Protecting Complex Infrastructures Against Strategic Attackers

Kjell Hausken
Faculty of Social Sciences
University of Stavanger
N-4036 Stavanger, Norway
E-mail: kjell.hausken@uis.no
Tel.: +47 51 831632, Fax: +47 51 831550

Version: January 2, 2007

Keywords: Complex infrastructures, game theory, reliability theory, contest success function, parallel system, series system, interlinked systems, interdependent systems, independent systems.

Acknowledgement
I thank Vicky M. Bier for useful comments.

Abstract

A framework is provided for how to analyze the strategic defense of an infrastructure attacked by multiple strategic attackers. Merging operations research, reliability theory, and game theory for optimal analytical impact, the optimization program for each agent is specified. Each agent determines how much to invest in defending versus attacking each of multiple targets. A target can have economic, human, and symbolic values, which generally vary across agents. Investment expenditure functions for each agent can be linear in the investment effort, concave, convex, logistic, can increase incrementally, or can be subject to budget constraints. Contest success functions (e.g. ratio and difference forms) determine the probability of a successful attack on each target, dependent on the relative investments of the defender and attackers on each target, and on characteristics of the contest. Targets can be in parallel, in series, interlinked, interdependent, or independent. The number of first order conditions for the optimization program equals the number of agents times the number of targets. These are conveniently solved applying conventional software on a computer, and give the optimal investments for each agent for each target. Alternative optimization programs are discussed, together with repeated games, dynamic games, and incomplete information. An example is provided for illustration.

1 Introduction

Threats against infrastructures emerge from nature, technology, and humans. Increasing complexity and population growth cause challenges protecting our infrastructures. The September 11, 2001 attack demonstrated that no targets and no methods of operation are out of bounds. Strategic attackers of all flavors go for targets (components) with economic, human, and symbolic value. The strategic decisions for the defender (attackers) are how much to allocate to defense (attack), how to allocate investments across targets, and what kinds of defense (attack) are suitable.

Operations research and reliability theory have traditionally been used to solve the defender's optimization problem.[1] A typical focus has been on hardening targets. The main limitation is that the external threat is usually assumed to be static, fixed and immutable. Some research applying game theory considers isolated targets.[2] For multiple targets one strand of literature associates one defender with each target.[3]

Another strand of literature, to which this article adds new dimensions, lets one defender defend an entire system. This literature is highly relevant for the defense of infrastructures of various kinds at the global, continental, national, regional, and local levels. Earlier promising research by Bier and Abhichandani (2002) and Bier et al. (2005) for series and parallel systems with independent targets have assumed that the defender minimizes the success probability, and expected damage, respectively, of an attack. The success probability is assumed to depend on the resources expended by the defender to strengthen each target. The probability of an attack is assumed to be exogenously given.[4] Azaiez and Bier (2006) assume that the success probability

---

[1] For example, cost-effective risk reduction strategies applying reliability analysis are determined by Levitin (2002, 2003a, 2003b), Levitin and Lisnianski (2000, 2001, 2003), and Levitin et al. (2003).

[2] See for example Major (2002), Woo (2002, 2003), O'Hanlon et al (2002).

[3] Conflicts then arise in series, parallel, and summation systems over which player(s) prefer(s) to incur the cost of risk reduction. Individual strategies at the subsystem level generally conflict with collective desires at the system level. Hausken (2002) lets each agent dichotomously choose a strategy which for his component causes either reliability zero with no cost of effort or reliability one for a fixed cost of effort. He finds that the series, parallel, and summation systems frequently correspond to the coordination game, the battle of the sexes and the chicken game, and prisoner's dilemma, respectively. Kunreuther and Heal (2003), Bier and Gupta (2006), and Hausken (2006a) analyze interdependent systems. Enders and Sandler (2003) and Hausken (2006a) analyze the substitution effect which causes a strategic attacker to substitute into the most optimal attack allocation across multiple targets, and the income effect which eliminates parts of the attacker's resource base. Within cyber security Gordon and Loeb (2002) and Gordon et al. (2003) determine the optimal investment for information protection, and Gal-Or and Ghose (2005) analyze how market characteristics affect security investment.

[4] Bier et al. (2005: 322) show that "if one component is more valuable than another, but has a lower probability of being attacked, then the more vulnerable but less valuable component may be more likely to be attacked, and hence

of an attack on each target is constant,[5] and that the defender attempts to deter attacks by making them as costly as possible to the attacker. This enables them to find closed-form results for systems with moderately general structures with both parallel and series subsystems.

This article introduces a conceptually new way of thinking. One strategic defender and arbitrarily many fully strategic attackers are assumed. The external threat is neither static, fixed, nor immutable. An arbitrarily complex system or infrastructure is considered with targets that are in parallel, in series, interlinked, interdependent, and independent.[6] The defender and attackers 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. The defender seeks functionality of the system while the attacker seeks non-functionality.

The approach allows analyzing the phenomenon from both the defender's and attackers' point of view. The latter has been missing in earlier research on reliability theory, and also in much other research. This constitutes a serious drawback in today's world, where the strategic nature, and ever changing dynamic, of multiple attackers need to be fully accounted for. The defender's point of view is of interest when defending infrastructures. The attacker's point of view is of interest when seeking to terminate infrastructures. Such attacks are often made by nations, organizations, or groups for reactive or proactive reasons. The legitimacy of terminating infrastructures varies across cases. One case considered to have high legitimacy is the objective of terminating the Al Queda infrastructure.

Section 2 discusses how to value targets, which may have economic, human, and symbolic values. Section 3 considers investment expenditure functions for defense and attack. Section 4 evaluates contest success functions. Section 5 describes systems with targets that are in parallel, in series, interlinked, interdependent, independent, and multi-use. Section 6 considers the optimization program for static and repeated games, with and without budget constraints, and with complete and incomplete information. Section 7 analyzes an example. Section 8 concludes.

---

merit greater investment." Bier et al. (2006) analyze the optimal allocation of defensive resources in the face of uncertainty about attacker goals, motivations, and valuations of potential targets.

[5] They also mention the simplification that the level of effort expended by the attacker on each component could be a constant.

2 How to value targets: Economic, human, and symbolic values

A target or component can be conceived to have economic value, human value, and/or symbolic value. These are generally different for the defender and attackers, perceived subjectively for each agent, different across attackers, and may be unknown to others, and sometimes unknown to oneself if a valuation has not been made. We could consider other kinds of value than these, but these have been common in the literature. Three values for each target is sufficient for many purposes, and makes the analysis tractable. Most targets possess two or three of these kinds of values. Let us consider three stereotypical examples.

First, a target such as $1 million has economic value, no human value, and usually limited symbolic value. $1 million may earn symbolic value dependent on the owner, the attacker, dependent on how it is obtained, how it is subsequently used (e.g. destroyed), how it is represented (e.g. in 100 dollar bills), and whether it is represented in U.S. dollars or alternatively in Yen, Euro, or Renminbi.

Second, a target such as one human being has human value which can be considered to be infinite in philosophical or religious terms, and symbolic value dependent on the nationality, competence, age, sex, conviction, and other characteristics of the human. The economic value is statistically often calculated as the cost of reducing the average number of deaths by one. Applying wage-fatality risk tradeoffs, a common estimate for the value of a statistical life is $7 million for U.S. workers (Viscusi 2005). Insurance values are often lower, e.g. $1 million for trains and $20,000 for automobiles.

Third, a target such as the U.S. Statue of Liberty has substantial symbolic value, and no human value. The economic value can in one sense be calculated from the raw materials. 100 tons of copper, priced at $5000 per ton, and 125 tons of steel, priced at $600 per ton, gives $575,000. In other senses, the economic value can be determined from its sales value if it were to be auctioned to the highest bidder, its reconstruction or replacement value if it were to be stolen or destroyed, or its value in impacting the U.S. economy, measured in some manner.

---

[6] See Hausken (2006b) for an analysis of series and parallel systems.

Bier et al. (2005:316) consider the "inherent value of a target," defined as "the loss incurred by the defender if a component is disabled." Similarly, they consider "the value of system functionality," defined as "the loss (in dollar terms) incurred by the defender if the system is disabled." These losses can have economic, human, and/or symbolic dimensions. If a target or system is disabled, repairing or replacing it can be given a value in dollar terms. Beitel et al. (2004) present six measures for the value of a target, with formulas for each. These are loss of life, primary economic loss, national economic stress and inconvenience, decrease Western presence, increase Islamic presence, opportunity to leverage with other terrorists.

The total value of a target has to be determined with care. For the defender we define the economic value of target i as e_i, the human value as h_i, and the symbolic value as s_i. For our purpose we define the total value of target i to the defender as $v_i = e_i + h_i + s_i$, which means that we interpret the three values to be disjoint. The total value thus has to be determined by assessing how the three kinds of values have been determined. For attacker j we define the total value of target i as $V_i^j = E_i^j + H_i^j + S_i^j$, subjectively determined by each attacker.[7]

3 Investment expenditure functions for defense and attack

Generally, targets have to be produced, maintained, repaired, inspected, and defended. There is a tradeoff between how much to invest in these various activities. The defender may prefer or need a high quality target, but high quality targets are more likely to be attacked, which suggests a high defense cost. Hausken (2005) analyzes the tradeoffs an agent makes between producing and defending a target when facing other attacking agents. This approach is contrasted with the approach where the value of the target is exogenously given but subject to defense and attack. Our infrastructures have been produced over time and are gradually improved, repaired, inspected, etc., subject to various tradeoffs. For our purpose, to make the analysis tractable, we consider the infrastructure or system as exogenously given, as has been common in the rent seeking literature.

[7] An alternative is $V_i^j = v_i + \varepsilon_i$, which is the defender's valuation plus an error term for target i. The error term can reflect attacker lack of information about the defender's valuations, or attacker-specific goals such as prominence of target i, or the cost of attacking target i. I thank Vicky Bier for this suggestion.

Generally, to defend target i with exogenously given value v_i, the defender incurs an investment effort $\boldsymbol{t_i}$ (investment, for short) which is a vector with elements that are capital and labor of various kinds. Again we simplify to the scalar t_i. The investment expenditure is $f_i = f_i(t_i)$, measured in dollar terms, where $\partial f_i / \partial t_i > 0$. The function f_i can take many different forms. First, it can increase linearly in t_i defined as $f_i = c_i t_i$, where c_i is the inefficiency of the defense investment for target *i*. Higher c_i means greater defense inefficiency, and $1/c_i$ is the efficiency. We can also interpret c_i as the unit cost of investment. Second, f_i can increase concavely in t_i, $\partial^2 f_i / \partial t_i^2 < 0$, which occurs when there is economy of scale. For example, one unit of effort may be expensive to produce, but producing further units may get successively cheaper as routine, division of labor, and coordination simplify. Third, and conversely, f_i can increase convexly in t_i, $\partial^2 f_i / \partial t_i^2 > 0$, which occurs when there are diseconomies of scale. For example, one worker may easily generate the first unit of effort if little physical or mental effort is required. However, producing additional units of effort may get successively more expensive as physical and mental exhaustion, strain, wear, and tear, start to operate. Going that extra mile may get extremely burdensome and costly. Fourth, f_i can increase logistically, which means convexly for small t_i and concavely for large t_i. Generating marketing effort often takes this form. Initial marketing is expensive with limited impact. As the expense exceeds certain thresholds, impact improves due to cascades and ripple effects. Thereafter impact is substantial due to economy of scale. Fifth, f_i can increase in an incremental step-wise manner. For example, a target may be defended by one type of technology up to a certain level, whereas more extensive defense may require investment in a different type of technology. For example, the employment of highly skilled security personnel trained to run 24-hours surveillance may be needed to handle certain attacks. Sixth, f_i can be subject to budget constraints which for political or other reasons may prevent investment beyond a certain level to defend target i.

Let us consider two examples. First, if the target is involved in production of goods and services such as water and food, communication, transport, finance, governmental functions, and health services, the investment consists in safeguarding the target with human inspection and patrolling, development of procedures, technology investments, surveillance of potential sources of threats, elimination of threats, and deterrence. Second, if the target is part of a cyber security

system, the defender hires security experts, installs firewalls, applies encryption techniques, access control mechanisms, develops intrusion detection systems, and designs the optimal defense for the system.

Let us then consider attacker j where analogous reasoning applies. To attack target i with value V_i^j, the attacker incurs an investment effort $\boldsymbol{T_i^j}$, a vector consisting of capital and labor. Simplifying to the scalar T_i^j, the investment expenditure is $F_i^j = F_i^j(T_i^j)$, measured in dollar terms, where $\partial F_i^j / \partial T_i^j > 0$. If F_i^j is linear, we set $F_i^j = C_i^j T_i^j$, where C_i^j is the inefficiency of the investment for target *i*, analogously to c_i for the defender. Alternatively, F_i^j may be concave ($\partial^2 F_i^j / \partial T_i^{j2} < 0$), convex ($\partial^2 F_i^j / \partial T_i^{j2} > 0$), logistic, a step function, or subject to a budget constraint.

Let us consider the same two examples from the perspective of attacker j. First, if the target is involved in production of goods and services, etc., the attacker's investment is directed towards destruction, distortion, theft, and interfering with production, human inspection and patrolling, avoidance of surveillance, covert action to avoid detection, manipulation of information, and public revelation of system weaknesses. Second, if the target is part of a cyber security system, the attacker seeks to break through the security defense, circumvent the work of the security experts, penetrate the firewalls, decipher the encryption, and bypass the access control mechanisms and intrusion detection systems. A successful attack reduces the reliability of the system through appropriating, getting access to, or confiscating, something of value within or related to the system, or securing information which can be used as means of reducing system reliability.

The cost functions may vary considerably across the targets. A target such as the US Gold Reserve stored at Ft. Knox has high defense inefficiency and even higher attack inefficiency. It is located for optimal defense, and is very hard to attack. Another target such as the U.S. Statue of Liberty has a more vulnerable location which increases the defense inefficiency and decreases the attack inefficiency. A target such as an underground transport system has high defense inefficiency since it is geographically dispersed, and low attack inefficiency. In contrast, a target buried deep within a mountain has low defense inefficiency and high attack inefficiency.

4 Contest success function

Whether a target is operational or not depends on the relative investments by the defender and attackers, which determine the reliability of the target, and thus also the success of defense and success of attack.[8] We define the probability of a successful attack on target i as

$$p_i = p_i(t_i, T_i^1, ..., T_i^m, m_i, r_i), \quad \partial p_i / \partial t_i < 0, \quad \partial p_i / \partial T_i^j > 0 \tag{1}$$

assuming m attackers, where m_i and r_i are parameters. The probability of a successful attack decreases in the defensive investment, and increases in the offensive investment. The successful attack probability equals the unreliability of target i, which equals one minus the reliability, and corresponds to the asset in the conflict literature. There is conflict over unreliability between the defender and the attackers, just as there is conflict over an asset between multiple contenders. The probability p_i can depend on t_i and T_i^j in extremely many different ways. The two most common contest success functions are the ratio and difference forms (Hirshleifer 1989, Skaperdas 1996). The ratio form (Tullock 1980) states that

$$p_i = \frac{(T_i^1)^{m_i} + ... + (T_i^m)^{m_i}}{t_i^{m_i} + (T_i^1)^{m_i} + ... + (T_i^m)^{m_i}} = \frac{\sum_{j=1}^{m} (T_i^j)^{m_i}}{t_i^{m_i} + \sum_{j=1}^{m} (T_i^j)^{m_i}} \tag{2}$$

where m_i is a decisiveness parameter for the contest over target i.[9] At the limit, with infinitely much defensive investment, and finite offensive investment, the target is 100% reliable and p_i=0. The same result follows with finite defensive investment and zero offensive investment. At the other limit, with infinitely much offensive investment, and finite defensive investment, the target is 0% reliable and p_i=1. The same result follows with finite offensive investment and zero defensive investment.

---

[8] Bier et al. (2006:316) define the probability of success of an attack on a component as a function of the investment by the defender to strengthen that component, where the probability of attack on the system is exogenously given.

[9] The decisiveness m_i is a characteristic of the contest. It can be well illustrated by the history of warfare. Low decisiveness occurs for systems that are defendable, predictable, and where the individual components are dispersed, i.e. physically distant or separated by barriers of various kinds. Neither the defender nor the attacker can get a significant upper hand. An example is the time prior to the emergence of cannons and modern fortifications in the fifteenth century. Another example is entrenchment combined with the machine gun, in multiply dispersed locations, in World War I. High decisiveness occurs for systems that are less predictable, easier to attack, and where the individual components are concentrated, i.e. close to each other or not separated by particular barriers. This may cause "winner-take-all" battles and dictatorship by the strongest. Either the defender or the attacker may get the upper hand. The combination of airplanes, tanks, and mechanized infantry in World War II allowed the offense to concentrate firepower more rapidly than the defense, which intensified the effect of force superiority (Hirshleifer 1995:32-33).

Fig. 1 illustrates how, for $T_i^j = T_i$ held fixed for one single attacker, the probability p_i responds to changes in the investment t_i for the defender. The sensitivity of p_i to t_i increases as the decisiveness parameter m_i increases. When $m_i=0$, the investments t_i and T_i have equal impact on the reliability regardless of their size which gives 50% reliability, $p_i=1/2$.[10] $0<m_i<1$ gives a disproportional advantage of investing less than one's opponent. When $m_i=1$, the investments have proportional impact on the reliability. $m_i>1$ gives a disproportional advantage of investing more than one's opponent. This is often realistic in praxis, as evidenced by benefits from economies of scale. Finally, $m_i=\infty$ gives a step function where "winner-takes-all". That is, the defender suffers probability one when t_i is marginally smaller than T_i, and enjoys probability zero when t_i is marginally larger than T_i.

The difference (logit) form contest success function states that

$$p_i = \frac{Exp[r_i T_i^1] + ... + Exp[r_i T_i^m]}{Exp[r_i t_i] + Exp[r_i T_i^1] + ... + Exp[r_i T_i^m]} = \frac{\sum_{j=1}^{m} Exp[r_i T_i^j]}{Exp[r_i t_i] + \sum_{j=1}^{m} Exp[r_i T_i^j]} = \frac{1}{1 + Exp[r_i (t_i - \sum_{j=1}^{m} T_i^j]} \qquad (3)$$

where r_i is a mass effect parameter for target i. The successful attack probability is strictly less than one also when the defender invests zero, $t_i=0$, as illustrated in Fig. 2. If the defender invests zero, it is not always realistic that the defender loses the target when the attackers invest a finite, and possibly arbitrarily small, amount, as the ratio form suggests. With the difference form, some targets may enjoy attack probability less than one even without defense investment. This is possible for targets that are technologically designed in a hardened manner, or when the attackers are less than fully alert and determined. Hirshleifer (1989) provides examples for when the difference form is realistic.[11]

[10] In the conflict literature this is referred to as egalitarian distribution of an asset independent of effort (investment), so that each agent receives 50%. In our context m=0 gives a certain "egalitarianism" between the defender and the attacker in the sense that the defender obtains half as much reliability as he maximally hopes for. We ignore m<0 which corresponds in one sense to altruism and in another sense to punishing individual investments and placing a premium on laziness.

[11] In struggles between nations, one side may surrender rather than resist against an unappeasable opponent, with the expectation of not losing everything, realizing the cost to the victor of locating and extracting all the spoils. Hirshleifer (1989:104) argues that "in a military context we might expect the ratio form of the Contest Success Function to be applicable when clashes take place under close to 'idealized' conditions such as: an undifferentiated battlefield, full information, and unflagging weapons effectiveness. In contrast, the difference form tends to apply

Both the ratio and difference forms assume that if the defender invests infinitely much, while the attackers invest finite amounts, then the successful attack probability equals zero. This is not always realistic, especially for targets that need to be available and accessible in order to be operational. Investing infinitely much to defend an information set within cyber security does not make it 100% secure since it needs to be available and accessible, which makes it vulnerable for attack (Hausken 2006c). A target such as a television station cannot be made 100% secure even with infinite defense investment since employees and others move in and out of the station, and since communication links with the outside world cannot be blocked. The following contest success function accounts for this

$$p_i = a_i \frac{\sum_{j=1}^{m} Exp[r_i T_i^j]}{1+\sum_{j=1}^{m} Exp[r_i T_i^j]} + (1-a_i)\frac{\sum_{j=1}^{m} Exp[r_i T_i^j]}{Exp[r_i t_i]+\sum_{j=1}^{m} Exp[r_i T_i^j]} \quad (4)$$

where $0 \le a_i < 1$. With zero defense investment $t_i = 0$, (3) and (4) are equivalent regardless of a_i. With infinite defense investment $t_i = \infty$, (3) gives $p_i = 0$, while (4) gives a fraction a_i of the probability that occurs with zero investment since the second term vanishes.

5 Systems with targets that are in parallel, in series, interlinked, interdependent, and independent

5.1 Targets in parallel

A parallel system with n targets is operational if at least one target is operational. Examples are two bridges across a river, and two broadcasting stations which can both serve the public if the other is disabled. For the defender, the expected damage for target i is $v_i p_i$, which decreases in t_i, and the investment expenditure is f_i, which increases in t_i. On the one hand, the contest success function p_i for target i can be conceived as deterministic if determined by deterministic effort levels by the defender and attacker. This causes the damage to be actual damage. On the other hand, p_i can be conceived as a probability and the damage as expected damage. The damage or expected damage if the entire system of n parallel targets is disabled is v, which occurs with probability $p_1 p_2 \cdots p_n$. In accordance with Bier et al. (2005), the expected damage d and utility u for the defender is

---

where there are sanctuaries and refuges, where information is imperfect, and where the victorious player is subject to fatigue and distraction."

$$d = \sum_{i=1}^{n} v_i p_i + v \prod_{i=1}^{n} p_i, \quad u = -\left(\sum_{i=1}^{n} v_i p_i + v \prod_{i=1}^{n} p_i \right) - \sum_{i=1}^{n} f_i \tag{5}$$

The defender maximizes the utility. The first order condition for target i is $\partial u / \partial t_i$=0, which gives n first order conditions to determine the n investments $t_1, t_2, \ldots, t_n$. The reasoning for attacker j, j=1,…,m, is analogous, but the valuations for target i and the system are V_i^j and V^j, respectively. The expected damage D^j and utility U^j for attacker j is

$$D^j = \sum_{i=1}^{n} V_i^j p_i + V^j \prod_{i=1}^{n} p_i, \quad U^j = \sum_{i=1}^{n} V_i^j p_i + V^j \prod_{i=1}^{n} p_i - \sum_{i=1}^{n} F_i^j \tag{6}$$

Attacker j maximizes the utility. The first order condition for target i is $\partial U^j / \partial T_i^j$=0, which gives n first order conditions to determine the n investments $T_1^j, T_2^j, \ldots, T_n^j$, which gives *nm* first order conditions for the m attackers. The value v_i may well differ substantially from V_i^j, which may again differ substantially across the m attackers. Analogously, v may differ from V^j, which may differ across the attackers. The optimization program in (5) and (6) is coupled or linked through the probability p_i of a successful attack on target i, which depends on the investments t_i and T_i^j, i=1,…,n, j=1,…,m as specified in section 4. This gives n(m+1) first order conditions when there are no constraints on the investments.

5.2 Targets in series

A series system with n targets is operational if all targets are operational. Examples are electricity transmission lines, oil/gas pipelines, and security procedures for valuable transport which can be violated at a variety of locations. As argued by Bier et al. (2005, 2006), the defender's focus should be on the highest value across the n targets, as evaluated by the attacker. If the defender were to equalize losses across targets according to his own perspective, he might waste money defending targets that the attacker has limited interest in. The defender's objective function equalizes the attacker's valuations because it is the most cost-effective way to achieve his own goals. Making all targets equally desirable to the attacker is thus the correct strategy. The intuition is the same in mixed equilibrium strategy calculations in game theory where one player randomizes to make the other player indifferent in his randomizing. A target may have a high $(V^j + V_i^j)p_i$ because it is highly valuable to attacker j (high $V^j + V_i^j$), or because the attack probability p_i for that target is high. Investing to defend another target makes no

difference unless target i has been sufficiently well defended through reducing p_i. In other words, the defender should adjust $t_1, t_2, \ldots, t_n$ to make the expected damage from an attack on each target equal to each other, as assessed by the attacker. With m attackers, the defender identifies for each target which attacker has the highest $(V^j + V_i^j)p_i$. Once these highest n values have been determined, the defender invests to make these values equal to each other. This does not mean that each target is made equally desirable for each attacker. Instead, it means that the defender invests so that the attacker most interested in a given target places the same value on this target as any of the m attackers most interested in any other target places on this other target. This gives the defender's expected damage and utility[12]

$$d = \max_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} [(V^j + V_i^j)p_i], \quad u = -\max_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} [(V^j + V_i^j)p_i] - \sum_{i=1}^{n} f_i \tag{7}$$

The expected damage and utility for attacker j is

$$D^j = \max_{i=1,\ldots,n} [(V^j + V_i^j)p_i], \quad U^j = \max_{i=1,\ldots,n} [(V^j + V_i^j)p_i] - \sum_{i=1}^{n} F_i^j \tag{8}$$

5.3 Interlinked targets

Some targets are interlinked in manners that are neither fully in parallel nor fully in series. Consider a military force consisting of three targets which are an army, a navy, and an air force. If the army is 100% eliminated through a successful attack, the military force becomes less operational, but not non-operational. The capacity for ground maneuvers is reduced, which can be partly compensated for by more heavy bombardment and employment of helicopters by the air force, or retraining of the navy to carry out army operations. If the military force had been a fully parallel system, eliminating the army would not reduce the operability of the military force. Conversely, if the military force had been a fully series system, eliminating the army would eliminate the operability. Various sufficiently complex combinations of serial and parallel links do not seem to describe the example. For example, consider three serial components, where each component is a parallel system with an army, a navy, and an air force. If the army is eliminated, the military force still operates as effectively as before. The difference is that each component then has two instead of three parallel links, which reduces the reliability.

[12] For the parallel system in section 5.1, one alternative is to let the attacker equalize the vulnerabilities of the targets as perceived by the defender, applying some sort of duality theorem. However, if the attacker has limited interest in how much the defender has to pay for defense, which is often realistic in practice, then that alternative may not be too useful.

One tentative step toward handling such systems is to define the object function for the defender as a weighted sum of the damage for parallel and series systems, i.e.

$$u = -\left(a\left[\sum_{i=1}^{n} v_i p_i + v\prod_{i=1}^{n} p_i \right] + (1-a)\left[\max_{\substack{i=1,\ldots,n \\ j=1,\ldots,m}} [(V^j + V_i^j)p_i] \right] \right) - \sum_{i=1}^{n} f_i \tag{9}$$

where $0 \le a \le 1$. The system is a parallel system when a=1, a series system when a=0, and otherwise a hybrid interlinked system. This not a real physical system, but may be an empirical approximation. Equation (9) is reminiscent of functions used in production and consumption theories. There are multiple inputs, and tradeoffs are made between these to maximize production or consumption. One example is the Cobb-Douglas function $y = x_1^{\alpha} x_2^{1-\alpha}$, where x_1 and x_2 are inputs, and $0<\alpha<1$. This would have been a series system if $\alpha = 1/2$, but $\alpha \neq 1/2$ gives unequal weight to the two inputs. If x_1 is steak and x_2 is potatoes, measured in weight, α allows giving different weights to steak and potatoes in one's design of the optimal dinner. Adapting the Cobb-Douglas function to our analysis, one possibility is

$$u = -\left((v_1 p_1)^{\alpha} (v_2 p_2)^{1-\alpha} + v p_1 p_2 \right) - \sum_{i=1}^{n} f_i \tag{10}$$

Another possibility is

$$d = -\left(((v+v_1)p_1)^{\alpha} ((v+v_2)p_2)^{1-\alpha} \right) - \sum_{i=1}^{n} f_i \tag{11}$$

Another function used in production and consumption theories is the constant elasticity of substitution (CES) function $y = [\lambda x_1^{\beta} + (1-\lambda)x_2^{\beta}]^{1/\beta}$, where $0<\lambda<1$, $\beta = (\gamma - 1)/\gamma$, and γ is the elasticity of substitution. This function is never a 100% series system since y does not equal zero if one of the inputs x_1 or x_2 is zero. However, neither is the system a 100% parallel system since reducing either x_1 or x_2 reduces y. Adapting the constant elasticity of substitution function to our analysis, three possibilities are

$$u = -\left(\sum_{i=1}^{n} \lambda_i (v_i p_i)^{\beta} + v\prod_{i=1}^{n} p_i \right)^{1/\beta} - \sum_{i=1}^{n} f_i, \quad \lambda_n = 1 - \sum_{i=1}^{n-1} \lambda_i \tag{12}$$

$$u = -\left(\left(\sum_{i=1}^{n} \lambda_i (v_i p_i)^{\beta} \right)^{1/\beta} + v\prod_{i=1}^{n} p_i \right) - \sum_{i=1}^{n} f_i, \quad \lambda_n = 1 - \sum_{i=1}^{n-1} \lambda_i \tag{13}$$

$$u = -\left(\sum_{i=1}^{n} \lambda_i ((v+v_i)p_i)^{\beta} \right)^{1/\beta} - \sum_{i=1}^{n} f_i, \quad \lambda_n = 1 - \sum_{i=1}^{n-1} \lambda_i \tag{14}$$

Analogously to (9), the expected utility for attacker j is

$$U^j = a\left[\sum_{i=1}^{n} V_i^j p_i + V^j \prod_{i=1}^{n} p_i\right] + (1-a)\left[\max_{i=1,\ldots,n}[(v+v_i)p_i]\right] - \sum_{i=1}^{n} F_i^j \quad (15)$$

which attacker j seeks to maximize. Analogs to (10)-(14) are straightforward to set up for attacker j.

5.4 Interdependent targets

Interdependent systems are systems where the defense of one target benefits all targets, and where the attack on one target usually also impacts other targets. Examples occur within the airline industry, computer networks, fire protection, theft protection, bankruptcy protection, vaccinations. Such systems have been analyzed by Kunreuther and Heal (2003). Bier and Gupta (2006) explore the effects of heterogeneous discount rates on the optimal defensive strategy in such systems. Hausken (2006a) finds that with increasing interdependence, each defending agent free rides by investing less, suffers lower profit, while the attacker enjoys higher profit. Kunreuther and Heal (2003:232) illustrate

> "by reference to an airline that is determining whether to install a baggage checking system voluntarily. In making this decision it needs to balance the cost of installing and operating such a system with the reduction in the risk of an explosion from a piece of luggage not only from the passengers who check in with it, but also from the bags of passengers who check in on other airlines and then transfer to it."

Each airline prefers all airlines to install baggage checking systems, but there is a free-rider dilemma. For cyber security, Hausken (2006a) states that

> "When firms are interconnected on a common platform or network such as in a supply chain where upstream suppliers are connected via Electronic Data Interchanges (EDI) to downstream manufacturers or retailers (which is an example of interdependent security), a security vulnerability in either the upstream or downstream firm can also impact the other firms. Consider the following scenario. Firm j is breached by a group of hackers and since firm i is connected to firm j through a common network (e.g. a virtual private network) it is also susceptible to a breach through the network. Now if firm i has invested in the best anti-intrusion technologies (for simplicity let us imagine installation of the most expensive firewalls at the edges - routers and switches), it is less likely to be hacked. Thus, the probability that firm i gets breached because its security risks are interdependent with firm j is likely to be dependent on the security investments made by both itself and the rival firm. Further the extent of the indirect attack would also depend on how closely connected the two firms are."

The expected damage and utility for the defender of a system of n interdependent targets are

$$d = \sum_{i=1}^{n} v_i p_i, \quad u = -\sum_{i=1}^{n} (v_i p_i + f_i) \quad (16)$$

The expected damage and utility for attacker j are

$$D^j = \sum_{i=1}^{n} V_i^j p_i, \quad U^j = \sum_{i=1}^{n} (V_i^j p_i - F_i^j) \tag{17}$$

To account for the interdependence, the probability p_i of a successful attack on target i has to be generalized beyond that of section 4. The ratio form in (2) generalizes to

$$p_i = \frac{\sum_{k=1}^{n} \alpha_{ik} \sum_{j=1}^{m} (T_k^j)^{m_k}}{\sum_{k=1}^{n} \alpha_{ik} \left(t_k^{m_k} + \sum_{j=1}^{m} (T_k^j)^{m_k} \right)}, \ \alpha_{ik} = 1 \ \ when \ \ i = k, \ 0 \le \alpha_{ik} \le 1 \ \ when \ \ i \ne k, \ \alpha_{ik} = \alpha_{ki} \tag{18}$$

where α_{ik} expresses the interdependence between target i and target k. Since α_{ik}=1 when i=k, the defender's defense $t_k^{m_k}$ and attacker j's defense $(T_k^j)^{m_k}$ have full impact for target i. Consider target k, where k ≠ i, and assume that α_{ik} is a number between zero and one. Because of the interdependence, attacker j's attack $(T_k^j)^{m_k}$ on target k gets transferred further, with weight α_{ik}, to an attack on target i. Analogously, the defender's defense $t_k^{m_k}$ of target k counteracts the attack on target k, and counteracts with weight α_{ik} the extent to which that attack gets transferred further to target i.

Analogously, the difference form in (3) generalizes to

$$p_i = \frac{\sum_{k=1}^{n} \alpha_{ik} \sum_{j=1}^{m} Exp[r_k T_k^j]}{\sum_{k=1}^{n} \alpha_{ik} \left(Exp[r_k t_k] + \sum_{j=1}^{m} Exp[r_k T_k^j] \right)}, \ \alpha_{ik} = 1 \ when \ i = k, \ 0 \le \alpha_{ik} \le 1 \ when \ i \ne k, \ \alpha_{ik} = \alpha_{ki} \tag{19}$$

Without interdependence, (18) and (19) simplifies to (2) and (3), respectively, when α_{ik}=0 for all $i \ne k$.

5.5 Independent targets

Independent targets have no connection with other targets. Examples are geographically remote targets which are self-sufficient with no external impact, or a country's interests of various kinds abroad. Independent targets are less common in today's interconnected and complex world, but they are theoretically possible, and targets which are almost independent may be approximated with independent targets. The expected damage and utility for the defender is

$$d = \sum_{i=1}^{n} v_i p_i, \quad u = -\sum_{i=1}^{n} (v_i p_i + f_i) \tag{20}$$

The expected damage and utility for attacker j is

$$D^j = \sum_{i=1}^{n} V_i^j p_i, \quad U^j = \sum_{i=1}^{n} (V_i^j p_i - F_i^j) \tag{21}$$

5.6 Multi-use systems[13]

Examples of "multi-use" systems are various transportation systems, consumption systems, or the Internet. Two links may be perceived as being in series for someone trying to go from one point to another, but in parallel for someone trying to go through one of the points to a third point. In consumption, two components may be perceived as strategic complements by some consumers, and strategic substitutes for other consumers. That is, one consumer may require both of two components in order to function (series system), while another consumer may function based on any one of the components in sufficient abundance (parallel system). Assume N users and assign weight w_i to user i, where $w_1+w_2+...+w_N=1$. If user i, i=1,…,M perceives a series system of two components A and B, the system is defended for user i as if it is a series system. Assume that this gives the optimal defense t_{sA} for component A and t_{sB} for component B. If user j, j=M+1,…,N perceives a parallel system of the two components A and B, the system is defended for user j as if it is a parallel system. Assume that this gives the optimal defense t_{pA} for component A and t_{pB} for component B. The two components then get defenses

$$t_A = Mt_{sA} \sum_{i=1}^{M} w_i + (N-M) t_{pA} \sum_{i=M+1}^{N} w_i, \quad t_B = Mt_{sB} \sum_{i=1}^{M} w_i + (N-M) t_{pB} \sum_{i=M+1}^{N} w_i \tag{zz}$$

which may be rephrased as the weighted sum in (9).

6 The optimization program for static and repeated games, with and without budget constraints, and with complete and incomplete information

A benchmark solution for the optimization program arises from letting the defender and m attackers choose their investments simultaneously and independently. The defender calculates $\partial u / \partial t_i = 0$ for the n targets to determine $t_1, t_2, \ldots, t_n$, and attacker j calculates $\partial U^j / \partial T_i^j = 0$ for the n targets to determine $T_1^j, T_2^j, \ldots, T_n^j$. This gives n(m+1) first order conditions for the global optimum when it corresponds to a local optimum. If corner solutions emerge, the equations for

[13] I thank Vicky Bier for suggesting multi-use systems.

these are determined. The n(m+1) equations are conveniently solved applying conventional software on a computer.

The defender is particularly interested in how these optimal benchmark investments $t_1, t_2, \ldots, t_n$ vary across the n targets, the relative size of each, the sum $\sum_{i=1}^{n} t_i$ of the investments, and how each investment t_i gets deployed into an actual defense investment from the realization that each investment is more generally a vector $\boldsymbol{t_i}$ as discussed in section 3. The defender and attackers can be assumed to be risk neutral, or the expected utilities u and U^j can be adjusted to account for risk averse or risk seeking attitudes.[14]

The m attackers can realistically be thought of as operating independently, or some of them can be merged so that the remaining can be conceived as independent. The m attackers rarely or never attack simultaneously, but assuming simultaneous attacks allows conceptualizing the total volume of attacks, and how this volume gets distributed across the n targets. Some of the m attackers may be more likely to attack than others. It is thus of interest to determine the impact if a subset of the m attackers or one attacker were to attack. One alternative to the benchmark solution is to solve the n first order conditions for the defender together with the n first order conditions for just one of the attackers, attacker j. This gives 2n first order conditions. Solving the equations gives different investments $t_1, t_2, \ldots, t_n$, generally different relative size for each investment, and a different sum $\sum_{i=1}^{n} t_i$. Solving the 2n first order conditions for each of the m attackers gives further investments, relative sizes, and sums that can be assessed. More generally, solving the n(k+1) first order conditions for any combination of k attackers, k=1,…,m, gives a variety of results. Analyzing these results together with assessments of how likely each of the m attackers are to attack, gives more fertile ground from which to assess the optimal benchmark investments $t_1, t_2, \ldots, t_n$.

The defender and attackers may be subject to constraints of various kinds. Examples are a total budget constraint, or a constraint for each target for economic or other reasons. Parts of an agent's budget may be "frozen", as is the case for some terrorist organizations. If the defender

[14] Much of the economic conflict literature related to production, appropriation, defense, and rent seeking assumes risk neutrality. See Skaperdas (1991) for an exception.

and m attackers all have a total budget constraint, there are (n-1)(m+1) first order conditions for the benchmark solution. If some have budget constraints and others do not, the number of first order conditions is between (n-1)(m+1) and n(m+1).

Complex infrastructures and systems of targets are usually built up over time reaching values assessed in section 2 for target i as $v_i = e_i + h_i + s_i$ for the defender and $V_i^j = E_i^j + H_i^j + S_i^j$ for attacker j. Defenses for each of these targets are usually also built up over time in association with the values of the targets, subject to various budgets, allocation procedures, political processes, precedent, historical inertia, and other influences. Hence an alternative to the benchmark static game is a two period game where the defender invests in the first period and the attackers invest simultaneously in the second period. The game is solved with backward recursion. The second period is solved first, which means calculating $\partial U^j / \partial T_i^j = 0$ and solving the nm first order conditions for the m attackers to determine $T_1^j, T_2^j, \ldots, T_n^j$, j=1,…,m, conditional on $t_1, t_2, \ldots, t_n$ having been determined in the first period. This means that the T_i^j's are determined as functions of the t_i's. Thereafter the first period is solved, inserting these T_i^j's into *u* for the defender. $\partial u / \partial t_i = 0$ is calculated and the m first order conditions are solved which gives the optimal $t_1, t_2, \ldots, t_n$ for the defender in equilibrium. Finally the t_i's are inserted into the T_i^j's to determine the equilibrium solution for the m attackers.

Examples of more complex repeated or dynamic games are as follows. First, the defender and attackers may invest simultaneously and independently in a finitely repeated or infinitely repeated game where each agent has a different discount parameter. Common equilibrium concepts for repeated games are sequential equilibrium (Kreps and Wilson 1982) and trembling-hand perfect equilibrium (Selten 1975). Second, the defender and attackers may invest alternately in successive time periods. Third, the defender and subsets of attackers may invest in prescribed manners in successive time periods. Fourth, each agent may invest in one target or subset k of targets, k=1,…,n, in successive periods, in prescribed manners for the defender and attackers. Fifth, each agent may split his investment in target i into arbitrarily many sub-investments to be deployed in successive periods, either in prescribed manners, or dependent on how the game evolves according to an updating mechanism. Sixth, in a dynamic game with

continuous time, each agent may invest or subinvest in any target at any point in time dependent on how the game evolves.

Defending and attacking infrastructures often involves assessing incomplete information (Dixit and Skeath 1999; Fudenberg and Tirole 1991; Rasmusen 2001). Incomplete information can be symmetric or asymmetric across players, e.g., one-sided, two-sided, or (m+1)-sided. Prominent candidates for incomplete information are the defender's valuations v_i, e_i, h_i, s_i, and the attackers' valuations $V_i^j, E_i^j, H_i^j, S_i^j$, of the total, economic, human, and symbolic values of target i, and the values v and V^j of system operability for the defender and attackers. Parameters in the investment expenditure functions f_i and F_i^j for the defender and attackers can also be incompletely known. For repeated games the agents' discount parameters can be incompletely known. The common method to model incomplete information is to apply the Harsanyi doctrine (Harsanyi 1967/68). Each player knows his own characteristics, but forms a subjective probability distribution over the alternative possibilities, or types, of incomplete information for the other players.[15] A player's type is his characteristics of psychological, physical, or other nature. Incomplete information can be introduced for static games, or repeated or dynamic games. For games where time plays a role, incomplete information can be updated successively, using for example Bayesian updating, as more information gets compiled by each player about the strategies chosen by all players as the game evolves.

Most defenders have to handle attackers that differ greatly in objectives, skills, methods of operation, and degrees of sanity. Examples are thieves, Islamic terrorists, disgruntled ex-employees, technological breakdowns, natural disasters. Assuming multiple attackers may imply that a particular level of defense may deter some attackers, but not others. This means that from the defender's point of view, the likelihood of a successful attack may be a non-convex function of the defensive investment, even if to each individual attacker, the likelihood of success is convex in the level of defensive investment. The problem likely has many local optima.

An alternative to the deterministic optimization program described here is stochastic optimization. Assume that the defender faces uncertainty about which type of attacker she faces, uncertainty about how strongly or where the attacker chooses to attack, or uncertainty about

[15] This superseded earlier infinite recursions of the kind "If I think that you think that I think ...."

when each type of attacker chooses to act. The defender may then prefer to choose a defensive strategy that is "robust" in the face of this uncertainty about the nature of the threat.

7 An example

Many empirical challenges are involved in determining the makeup of an infrastructure. Assume that thorough analysis has given the system in Fig. 3. To determine the expected damage and utility for the defender, let us start with the parallel and series system. Using (5), the parallel targets 2 and 3 have an expected damage

$$d_{23} = v_2 p_2 + v_3 p_3 + v_{23} p_2 p_3 \tag{22}$$

where subscript "23" refers to targets 2 and 3, so that v_{23} is the damage if both targets 2 and 3 are disabled. Joining in target 1, which is in series with 2 and 3 in parallel, and using (7), the expected damage of targets 1,2,3 is

$$d_{123} = \max[(V_{123} + V_1) p_1, D_{23}] \tag{23}$$

where subscript "123" refers to targets 1,2,3, and where D_{23} is determined below. Joining in target 4 in parallel, using (5), gives the expected damage

$$d_{1234} = d_{123} + v_4 p_4 + v_{1234} p_4 p_1 [1 - (1 - p_2)(1 - p_3)] \tag{24}$$

where $p_1[1 - (1 - p_2)(1 - p_3)]$ is the probability of a successful attack on targets 1,2,3. Joining in target 5 in series, and using (7), the expected damage of targets 1-5 is

$$d_{12345} = \max[(V_{12345} + V_5) p_5, D_{1234}] \tag{25}$$

where D_{1234} is determined below. Targets 6 and 7 are interlinked. Using (9), the expected damage to the defender is

$$d_{67} = a\left[v_6 p_6 + v_7 p_7 + v_{67} p_6 p_7\right] + (1 - a)\left[\max[(V_{67} + V_6) p_6, (V_{67} + V_7) p_7]\right] \tag{26}$$

For targets 1-7 and 11 the contest success functions in section 4 determine the probability p_i of a successful attack on target i. Assume one attacker so that m=1, and suppress the superscript j in the attacker notation. Using (2) and (3) for targets 1-7 and 11, the success probability is

$$p_i^r = \frac{T_i^{m_i}}{t_i^{m_i} + T_i^{m_i}}, \quad p_i^d = \frac{Exp[r_i T_i]}{Exp[r_i t_i] + Exp[r_i T_i]}, \quad i = 1,...,7,11 \tag{27}$$

where superscripts r and d on p_i refer to the ratio form and difference form, respectively.

Targets 8,9,10 are interdependent. Using (16), the expected damage for the defender is

$$d_{89,10} = v_8 p_8 + v_9 p_9 + v_{10} p_{10} \tag{28}$$

where the comma in the subscript is used to distinguish "10" from "8" and "9". To determine the probability p_i accounting for the interdependence, the ratio form in (18) gives

$$\begin{aligned} p_8^r &= \frac{T_8^{m8} + \alpha_{89} T_9^{m9} + \alpha_{8,10} T_{10}^{m10}}{t_8^{m8} + T_8^{m8} + \alpha_{89}(t_9^{m9} + T_9^{m9}) + \alpha_{8,10}(t_{10}^{m10} + T_{10}^{m10})}, \\ p_9^r &= \frac{\alpha_{98} T_8^{m8} + T_9^{m9} + \alpha_{9,10} T_{10}^{m10}}{\alpha_{98}(t_8^{m8} + T_8^{m8}) + t_9^{m9} + T_9^{m9} + \alpha_{9,10}(t_{10}^{m10} + T_{10}^{m10})}, \\ p_{10}^r &= \frac{\alpha_{10,8} T_8^{m8} + \alpha_{10,9} T_9^{m9} + T_{10}^{m10}}{\alpha_{10,8}(t_8^{m8} + T_8^{m8}) + \alpha_{10,9}(t_9^{m9} + T_9^{m9}) + t_{10}^{m10} + T_{10}^{m10}} \end{aligned} \tag{29}$$

and the difference form in (19) gives

$$\begin{aligned} p_8^d &= \frac{Exp[r_8 T_8] + \alpha_{89} Exp[r_9 T_9] + \alpha_{8,10} Exp[r_{10} T_{10}]}{Exp[r_8 t_8] + Exp[r_8 T_8] + \alpha_{89}(Exp[r_9 t_9] + Exp[r_9 T_9]) + \alpha_{8,10}(Exp[r_9 t_9] + Exp[r_9 T_9])}, \\ p_9^d &= \frac{\alpha_{98} Exp[r_8 T_8] + Exp[r_9 T_9] + \alpha_{9,10} Exp[r_{10} T_{10}]}{\alpha_{98}(Exp[r_8 t_8] + Exp[r_8 T_8]) + Exp[r_9 t_9] + Exp[r_9 T_9] + \alpha_{9,10}(Exp[r_9 t_9] + Exp[r_9 T_9])}, \\ p_{10}^d &= \frac{\alpha_{10,8} Exp[r_8 T_8] + \alpha_{10,9} Exp[r_9 T_9] + Exp[r_{10} T_{10}]}{\alpha_{10,8}(Exp[r_8 t_8] + Exp[r_8 T_8]) + \alpha_{10,9}(Exp[r_9 t_9] + Exp[r_9 T_9]) + Exp[r_9 t_9] + Exp[r_9 T_9]} \end{aligned} \tag{30}$$

Target 11 is independent. Using (20), the expected damage for the defender is

$$d_{11} = v_{11} p_{11} \tag{31}$$

Summing up across the 11 targets gives the defender's expected damage and utility

$$d = d_{12345} + d_{67} + d_{89,10} + d_{11}, \quad u = -d - \sum_{i=1}^{11} f_i \tag{32}$$

Proceeding to the attacker, the analogous equations are

$$D_{23} = V_2 p_2 + V_3 p_3 + V_{23} p_2 p_3 \tag{33}$$

$$D_{123} = \max[(V_{123} + V_1) p_1, D_{23}] \tag{34}$$

$$D_{1234} = D_{123} + V_4 p_4 + V_{1234} p_4 p_1 [1 - (1 - p_2)(1 - p_3)] \tag{35}$$

$$D_{12345} = \max[(V_{12345} + V_5) p_5, D_{1234}] \tag{36}$$

$$D_{67} = a\left[V_6 p_6 + V_7 p_7 + V_{67} p_6 p_7\right] + (1 - a)\left[\max[(V_{67} + V_6) p_6, (V_{67} + V_7) p_7]\right] \tag{37}$$

$$D_{89,10} = V_8 p_8 + V_9 p_9 + V_{10} p_{10} \tag{38}$$

$$D_{11} = V_{11} p_{11} \tag{39}$$

$$D = D_{12345} + D_{67} + D_{89,10} + D_{11}, \quad U = D - \sum_{i=1}^{11} F_i \tag{40}$$

8 Conclusion

The article provides a framework for how to analyze the strategic defense of an infrastructure attacked by multiple fully strategic attackers. Each agent on the defensive and offensive side faces an optimization program that is specified. The strategic decision for each agent is how much to invest in defending versus attacking each target within the infrastructure, how to allocate investments across targets, and what kinds of investments are suitable. Operations research, reliability theory, and game theory are merged for optimal analytical impact.

A target can have economic, human, and symbolic values. These values are discussed and exemplified, and are generally different for the defender and attackers. Thereafter investment expenditure functions are considered. These can be linear in the investment effort for each agent, concave, convex, logistic, can increase in an incremental step-wise manner, or can be subject to budget constraints. To determine the probability of a successful attack on a target, contest success functions are introduced which depend on the relative investments of the defender and attackers on each target, and on characteristics of the contest over each target such as its decisiveness and whether there is a mass effect for investments. Examples of such functions are the ratio and difference forms.

Targets can be in parallel, in series, interlinked, interdependent, independent, or multi-use. Interlinked targets are neither fully in parallel nor fully in series, exemplified with a military force consisting of an army, a navy, and an air force. For interdependent systems the defense of one target benefits all targets, and the attack on one target usually impacts other targets. Examples are within the airline industry, and computer networks. Independent targets are not connected with other targets, for example because of geographical remoteness or self-sufficiency. Multi-use systems are viewed differently by different agents.

The optimization program for the defender and each of multiple attackers is specified. The defender seeks to minimize the expected damage accounting for his valuation of targets, and minimize defense costs. Each attacker seeks to maximize the expected damage accounting for a possibly different valuation of targets, and minimize costs of attack. The number of first order conditions for the benchmark case equals the number of agents times the number of targets. These are conveniently solved applying conventional software on a computer, and give the

optimal investments for each agent for each target. Each agent is interested in how the investments vary across the targets, the relative size of each, and the sum of the investments. Alternative optimization programs assuming one defender and one or a subset of attackers are convenient to analyze the impact on the distribution of investments. If all agents have a budget constraint, the number of first order conditions equals the number of agents times the number of targets minus one.

Infrastructures are built over time. A two period game that is often realistic is to assume that the defender chooses investments in the first period, while the attackers choose investments in the second period. Such games are solved with backward recursion. The game may be repeated finitely or infinitely many times, with alternating investments for agents or groups of agents, and with different discount parameters for each agent. More generally, each agent may invest or subinvest in any target at any point in time dependent on how the game evolves.

Defending and attacking infrastructures often involves assessing incomplete information, which may be symmetric or asymmetric across players. Examples of incomplete information are the agents' valuations of the targets, parameters in the investment expenditure functions, or the agents' discount parameters for repeated games. Finally an example of a system with 11 targets is analyzed.

References

Azaiez, N., Bier, V.M., 2006. Optimal Resource Allocation for Security in Reliability Systems. European Journal of Operational Research, Forthcoming.

Beitel, G.A., Gertman, D.I. and Plum, M.M. (2004), "Balanced Scorecard Method for Predicting the Probability of a Terrorist Attack," Idaho National Engineering and Environmental Laboratory, Idaho Falls, Idaho, USA.

Bier, V.M., 1995. Perfect Aggregation for a Class of General Reliability Models with Bayesian Updating. Applied Mathematics and Computation 73, 281-302.

Bier, V.M., 2004. Game-theoretic and Reliability Methods in Counter-Terrorism and Security. In Mathematical and Statistical Methods in Reliability (Wilson et al., editors), Series on Quality, Reliability and Engineering Statistics, World Scientific, Singapore, 2005, pages 17-28.

Bier, V.M., Gupta, A., 2006. Myopic Agents and Interdependent Security Risks: A Comment on 'Interdependent Security' by Kunreuther and Heal. Ms.

Bier, V.M., Abhichandani, V., 2002. Optimal Allocation of Resources for Defense of Simple Series and Parallel Systems from Determined Adversaries. Proceedings of the Engineering Foundation Conference on Risk-Based Decision Making in Water Resources X, Santa Barbara, CA: American Society of Civil Engineers.

Bier, V.M., Nagaraj, A., Abhichandani, V., 2005. Protection of Simple Series and Parallel Systems with Components of Different Values. Reliability Engineering and System Safety 87, 315-323.

Bier, V.M., Oliveros, S., Samuelson, L., 2006. Choosing What to Protect: Strategic Defense Allocation Against an Unknown Attacker. Journal of Public Economic Theory, Forthcoming.

Dixit, A. and Skeath, S. 1999. Games of Strategy, Norton, New York.

Enders, W., Sandler, T., 2003. What do we know about the substitution effect in transnational terrorism?. in A. Silke and G. Ilardi (eds) Researching Terrorism: Trends, Achievements, Failures (Frank Cass, Ilfords, UK), http://www-rcf.usc.edu/~tsandler/substitution2ms.pdf.

Fudenberg. D. M. and Tirole, J. 1991. Game Theory, MIT Press, Cambridge.

Gal-Or, E., Ghose, A., 2005. The economic incentives for sharing security information. Information Systems Research 16 (2), 186-208.

Gordon, L.A., Loeb, M., 2002. The economics of information security investment. ACM Transactions on Information and System Security 5 (4), 438-457.

Gordon, L.A., Loeb, M., Lucyshyn, W., 2003. Sharing information on computer systems security: An economic analysis. Journal of Accounting and Public Policy 22 (6), 461-485.

Harsanyi, J. 1967/68. Games with Incomplete Information Played by 'Bayesian Players', I-III Management Science 14, 159-183, 320-334, 486-501.

Hausken, K., 2002. Probabilistic risk analysis and game theory. Risk Analysis 22 (1), 17-27.

Hausken, K., 2005. Production and conflict models versus rent seeking models. Public Choice 123, 59-93.

Hausken, K., 2006a. Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. Journal of Accounting and Public Policy, Forthcoming.

Hausken, K., 2006b. Strategic Defense and Attack for Series and Parallel Reliability Systems, Ms.

Hausken, K. 2006c. Returns to Information Security Investment: The Effect of Alternative Information Security Breach Functions on Optimal Investment and Sensitivity to Vulnerability. Information Systems Frontiers, Forthcoming, Volume 8, Number 5.

Hirshleifer, J., 1989. Conflict and rent-seeking success functions: Ratio vs. difference models of relative success. Public Choice 63, 101-112.

Hirshleifer, J. 1995. Anarchy and Its Breakdown. Journal of Political Economy 103, 1, 26-52.

Kreps, D. M. and Wilson, R. 1982. Sequential Equilibria. Econometrica 50, 863-894.

Kunreuther, H., Heal, G., 2003. Interdependent security. The Journal of Risk and Uncertainty 26, 2/3, 231-249.

Levitin, G., 2002. Maximizing survivability of acyclic transmission networks with multi-state retransmitters and vulnerable nodes, Reliability Engineering and System Safety 77 189-199.

Levitin, G., 2003a. Optimal multilevel protection in series-parallel systems, Reliability Engineering and System Safety 81, 93-102.

Levitin, G., 2003b. Optimal allocation of multi-state elements in linear consecutively connected systems with vulnerable nodes, European Journal of Operational Research 150, 406-419.

Levitin, G., Lisnianski, A., 2000. Survivability maximization for vulnerable multi-state systems with bridge topology, Reliability Engineering and System Safety 70, 125-140.

Levitin, G., Lisnianski, A., 2001. Optimal separation of elements in vulnerable multi-state systems, Reliability Engineering and System Safety 73, 55-66.

Levitin, G., Lisnianski, A., 2003. Optimizing survivability of vulnerable series-parallel multi-state systems, Reliability Engineering and System Safety 79, 319-331.

Levitin, G., Dai, Y., Xie, M., Poh, K.L., 2003. Optimizing survivability of multi-state systems with multi-level protection by multi-processor genetic algorithm, Reliability Engineering and System Safety 82, 93-104.

Major, J., 2002. Advanced techniques for modeling terrorism risk, Journal of Risk Finance 4 (1) 15-24.

O'Hanlon, M., Orszag, P., Daalder, I., Destler, M., Gunter, D., Litan, R., Steinberg, J., 2002. Protecting the American Homeland, Brookings Institution, Washington, DC.

Rasmusen. E. 2001. Games and Information, Basil Blackwell, Inc., Cambridge.

Selten, R. 1975. Reexamination of the Perfectness Concept for Equilibrium Points in Extensive Games. International Journal of Game Theory 4, 25-55.

Skaperdas, S., 1991. Conflict and attitudes toward risk. American Economic Review 81, 116-120.

Skaperdas, S., 1996. Contest success functions. Economic Theory 7, 283-290.

Tullock, G. 1980. Efficient Rent-Seeking. in Buchanan, J.M., Tollison, R.D., and Tullock, G., Toward a Theory of the Rent-Seeking Society, Texas A. & M. University Press, College Station, 97-112.

Viscusi, W. K. 2005. The Value of Life. New Palgrave Dictionary of Economics and the Law, 2nd Edition. SSRN: http://ssrn.com/abstract=827205.

Woo, G., 2002. Quantitative terrorism risk assessment, Journal of Risk Finance 4 (1) 7-14.

Woo, G., 2003. Insuring against Al-Qaeda, Insurance Project Workshop, National Bureau of Economic Research, Inc. (Downloadable from website http://www.nber.org/~confer/2003/insurance03/woo.pdf).

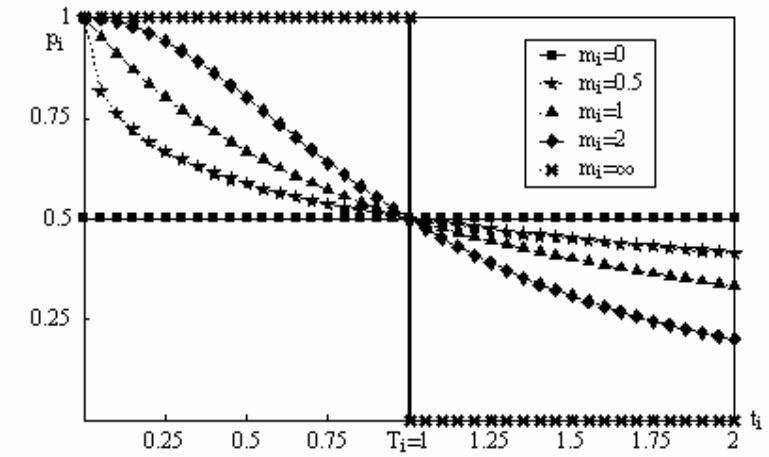

Fig. 1. Ratio form: Successful attack probability p_i as a function of the investment t_i for various m_i when $T_i = 1$.

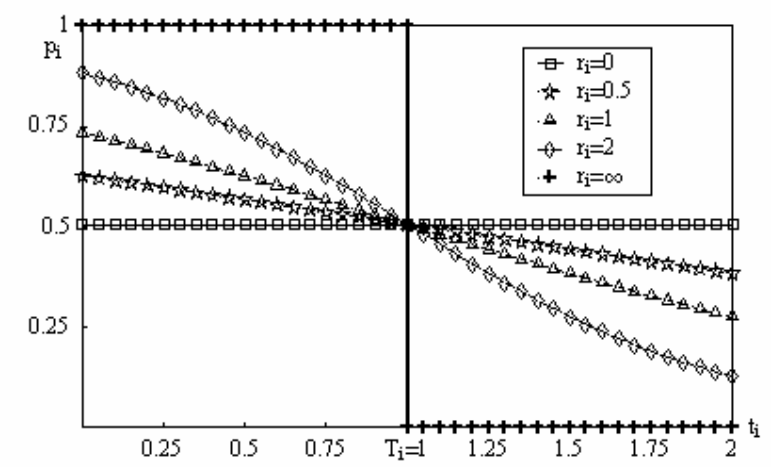

Fig. 2. Difference form: Successful attack probability p_i as a function of the investment t_i for various r_i when T_i=1.

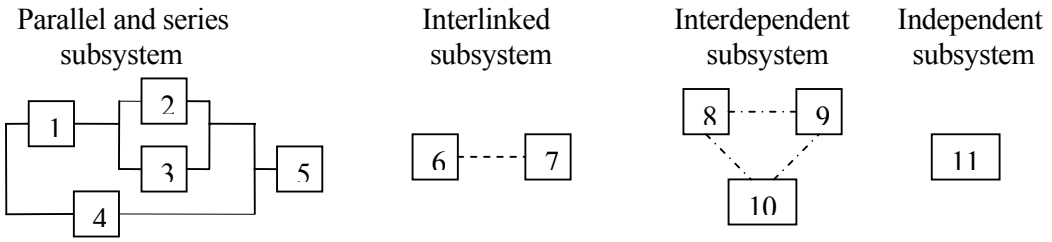

Fig. 3. Example of system with 11 targets.