Reliability Engineering and System Safety 95 (2010) 29–42

Contents lists available at ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Defense and attack of complex and dependent systems

Kjell Hausken *

Faculty of Social Sciences, University of Stavanger, N-4036 Stavanger, Norway

ARTICLE INFO

Article history:
Received 23 January 2009
Received in revised form
13 July 2009
Accepted 27 July 2009
Available online 6 August 2009

Keywords:
Complex infrastructures
Reliability theory
Game theory
Defense
Attack
Contest success function
Parallel system
Series system
Complex systems
Dependent systems
Interdependent systems
Protection
Terrorism

ABSTRACT

A framework is constructed for how to analyze the strategic defense of an infrastructure subject to attack by a strategic attacker. Merging operations research, reliability theory, and game theory for optimal analytical impact, the optimization program for the defender and attacker is specified. Targets can be in parallel, series, combined series-parallel, complex, *k*-out-of-*n* redundancy, independent, interdependent, and dependent. The defender and attacker determine how much to invest in defending versus attacking each of multiple targets. A target can have economic, human, and symbolic values, subjectively assessed by the defender and attacker. A contest success function determines the probability of a successful attack on each target, dependent on the investments by the defender and attacker into each target, and on characteristics of the contest. The defender minimizes the expected damage plus the defense costs. The attacker maximizes the expected damage minus the attack costs. Each agent is concerned about how his investments vary across the targets, and the impact on his utilities. Interdependent systems are analyzed where the defense and attack on one target impacts all targets. Dependent systems are analyzed applying Markov analysis and repeated games where a successful attack on one target in the first period impacts the unit costs of defense and attack, and the contest intensity, for the other target in the second period.

1. Introduction

Infrastructure threats emerge from nature, technology, and humans, exacerbated by complexity and population growth. The September 11, 2001 attack demonstrated that no targets and no methods of operation are out of bounds. Crucial strategic decisions for defenders and attackers are resource allocation across targets.

Reliability theory has traditionally solved the defender's optimization problem, hardening targets and increasing the probability of system survival. Parts of the literature associates one defender with each target, which causes conflict when defending multiple targets. Kunreuther and Heal [1], Zhuang et al. [2], and Hausken [3] analyze interdependent systems, Enders and Sandler [4] analyze substitution across targets, and Gordon and Loeb [5] analyze cyber security resource allocation. The alternative is to let one defender defend an entire system. Bier et al. analyze [6] series and parallel systems with independent targets. Azaiez and Bier [7] let the defender deter attacks by making them costly, assuming constant attack success probability.[1]

Accounting for both the defender's and attacker's viewpoints have become more prominent in recent research, notably by Bier and Azaiez's [8] edited book. Guikema [9] reviews game theory models of intelligent actors in reliability analysis. Levitin [10] determines defense strategies for complex multi-state systems. Hausken et al. [11] consider protection against natural disaster, terrorism, and all-hazards where agents move simultaneously or sequentially. Azaiez [12] analyzes a game of information in optimal attack/defense strategies. Gaver et al. [13] evaluate how a counter terrorist seeks early detection and neutralization of a terrorist. Paté-Cornell et al. [14] apply single and alternate move

[1] Brown et al. [23] consider interdiction models and defender–attacker–defender models. Patterson and Apostolakis [24] introduced important measures for ranking the system elements (geographic regions) in complex systems, allowing decision makers to determine critical locations susceptible to terrorist attacks. Michaud and Apostolakis [34] analyzed such measures of damage caused by the terror as impact on people, impact on environment, impact on public image, etc. Zhuang and Bier [25] consider defender resource allocation for countering terrorism and natural disasters. Hausken and Levitin [26] present algorithms for separation and protection. Levitin and Hausken [27] analyze redundancy, protection, and false targets. Within political economy and political science strategic interaction has been accounted for more extensively. See Powell [28], and Sandler and Siqueira [29] for recent developments.

* Tel.: +47 51 831632; fax: +47 51 831550.
E-mail address: kjell.hausken@uis.no

0951-8320/$ - see front matter © 2009 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2009.07.006

Nomenclature

n	number of targets
t_i	defender's investment for target i
T_i	attacker's investment for target i
c_i	defender's unit cost of investment for target i
C_i	attacker's unit cost of investment for target i
v_i	defender's valuation of target i
V_i	attacker's valuation of target i
v	defender's valuation of system functionality
V	attacker's valuation of system functionality
p_i	probability of successful attack on target i
m_i	attacker–defender contest intensity for target i
P_k	probability of successful attack on at least k out of n identical targets
d_i	defender's expected damage for target i
D_i	attacker's expected damage for target i
d	defender's expected system damage
D	attacker's expected system damage
α_{ik}	interdependence between targets i and k
τ	time
$\gamma(\tau)$	attack success rate
$Q_j(\tau)$	probability of being in state j at time τ
u	defender's utility
U	attacker's utility

games and probabilistic risk analysis to determine system states including probabilities of outcomes and risks of failures. Cox [15] evaluates how to make telecommunications networks resilient against terrorism. Kanturska et al. [16] assess how to improve the reliability of transportation networks through multi-path routing and link defense.

This article accounts for many of the developments above and introduces a conceptually new way of thinking. The strategic nature, and ever changing dynamic, of multiple attackers interacting with defenders need to be fully accounted for. External threats are neither static, fixed, nor immutable. The defender's point of view is of interest when defending infrastructures. The attacker's point of view is of interest when terminating infrastructures or ensuring that these malfunction. Attacks on infrastructures are made by both illegitimate and legitimate actors, groups, organizations, and nations. The legitimacy of attacks is usually perceived differently by different groups and audiences, and usually also varies across cases. An arbitrarily complex system or infrastructure is considered with targets that are in parallel, series, combined series-parallel, complex, k-out-of-n redundancy, assuming targets that can be independent, interdependent, or dependent. The defender and attacker adapt to each other optimally choosing defensive and offensive investments for each target. The functionality or successful operation of each target depends on the relative investments in defense versus attack. The functionality of the system depends on how the targets are joined together.

This paper provides a framework and lays out a research agenda. We ask, how can the value of infrastructure systems be estimated, how can different system structures be analyzed in a reasonably simple and parsimonious (if approximate) manner, which defender and attacker objective functions are reasonable, how can the resulting optimization problems be solved, etc.

Section 2 defines the problem. Section 3 considers defense and attack investments. Section 4 describes the contest success function. Section 5 describes systems with targets that are in parallel, series, combined series-parallel, complex systems, k-out-of-n redundancy, independent targets, and independent subsystems. Section 6 considers interdependent targets, illustrated with two examples. Section 7 considers state dependent systems analyzed with Markov analysis, and determines attack success rates. Section 8 analyzes dependent systems as repeated games, illustrated with load sharing system. Section 9 concludes.

2. Defining the problem

Consider an infrastructure system with n targets (components) in parallel, series, combined series-parallel, complex, interdependent, independent, and dependent. An infrastructure refers to assets that support an economy, such as roads, power supply, telecommunications systems, water supply, political and economic institutions, businesses, schools, hospitals, recreational facilities, and other assets. A defender minimizes the expected damage of the infrastructure and the investment incurred to protect the system. Damage measures the value,[2] including a system's ability to function reliability according to its stated objective, such as serving a population.

Investments to protect a system can mean hardening targets with defensive fortifications or patrols. The attacker maximizes the expected damage minus the investment costs. This can mean destroying the system, or eliminating or disabling crucial parts so that it cannot operate. For example, roads can be bombed or blocked. Power generators can be destroyed or telecommunication lines cut. Water supply can be diverted or contaminated. A hospital can be destroyed by an air attack, or its health personnel disabled by a chemical attack.

The defender makes n investments $t_1, t_2, \ldots, t_n$ to ensure that the n targets function reliably, and the attacker similarly makes n investments $T_1, T_2, \ldots, T_n$, to ensure that the n targets do not function reliably. Defense and attack are considered in a broad sense. Defense means protecting against the attack, and maintaining and repairing the system so that it does not break down. Attacking means attacking the system, which may get aided by natural factors (technology, weather, temperature, humidity, etc.), to ensure that the system breaks down. The defender and attacker seek to determine the size of their investments, how their investments vary across the n targets, and the effect on their utilities.

A common game theoretic method is to assume that the defender and attacker choose their investments simultaneously and independently for each of the n targets. This gives a non-cooperative game with $2n$ free choice variables.[3] Some infrastructures are built quickly,

[2] A target has economic, human, and/or symbolic value. These are generally different for the defender and attacker, perceived subjectively, and may be unknown to various actors. Most targets possess two or three of these kinds of values. As an example, a target such as $1 million has economic value, no human value, and usually limited symbolic value. Second, a target such as one human being has human value, and symbolic value dependent on its characteristics. The economic value is statistically often calculated as the cost of reducing the average number of deaths by one. Third, a target such as the US Statue of Liberty has substantial symbolic value, and no human value. The economic value can be calculated from its materials, from sales, replacement, or its impact on the economy. Bier et al. [6] consider the "inherent value of a target," defined as "the loss incurred by the defender if a component is disabled." Beitel et al. [30] present six measures for the value of a target.

[3] A variety of tools can be used to determine the optimal strategic choice variables. The utilities, free choice variables, and constraints are programmed into an optimization program, which is solved analytically or numerically on a computer, by the defender, attacker, or an outside analyst.