as shown.

In the next section, we provide a brief review of the relevant literature. The section that follows, further divided into several subsections, incrementally contextualizes the decision theoretic investment models to suit the dynamical and pragmatic considerations of cyber terrorism. We then discuss the insights from the analysis of this model development effort and present our concluding thoughts.

LITERATURE REVIEW

Researchers have provided varying definitions and criteria for cyber terrorism. For example,
Aligning Two Specifications for Controlling Information Security
www.igi-global.com/article/aligning-two-specifications-for-controlling-information-security/123512?camid=4v1a