The Economics of Security and ITS
Security Characteristics of ITS Deployments*

David Gillen
Centre for Transportation Studies
Sauder School of Business
University of British Columbia
Vancouver, BC
Email: david.gillen@CTS.ubc.ca

Alicja Gados
Centre for Transportation Studies
Sauder School of Business
University of British Columbia
Vancouver, BC
**Summary**

The purpose of this paper is to examine the topic of security and apply it to intelligent transportation systems (ITS). ITS have many capabilities and one of them may be improving security. Security is a prominent issue in the advent of 9/11 terrorist attacks. Since the event, several things were realized. One, we are not as secure as we think we are. North Americans have had the luxury of being removed from areas of conflict and war. Our feelings of insecurity have increased. Second, how do we gauge security? Where is the level of protection where the security provided is enough, and how do we measure an improvement in security? What is security?

The new questions have demanded that action be taken to improve security, and because security is a public good, the government has indeed been responsible for taking action. It has become apparent that security is difficult to measure because of a lack of a conceptual definition. We have observed what scholars have warned can stem when there is no definition of security and a tendency for governments to militarize in response to perceived security threat. The failure of governments to offer suitable protection and the feelings of insecurity lead us to ask, why is security under provided?

Security has often been looked at from the technical side, but has failed to explain the lack of security we observe. Recently, economic aspects of security have been noticed by governments: an E.U. proposal recommends that governments respond to market imperfections where market prices do not accurately reflect costs and benefits of improved network security. In light of the literature reviewed, this attempt to smooth out externalities in security spending could make an improvement in security since it improves incentives. Incentives are important economic components that can cause security to fail or succeed.

A literature review of security shows research has mostly been in computer science and information technology. In information technology, security has failed to be provided. Developers constantly come up with new software and systems but due to economic incentives, it is more profitable for them to release something quickly before security bugs are addressed and put out patches later. Due to this, the duty of care to ensure security has been shifted onto the consumer. The consumer is responsible for their own security, so we would tend to think they would tend to err on the side of caution, and provide security for their systems. However, this poses another problem. Most consumers have a problem understanding technology, and this causes them to prefer the 'vulnerable' systems even though it would seem obvious that it is more optimal to secure the systems. This causes more issues. One, their own systems are more vulnerable to attack, and two, their computer can be used to launch an attack on an organization. The first problem is often unaddressed because of consumer's problem with technology – the second is an incentive failure. A paper reveals that a consumer will be willing to spend $100 on a security package for their own security, is unwilling to spend even $1 to prevent their computers from being used in an attack against an organization.

*Research funded by a grant from the Bureau of Intelligent Transportation Systems and Freight Security.*
Security is a public good that competes for resources along with other goods, both in the public and private sector. It is important to realize that security has tradeoffs and opportunity costs, and that decisions are ultimately biased in favor of the decision that will cost least for the player. This means that if security can be offloaded to the consumer at the lower cost, the company will do so. If consumers do not have incentive to protect their machines, and their vulnerabilities are exploited to launch attacks on the company, the company may either build security in, or transfer incentives to the consumer for the duty of care.

Security literature is also based in political science literature. In politics, the pursuit of security is often masks real policy motives. Security has been used and misused as a smokescreen for defending military action. In industry, trade offs have played an important role in stifling an appropriate level of security. Security has not been developed appropriately because entrenching monopolies and price discrimination have been a more important concern. In addition, developers are constantly at work, developing patches and fixing bugs, however it is difficult for them to always fix security because it is worthwhile for them to always introduce new products into the market. This causes the emergence of unsecured systems. The lack of a control loop that shifts incentives fails to control the cycle.

Lastly, (research in IT has found) humans seem to tolerate a level of insecurity, which makes absolute security obsolete. Not only is absolute security unattainable, if it was it could never be measured, but it is completely unnecessary. On par with diminishing marginal returns, the tradeoffs are too high and there is too much to give up for an additional increment of security. An additional increment of security is not valued if one already has ample security or feels adequately secure.

Following the analysis on computer security, we turn to the application of security to transportation and ITS. Since ITS is aimed to increase productivity of the transportation system, we look at how security may be implemented with ITS, with these capabilities. We find that due to the difficulty in providing secure systems, and difficulty in measuring security, leads to a conclusion that an ITS system will be successful and adopted, if it leads to an increase in productivity.

The security concept
No social science subject has been more used and misused than the concept of national security. This carelessness has rendered it useless for everyone but politicians (Baldwin 1997). The lack of definition of security is serious because if it is not defined, it can never be achieved. In moving towards a more comprehensive definition of security, it is necessary to ask what would one be willing to give up to obtain more security. However this question is difficult to answer when there is no comprehensive concept of security. The statement “we may not realize what it [security] is until we are threatened with losing it” (Ullman) is difficult and true after 9/11. Inquiring into the opportunity costs, and economics of security is an excellent way to determine the value of security, but it does not help to determine what security really is.

Several conceptual ideas are examined by Baldwin (1997). Most efforts to define security are concerned with redefining the policy agendas of nation states than with the concept of security itself. Security is concerned with which group or the values of which group should be protected,
and empirical arguments as to the nature and magnitude of threats to those risks (Baldwin 1997).
Understanding the concept of security is a fundamentally different kind of intellectual exercise from
specifying the conditions under which security may be attained. Conceptual clarification logically
precedes the search for the necessary conditions of security, because the identification of such
conditions presupposes a concept of security (Baldwin 1997).

Since the cold war, security, especially national security has been much of a neglected concept –
though there were endless attempts to redefine the term. Security, has been used to justify
suspending civil liberties, making war, and massively reallocating resources in the latter part of
the last century, but has not been well defined conceptually. There is evidence that information warfare
programs exist among many national governments (Sutton and Nagle 2006). Security has not
received serious attention according to the principles of justice, freedom, equality, obligation,
representation and power (Digeser 1994).

Since security is a difficult concept, there is an overlap between concepts of security and power,
and security scholars are involved with technological and policy developments as an ex-post
contribution to security versus ex ante. Certainly this is a criticism of ITS technologies – the evident
fascination with technology precedes the questions of where the product fits in with the system.

A classic paper on the concept of security by Wolfers (1952) has defined security as a low
probability of damage to acquired values. Threats do exist, and this does not lower the probability
of the threat occurring. This can be observed in the US, with post- September 11 regulatory
strategies targeting supply chain security.¹ These recognize that there are terrorist threats out
there, but tries to minimize the damage they can inflict by correcting vulnerabilities and permeability
so damage is minimized.

Obscure definitions of security can be politically harmful. Policy makers have found the obscure
definition of national security useful (Baldwin 1997). The realization that military force and not
security has been the central force of security studies, clarifies why the concept of security has
been ignored. In response to threat of military attack, states develop deterrence policies. The
traditional values for which security stands are political independence and territorial integrity, but
other values are sometimes added. There is a subjective and objective dimension of security,
where states might over or underestimate the actual probability of damage to acquired values.
Unjustified fears might be the objective of security policy; also, a state may consider itself secure
when it is not.

Another question is how much security is enough. Not all views classify security as a matter of
degree. Some think national security is not a condition which cannot be specified: you are either
secure or insecure, and partial security is not possible (Brodie 1950). The word defines an absolute
condition and does not lend itself to the graded spectrum. However if this was the case security
would not lend itself from common usage as an analytical concept. It is quite common to refer to
varying degrees of security. This agrees with economic theory of marginal returns and tradeoffs.
Since security is a good, it has an opportunity cost and things must be given up in order to obtain it.

¹ Since 9/11, the US has realized that the border is a source of vulnerability as it is relatively “open” to trade.
Since that time, regulations have been tightened and supply chain security of trading partners, which travels
along the entire supply chain often not even on US soil, has been scrutinized.
In any case, absolute security is unattainable. A country would not be able to conduct trade with others, there would be no open markets and exchange relationships with other nations would be deemed too risky. The question is which matters more, security or conducting trade, and is always about allocating resources to their first best use. Security is always a matter of degree, and in a world where scarce resources must be allocated among competing objectives, the question of how much security is enough will, and should always be asked.

The goal of security can be pursued by a variety of means. Different policies may plausibly be adopted in pursuit of security – specification of this dimension of security is especially important in international politics. The tendency of security scholars to define security in military terms, or in terms of ‘threat, use and control of military force can lead to confusion as to the means by which security may be pursued. It can also prejudice discussion in favour of military solutions to security problems (Baldwin 1997).

One must keep in mind the sacrifice of other goals that could have been pursued with the resources devoted to security because costs always matter. Only the assumption of the cost-free world would eliminate the necessary conflict among such goals as they compete for scarce resources. The sacrifice of other values for the sake of security inevitably makes such policies subject for moral judgment, given the crimes that have been committed in the name of national security (Baldwin 1997). It is also important to understand that short-run security policies may also be in conflict with long run security policies.

The pursuit of security necessitates the sacrifice of other values. Thomas Hobbes’ reasoning has led scholars to the ‘primacy’ of security: life would be short, nasty and brutal without it. Security is a prerequisite for the enjoyment of other values, such as prosperity or freedom. This has been recognized by the US and their establishment of central security quarters in the Department of Homeland Security is testament (Wise 2002). The value of something, be it gold, water, or security, is not an inherent quality of the good but a result of external social conditions, or consequences of basic supply and demand. In security, like with other values, there are diminishing marginal returns, that is, the more security one has, the less they are likely to value an additional increment of security. Modern states do not allocate all of their resources to the pursuit of security, even in wartime. Even a poor society gives it's population food, clothing and shelter.

In approaching security, marginal value is the only one that provides a solution to the resource allocation problem. This is rooted in the law of diminishing marginal utility is as applicable to security as it is to other values. Security is one of many policy objectives competing for scarce resources and subject to the law of diminishing returns. In light of 9/11 for instance, states and businesses have felt pressure to increase security. The focus on security of course takes away from focusing on other agendas, and can lead to a decrease in productivity (Hobijn 2002). In theory, rational policy makers will allocate resources to security only as long as the marginal return is greater for security than for other uses of the resources.

Almost everyone agrees that common usage tends to equate security issues with important issues deserving of national prominence and financial support. But if national security issues are defined as important, attempts to compare them with other issues will be prejudiced from the start.
Although it is often asserted that international security, unlike national security denotes the interdependence of nation-states with respect to their security relations, the logic is unclear. The 'concept' of security implies nothing about the degree of interdependence among states with security relations – this is a subjective exercise that is case specific. The matter is best left as empirical investigation and should be excluded from the conceptual definition of security.

**Intelligent Transportation Systems**

Security and transportation are tied because they are both public goods. Economists cite two rationales for government intervention in providing transportation goods and services: market failure and distribution of wealth (Engel, Fischer et al. 2006). Markets may not function effectively when one person's use of a good or service does not interfere with that of another person, rival consumption, or when excluding users not willing to pay is impossible (called non-excludability). Both situation give rise to externalities, where people who do not pay for the good benefit from it, people who do not use the good bear the cost. The role of governments is to distribute burden and benefit evenly. The governments' role in providing ITS stems from their traditional involvement in providing transportation infrastructure.

The government spends considerable resources on transportation. In the fiscal years 2004/05, transportation expenditures totaled $21.9 billion, up by $1.5 billion from the year before (Transport Canada 2005). Transportation investments are not as productive as they were up until the interstate highway system was completed in 1970 (Boarnet 1997) hence attention has been turned to ITS and demand management systems. Technology has been increasingly incorporated in the transportation sector with the growing popularity of ITS. In Canada the strategic highway infrastructure (SHIP) program has set out $30 million of total funding from 2001 through 2006 for ITS development nation-wide.

ITS differs from transportation infrastructure from both the supply and demand side. From the supply side, ITS is based entirely on new, relatively unknown, technology, versus known technology like road or bridge construction. From the demand side, success in an ITS system requires user participation, who must be aware of and understand the technology. For example, the market is relatively unknown for advanced traveler information systems (ATIS) because it has been difficult to encourage use of the systems, so projects involve a great deal of risk (DeCorla-Souza and Barker 2005).

There are several ways in which ITS differs from conventional transportation investments:

1. Conventional finance for transportation infrastructure aims to support government led provision of basic amenities to the public, whereas ITS attempts to improve performance of the system by encouraging participation from the private sector.
2. ITS ability to reduce adverse environmental effects, which were externalities in conventional transportation.
3. ITS is based on new, unknown technologies, whereas conventional is based on known technologies (supply side differences).
4. Unknown market for ITS which could play a role in unadoption of technology particularly when voluntary. Advanced Traveler Information systems (ATIS) for instance, require user interaction, and characterize differences from the demand side.

The transportation and ITS contract are also different. Where transportation contracts are largely publicly funded and only involve the private sector in terms of basic contracting out of services, ITS projects are mostly deployed through public-private partnerships (PPPs) that rely on the inherent knowledge of ITS systems and markets (Glaister 1999). Encouraging user of private sector is much like the public agency purchasing an insurance contract (Hall 1998) as it helps the public agency to minimize or shift risk.

**Productivity in information technology**

Growth in knowledge and information based sectors of the economy has outstripped growth in most other sectors. Our increasing reliance on information technology (IT), due to its high productivity benefits has allowed the technology sector to explode. Companies that have invested in IT in the 1980’s experienced exponential growth and productivity in the 90’s. In fact, microeconomic studies found that the production and use of IT assets have contributed substantially to the U.S. aggregate productivity revival in the late 1990’s (Stiroh 2002). Two defining characteristics of the US economy in the late 90’s were faster labour productivity growth, attributed to IT advances, and strong investment in IT assets.

ITS is likely to become very popular due to the potential contributions it can make to productivity, much like IT did in the 90s. IT has become popular because they have been profitable to the economy. In the 1990s, North America experienced a productivity revival that has been attributed to the increased use of IT (Stiroh 2002). The productivity revival, attributed to IT is now spilling over to transportation, to make better use of existing infrastructure. ITS technologies are factor-specific technologies, such as computer systems (IT) designed to improve productivity of transportation. ITS, like IT, is a better way of making use of assets which may allow parallels to be made between the two industries. For instance, IT allowed some businesses to exist that didn’t exist before. It may be that over time ITS can eventually redefine the trucking industry or changing trading patterns. For example the quickly changing interface for technology will require highly adaptable approaches in transport logistics (Janelle and Beuthe 1997). However, the literature has failed to exemplify the full spectrum of effects. The literature is not developed well enough at this point in ITS and all analysis are very speculative.

The strong literature on IT productivity builds an important case for ITS investments. That, coupled with the declining contributions to productivity that transportation infrastructure investments make present a favorable environment for ITS expansion. In terms of productivity of the transportation system, Boarnet (1997) showed that at the margin, investments in highway infrastructure are not economically productive. This is an important point because it exemplifies where funding should be tailored to in the future. Studies have shown that reducing congestion can increase economic output and labour productivity, and the success of Orange County peak-period pricing for road use...

---

2Socio-economic variables arising from investment in ITS have not been thoroughly investigated. ITS, may be expected to cause large, unexpected effects, such as information technology (IT) did in the 90's. These benefits have not yet been fully captured in the literature.
has shown that demand management may be more productive than building new roads (Boarnet 1997). This creates a convincing case for ITS investment in the future.

**ITS application to security**

Information has unencumbered potential in the application of transportation problems. In a paper Berdica (2002) offers that instead of increasing capacity, which is often very capital intensive, it may be more effective to reduce expected costs of travel by reducing travel time uncertainty – such as providing information about road conditions to users, travel time variance and changing congestion conditions. Advanced traveler information systems (ATIS) could allow us to use existing capacity more efficiently (Berdica 2002).

ITS built into border infrastructure can make significant contributions to security. Dedicated trade lanes, advance notification and the electronics-enabling technologies of required paperwork such as manifests are examples of ITS solutions for border. Collection of data can establish patterns can point to aberrant behaviors and anomaly detection can be used to monitor security of the system. This method is in fact the most promising in computer industry for detecting hackers intent on stealing data or transmitting viruses (Flynn 2002).

The initial application of ITS to improve efficiency at borders and minimize transactions costs in trade has been extended to include provisions for enhancing security since 9/11 (Johnson 2004). Initiatives originally designed to smooth out transactions have been used to manage the increased security scrutiny and surveillance applied to borders, ports and airports.

The literature on productivity changes reveals that productivity was not highly adversely affected due to security spending. The increase in security has found to have a minimal impact on productivity on the macro scale. Proposed security spending on the department of homeland security, the new bureau set up to counter terrorism after 9/11 accounted for 0.35% of GDP in 2003, or one-tenth of national defense spending (Hobijn 2002). On the aggregate, the loss of productivity due to new security policies enacted by the U.S. government since 9/11 is estimated to decrease private sector productivity by 0.8%. However other studies have argued that the defense expenditures and the security expenditures are irrevocably tied, therefore, a much larger fraction of GDP is being spent on “security” per se than before, and the effect on productivity is actually higher. Some empirical analysis would clarify this difficulty (Bruck 2004).

In the US, the government is placing several new regulatory requirements on trade, some of which are emphasized by mandatory ITS compliance, for example the advance sending of electronic manifests. This and other requirements can act as a tax on the sector as taxes also reduce productivity. However, taxes increase revenue and can be used in some other fashion for betterment of the social good, or to compensate another economic agent. Threatened sectors may be doubly affected by insecurity, once through security risk and security legislation. There is some evidence that the trucking sector has borne much of the risk in security legislation. Currently costs are internalized but eventually will be passed on to consumers in the form of higher prices. An empirical study on the effects of these changes needs to be undertaken.
Overall, security spending and measures have strong effects – border delays, government military spending, reduction in productivity, restriction in trade, growth and economic activities. Depending on the nature of the economy, security policies can have a differing impact, in the long term, where operate strong forces can alleviate the negative economic effects of security policies.

**ITS evaluation in the literature**

Numerous studies on ITS have focus on the technical aspects, and on benefit cost analysis. Due to the differences between ITS and transportation infrastructure investments, several authors have argued BCA fails to capture all of the benefits or costs related to ITS (Leviakangas and Lahesmaa 2002).

Most analysis of ITS deployment has been favorable, for commercial vehicle operations, border efficiency, and congestion management (Peng, Beimborn et al. 2000), (Zhicai, Jianping et al. 2006), (ICF Consulting, HLB Decision Economics et al. 2001), (ICF Consulting and HLB Decision Economics 2004), (IBI Group 2004), (Jensen, Wik et al. 2003), (Orban, Brown et al. 2002) and (Maccubbin, Staples et al. 2005). The case for ITS in commercial vehicle operations is very compelling (Gillen and Haynes 2002) however the economics mechanism has not been fully comprehended nor quantified, and much of the study of ITS goes towards technical features or evaluation engineering side rather than where it fits into the network (Gillen and Levinson 2004).

ITS has many capabilities, the most promising of which is to improve productivity of existing assets. If productivity and security can be increased at the same time, such as through border ITS, it could be very valuable. Though conceptually it is easy to imagine how ITS may improve security, it is difficult measure. First of all, very little empirical work has been done to examine the productivity of ITS. The studies that have been done have been purely engineering based, and fail to grasp an ‘economics of’ concept or on the socio-economic effects of ITS (Zhicai, Jianping et al. 2006). Therefore, there is uncertainty about socioeconomic productivity of an investment. Second, security is difficult to measure due to the high tradeoffs and opportunity costs for a high level of security.

Few studies have aimed to look at the non-technical aspects of ITS, of those, a study by Gillen and Levinson (2004) has determined that in ITS implementation, the engineering aspects take precedents over economic value (Gillen and Levinson 2004). Gillen and Haynes (2002) have emphasized the promise the ITS holds for commercial vehicle operations, and supply chain management for both public and private sector. The benefits and costs of ITS are generally not well understood, but even more so for commercial vehicle operations, where they offer substantial potential savings in initial evaluations (Gillen and Haynes 2002).

The main difficulty we explore in this paper is finding a conceptual definition of security, and where ITS fits. It is found that security is not a goal that is in of itself, but the increased productivity ITS can offer actually helps to increase security.

**Economic characteristics of security**

Terrorism breeds in openness and globalization, requiring high-profile visible targets, often transportation systems. The solution, inevitably resides in global coordination because global
security is a public good. There are many instances where uncooperative behavior falls short of the optimal outcome: the under supply of pro-active goods and over supply of defense, for instance, show the difficulty. In the first instance, nations are stuck in a prisoners’ dilemma with a Nash equilibrium of mutual inaction. The second case reveals a tragedy of the commons (Bruck 2004). The tragedy of the commons parable demonstrates how free access and unrestricted demand for a finite resource ultimately dooms the resource through over-exploitation is a very serious issue, as it can lead to armament and war in politics, and congestion problems and other issues in transportation.

Many people agree the world has become more vulnerable, especially after 9/11. A variety of risks, such as increase in computer viruses, worms, spam, sniper attacks, anthrax, e-commerce fraud and international financial instability are also examples. In the insecure world, because security is a public good that has opportunity costs, our governments are faced with public policy choices. Public policy choices have to do with risk (private and social), security (national and international) and security policies (private and public) (Bruck 2004).

Risk can come from many sources, political, globalization, technological, social, market or economic forces. When it comes to terrorism, a broad definition of risk applies: this is an aggregate and unquantifiable form of risk, from different sources. Security is a public good because it’s non-rival in consumption, that is, each citizen enjoys the amount of security equally, without infringing on other’s ability to consume security. From the point of view of consumers, security provided by the private sector would be suboptimal. It is impossible to exclude citizens from the provision of national security, justifying public provision or regulation of security (Bruck 2004). This presents a challenge for providing security with ITS.

In the international sphere, security is an important public good. Instances such as the cold war, threat of nuclear war, terrorism and environmental damage demonstrate the universal threat to security. The nature of the public good is that countries fail to internalize foreign costs and benefits of their actions (or inactions) concerning matters of global risk. In addition, national defense measures aimed at diverting risks of harmful consequences of global risks may be over-supplied from a social planning perspective, such as the attack on nationals living abroad. Indeed, less protected countries bear an increasing share of terrorist attacks.

National pro-active measures aimed at reducing global risks have positive externalities – these measures are often under-provided. Cutting greenhouse gas emissions nationally has important global effects but national-level effects are lower. In the existence of global threats to security, actions will be under-provided by national governments. This provides incentive for a global collective on security for internationally coordinating security regimes. The weakest-link paridy is important since the security will only be as good enough as the level of the weakest security regime. This is why terrorists are centered in countries where there is less regulation on terrorism or where there may be a large number of people who pursue it where authorities cannot penetrate.

Insecurity imposes costs on those who are risk-averse. These economic agents prefer a world with less insecurity and are willing to pay a premium to reduce risk. The costs of insecurity are comprised of three events: 1. Direct costs from the risky event itself, 2. Indirect first-order costs from the agent’s reaction to the event, and 3. The indirect, second order costs caused by both policy effects and the agent’s reaction (Bruck 2004).
A study by Siems and Chen (2004) found that indirect effects of security problems outweigh the direct effects rising immediately after the event in terms of economic performance. Indeed, American capital markets have improved their response to cataclysmic events in the last fifty years (Chen and Siems 2004). In fact, it is often not the nature and direct effects of a disastrous incident that determines its consequences but also the reactions of agents and policy makers, or the indirect effects. Extending to ITS, if ITS is meant to serve this security function, in stopping the severity of an attack may not only improve the first-order insecurity (by managing response) but also indirectly by halting compound damage – by routing people away from disaster areas and preventing further deaths. In this environment, people may feel less insecure in knowing an effective, coordinated response is available when crisis hits.

Take for example the Northridge earthquake of 1994. Many deaths have been prevented because ITS was used to reroute people to less critical zones and keeping them off collapsing structures and hazard areas. The Advanced Traffic Signal and Control (ATSAC) system helped travelers cope with the temporary loss of the Santa Monica Freeway (Miller 1998).

One important effect of insecurity is a rise in private sector security spending: firms decide to spend in short term to minimize long term costs. Such spending is akin to insurance spending and reflects a firm's information and preferences. Also, firms can respond to market forces because employees can require employers to provide them. Thirdly, firms are legally obligated to implement security measures. In this third case, mandatory regulation acts as an environmental regulation aimed at increasing social welfare. For a closed economy, this implies costs are borne uniformly by all firms in a given sector, however internationally (as most security policies are aimed) this may not hold and raises important trade policy issues. Such regulation raises costs but not private, firm level benefits. Within sector productivity will fall as a result of such enforced spending. Therefore, a security system that is mandatory must also increase productivity. Indeed, some ITS systems offer both, such as in the case of ITS for freight security, such as RFID container tags which improve scheduling.3

Public and private security spending can be consumptive since output is not positively affected by spending and can cause productivity to fall (Bruck 2004). Productive investments are likely to be crowded out and growth is slowed. Efficiency is another issue. This refers to the equilibrium position on the production possibility frontier (PPF) where the marginal rate of substitution between the security good and the alternative good equals the price ratio between the goods. If an exogenous shock requires a higher provision of security this may lead to a reallocation of production from the alternative good to the production of security. The new equilibrium is efficient if at that point to price ratio equals the marginal rate of substitution (MRS) between the two goods. And inefficient level of security would be obtained if production of either or both goods was within the PPF, if MRS did not equal the price ratio, or if a tax levied to finance security created an excess burden. Another instance may prevent an equilibrium establishing itself in response to technological change, and could potentially extend the PPF outwards.

Globalization and technological change induce structural change in open economies. This may be induced by investments to security infrastructure, such as automation, surveillance and information

3 These are not mandatory but are growing in popularity voluntarily, as a productivity enhancing and scheduling tool, and in reducing transactions costs.
exchange in harbours, airports and border crossings. Globalization in fact may serve as the very means that make the trade off between security and efficiency diminish in the long run. One important policy change of technical security protocols into international organizations are promoting transparency and harmonization and are reducing transactions costs.

Since the economy is focusing around the development of networks due to the information available from advanced technologies, privacy issues are raised. Supply chains are becoming increasingly sophisticated as information chains become more complex. The use of smart tags has risen, positioning and navigation systems are used in combination with mobile technologies. Forcing the resolution of security issues may actually accelerate the development of information systems. But this also makes risks more transparent.

Policy coordination is important, the under supply of pro-active policies and over supply of defensive measures may serve as examples. As demonstrated above, nations are stuck in an incident of uncooperative behavior that falls short of the socially optimal outcome, or “tragedy of the commons.” The same happens with security levels of airports, as shown by Coughlin et al. (2002). When airports do not coordinate their security levels (using game theory to illustrate) the dominant strategy is for both airports to under provide security, leading to a less safe network (Coughlin, Cohen et al. 2002). Nations are stuck in a Nash equilibrium of mutual inaction. Tragedy of the commons occurs with over supply of defensive measures.

The weakest link concept is prevalent in the literature. It is the weakest link public good that emphasizes the need for international cooperation and intervention. Whenever the least contributor sets the overall level, competition fails to achieve the efficient level of security. Even a country, or a business, that heavily invests in security is still vulnerable as it is linked with other less secure countries/establishments through trade, travel and migration. Weakest link members often do not have the capacity to conform to international standards, as a consequence, the international community must support them somehow, which also poses a collective action problem. The Container Security Initiative (CSI) addresses this, in order to protect security of the US, they station US Customs officials at foreign ports to judge whether or not to accept goods bound for the US. Governments face a standard free rider situation. Coordination between governments is difficult because it tends to be myopic and changes with the electoral process. Therefore the governments view tends to be short run which battles with better defined long run focus of terrorists.

Risk and insurance
Indirect first order effects concerning the behavior of agents in response to risky events can be analyzed using insurance theory. By a large set of agents forming an insurance, they can spread risk and improve welfare. The insurance parity provides a few concerns, one of which is moral hazard, and that more risky agents are attracted to the pool, therefore actually increasing risk levels than in the absence of insurance (or regulation). Adverse selection is the other issue – high risk insured can take up the insurance but insurers cannot differentiate them from other individuals due to asymmetric information. Indirect effects from the supply side also affect the insurance market. Standard war and terror risks can be insured in the market but at unacceptable premiums due to their occurrence is too strongly correlated across contracts for insurers to be able to pools it’s risks effectively.
Greater insecurity may lead to changes in demand for tourism services or the supply of foreign direct investment, may lead to the redesign of supply chains, reduced benefits from just-in-time production processes. Firms may choose to source products from local suppliers who are less subject to insecurity, leading to a rise in costs. A study of this sort was undertaken by the University of Buffalo – but actually found this was not taking place to a great extent in the Ontario-NY region.

In general, insecurity thrives on openness. An insecure economy would lower GDP growth more than otherwise. But security is very much a matter of perception. Actual risks are very difficult to assess. There is evidence that people are poor judges of objective levels of risk, especially when emotions of fear are involved, focusing on worst-case scenarios rather than the probability of the event occurring. As a result, people over estimate minor risks or neglect significant risks. This is worsened by the skewed public misrepresentation of insecurity. Compare for instance car crashes versus airplane crashes: people are much more frightened of airplane crashes, even though they cause fewer fatalities. For these reasons it is likely that the private sector and policy makers over-provide security and legislation, so the costs of security may easily exceed it’s benefits.

It has also been argued otherwise, that on the demand side people tend to underestimate the risks for large-scale disasters, which is another obstacle in creating an insurance market for disastrous events. The events of 9/11 have helped people readjust the risks they face, which means the market adjustments, such as a reduced demand for air travel, supply chain restructuring, may not be inefficient but the result of an adjustment process to equilibrium.

Government regulation can cause insecurity: regulatory insecurity aimed at increasing social welfare increases uncertainty for firms, and certain types of regulation may trigger illegal responses, such as black or grey market activities. Since 9/11, inspections and other security related delays at borders increased shipping times and reduced border permeability. Regulation hence enhances the direct effect of insecurity on trade.

Terrorism insurance is an example of where differing policy reactions can be pursued. After 9/11, the US government required insurance firms to offer terror insurance, which it did, at very unattractive prices. In Germany, the government helped subsidize a monopolist PPP to cover the potential risks. Public intervention and even subsidies can be necessary for maintaining some market forces, rather than using regulation.

**Why is security lacking? Evidence from computer science literature**

It has been demonstrated why security may fail on the public scale, and a look at the private sector may shed more light on the difficulty of providing security. The technical literature on security is very heavily based on computer science, but from lessons in this area, we can develop a deeper understanding why security “fails.” Not only politically does society experience insecurity, but also in the consumer product market. Why can't we 'purchase' security?

In fact, both the federal government and the private sector have recognized a strong need to improve cyber security and to treat the security of critical infrastructure assets as a strategic initiative, rather than a compliance burden (Gal-Or and Ghose 2004). Computer and communication security attract extensive press coverage and are a priority to government and
corporate decision makers (Odlyzko 2002). This is due largely to society’s increasing reliance on communication infrastructure.

The security of information technology (IT) has emerged as an important issue in the last few years has been reflected with the US federal government establishment of several industry-based Information Sharing & Analysis Centers (ISACs). The centers are designed to promote disclosure and sharing security vulnerabilities and technological solutions for the correction of security breaches (Gal-Or and Ghose 2004). In a paper, Gal-Or and Ghose work out several economic issues and competitive implications of sharing security information and investments in security technologies.

Increasing evidence to attaining increased security leads to the importance on understanding the economics of security or the non-technical (features) of security. This approach recognizes that there are tradeoffs between costs and benefits. There are incentives to make investments in security and incentives for those players to pass security costs onto others, or to use security for other purposes, such as protecting monopolies. In fact, Microsoft itself gained it’s disproportional market share on this premise (Odlyzko 2002).

Odlyzko (2002) discusses the difficulty of developing secure systems. One barrier is our fundamental social nature allows humans to have some level of tolerance for vulnerability. Promises to fix vulnerable systems and introduce full security have been around for years, but have never been fulfilled. At the same time, there have been no major disasters arising from information systems insecurity. Why do we choose to put up with a level of insecurity? Why do so many systems remain unsecured?

People and formal methodology do not mix well. You are not required to know the intimate details of a technology in order to benefit from it. For instance, you do not need to know that bridge construction and materials have improved over the years to benefit from the improvements, we only need assurance that the bridge is safe. Since it is the consumer that is responsible for their computer security once they purchase software the response of technologists is to improve education to help consumers understand security is important. However this has been proven not to work effectively. In a simple experiment, Odlyzko has shown that humans manage to live with the limitation of not understanding technical systems. Formal methods and human nature are incompatible except for a small percentage of the population: those people who become technologists.

The difficulty with formal methods for the bulk of people is in fact the exact reason people have difficulty with security systems. Technologists develop security systems, and technologists are the small fraction of people that are comfortable with formal systems. In addition, technologists generally have little patience for human factors and social relations; expect others to think the way they do, and to be as skilled at the formal thinking that the design and operation of a proper formal system require. Therefore much like in national matters, in IT, security tends to be underprovided.

These perverse incentives support findings by Gordon (2002) that many firms are not adequately investing in information security. A survey done by the computer Security Institute found 91% of respondents detected computer security breaches in a 12 month period, and losses averaged over $2 million per organization (Power 2001). The importance of information security has resulted in a
flood of research examining the technical aspects defense: encryption, access control and firewalls for instance, with markedly less literature on the economics mechanism of information security (Gordon and Loeb 2002).

Security is not an isolated good, and is an integrated component of a complicated economy, which poses limitations on how effective it can be. Interactions of human society and the nature of that society suggest security will continue to be applied as an afterthought. But this will not be fatal to the application of information technology. Security will not ever offer complete protection, however it will offer protection in terms of decreasing velocity and impact of electronic attacks to a level where other protection mechanisms can operate. Often, this level of protection is acceptable (Odlyzko 2002). There is no propriety for security, and in fact, ‘speed bumps’ are sufficient to realize economic value.

Interesting ideas to apply to the problem of information security are developed in Anderson (2001). His analysis points, that when a party in the position to protect a system is not the party who would suffer the results of a security failure, problems can be expected, called incentive failure (Anderson 2001). For example, computer users will likely spend $100 to protect their own computers against malicious attack, however, few will pay even as little as $1 to prevent their computer from being used to launch attacks against companies such as Amazon or Microsoft.

Incentives for security: the building of networks

The evolution of a network economy and the evolution of a security economy are closely related. The security economy very much depends on the robustness of networks. Successful networks are created via positive feedback mechanisms: the more people use it, the more valuable it becomes. This is true with credit cards, which took about 20 years to establish successfully. Also it is true for virtual networks, as positive feedback squeezed the Mac out of most markets. Developers were producing software for PC first, and Mac later, if at all (Anderson 2001). As more people were using PCs, developers saw this and produced for PCs first, and this loop was created until PCs had significant dominance in most markets.

Networks are not solely important in computer science literature: many public goods attribute the development of networks to their success. This phenomenon is rather general and applies to goods provided by the network, such as telephone and airline services, and to goods where there are positive externalities (Pindyck and Rubinfeld 1992). Highways are characterized by network externalities and spillover benefits. Before a network is complete, connecting additional locations increases the usefulness of the network (Boarnet 1997).

Winner take all market structures, such as the one observed by PC over Mac, was exemplified by the following characteristics:

1) Value of product to user depends on how many other users adopt it;
2) Technology has high fixed costs, and low marginal costs, and applies to both information markets and transportation markets; and
3) Large costs to users for switching technologies.
It is important to get into markets quickly because of huge first mover advantages and strong positive feedback. The success of the internet and Microsoft is because it appealed in this fashion to developers. But why do we see such low levels of security in software? Often, freshly developed software is sold without proper security protection, since mandatory security would decrease the value of the product and would make life difficult for application developers. Not having security appeals to developers because the bulk of support costs fall on users rather than developers.

Price discrimination is a common objective of software manufacturers. This can be seen in ‘seat sales’ in airline markets, where the price differentials are huge between first class, second class, and coach. Price discrimination has been around for, and understood, for a very long time by economists. In 1849, a French economist, Jules Dupuit had written about why third class seats in rail coaches are of such miserable quality – uncovered, open carriages with wooden benches. He says it is not about the cost of putting a roof overhead, or upholstering the seats, but it is to frighten the rich into choosing the more expensive seats. They do that, of course, at the expense of hurting the poor, though this is not their intent (Dupuit 1849).

Today, price discrimination is also achieved my manipulating switching costs. You increase the costs of switching, such as Microsoft has done, by making the systems hard to reverse engineer and make them incompatible with other platforms. This means you have to constantly produce software that is often not tested appropriately, and fixed by constant security patches, and security therefore never has a large role because it’s applied as an afterthought.

Microsoft passport is a secure log on site to access different web pages, including web purchasing without having to remember different log on names and passwords. But actually, the program is not so much about security as a play for control of web server and purchasing information markets. The sites that use MS Passport encoding are able to get their clients information and trade information with other vendors, but at the same time are reliant on the network that is owned by MS passport. This type of a struggle to entrench or undermine monopolies and segment or control markets determines the conditions that make creating security products harder.

One of the most important aspects of a new technology package is if it favors offense or defense in warfare. The machine gave in advantage to defense in World War one, and the tank giving it to offence in World War two. Information warfare is much like warfare in the 20s and 30s; attack is simply easier than defense. The difficulties of developing secure software has been because defense is proving much harder than offence because defending a modern information system is much like defending a large, thinly-populated territory like the 19th century wild west (Anderson 2001). Even a moderately resourced hacker can break anything that is at all large and complex. The men in ‘black hats’ can attack anywhere, and the men in ‘white hats’ have to defend everywhere. Technical bias in favor of attack is made worse by asymmetric information, ie., smaller countries have fewer citizens to defend but more foreigners to attack.

The concept of ‘security by obscurity’ relies on a hacker's ignorance of system design. Obscure designs are used deliberately as a means of entrenching monopolies. But in competitive security product markets, bad product tend to drive out the good because asymmetric information causes a decrease in both price and quality. Anderson (2001) exemplifies with the used car market. If a used car dealership has two types of cars for sale, ones in great condition and lemons, (100 of each) where the good cars are worth $3000 and the lemons are worth $1000, and the customer has no
information on which is which (only the vendor knows), what will be the equilibrium price offered? If customers think that the probability of getting a lemon is equal to the probability of getting a good car, the market price will be $2000. However, that falls beneath the value of the good cars, so at that price only lemons will be sold. So when buyers don’t have the same information about quality as sellers, price and quality drop quickly.

The problem with asymmetric information is made worse when people evaluating a system aren’t the people who suffer when systems fail, such is the case of improper incentives. Perverse incentives cause a security evaluation to actually decrease the value of the product in consumer’s eyes. They also can contribute to delays with release of new products, which undermine the entrenching of a monopoly.

Anderson establishes that the desires behind security systems designs are to:

1) Grab a monopoly
2) Price discriminate
3) Dump (dispose of) risk

All of these are rational objectives from a utility-maximizing firm. It is clear that the pursuit of security is not altruistic. The removal of perverse incentives would depoliticize most issues, and we would see risk management instead of risk shifting (or dumping). Information security is about power and money, raising barriers to trade, segmenting markets and differentiating products. To solve security problems, not just technical tools are required, but analysis of economic information with asymmetric information, and moral hazard. Management of information security is a much deeper problem then most people realize and simplistic technical approaches usually fail.

This has been observed with the introduction of IDAS ITS evaluation tool. This tool assesses ITS deployment plans for metropolitan applications. Though it organizes applications nicely, it has given municipalities a feeling of security that they can, by using this tool, just throw ITS into their systems without proper analysis of applicability to their systems. This has resulted in a lot of money wasted and problems that ITS was supposed to address were not resolved. Three issues were identified: (i) overestimation of ITS option benefits when the benefits are estimated from travel time savings, (ii) incorrect interpolation on travel time reliability rates, and (iii) insensitive cost savings for combined ITS options (Yun and Park 2003).

In terms of actual security software, while is a product of developers, the security it provides is a collaboration between users and developers. It is not enough to make software that can be used securely, software that is difficult to use often suffers in security as a result. This echoes Anderson (2001) that most people have a problem with technology.

In order to protect security of users, it is important to build a secure network. The system the user utilizes must also be useable to other users as well, and much like a network creates value for a company, usability creates greater security. Anonymity networks work by hiding users among users. The larger the set, the more anonymous the participants (Dingledine and Mathewson 2004). To provide anonymity to any of it’s users, the network must accept traffic from external users so the various user groups can blend together. The difficulty of gaining reputability in security is an issue: networks need users for privacy, but need privacy for users. Since a new system will attract users once it has become more popular, low-needs users can break the deadlock. The impact of public
perception on security is especially important in the phase where the network attempts to acquire more users, where the first few widely publicized users of the network can dictate what kind of users it attracts next.

September 11 shows that security applies to infrastructure as much as it does to protecting information. Operational responsibility for protection should be part of the liability for the failure of that protection. The ‘black hats’ mentioned earlier have huge economic advantage, local defensive protection is not enough, there is an essential role for global defense, of which deterrence and retribution may be an unavoidable part. Piracy provides some parallel- governments agreed to the use of pirates as instruments of state policy as unacceptable, it took several treaties, naval actions and overthrow of rogue governments before the world's oceans were pacified. This project became intertwined with the abolition of slavery and spread of colonialism. In the end, economic factors were politically decisive, as piracy simply caused businesses too much money.

The transportation system is one of the subject of attacks from ‘black hats.’ Much like a network of computer users, the transportation system is vast. This makes it vulnerable especially at certain points, ports, borders and intermodal points are susceptible because they are more permeable. Attack from anywhere means that we have to protect everywhere, so to speak. But of course, as noted by Baldwin (1997) it is impossible. Gordon and Loeb (2002) security investments must be targeted where they will be the most productive.

An economics perspective recognizes that while investment in information security is good, more security is not always worth the cost (Gordon and Loeb 2002). This ties back to our discussion on tradeoffs and diminishing marginal returns. Modeling the data naturally recognizes that while some investment security is useful, extra security is not always worth the cost. Models should consider how the vulnerability, and the loss associated with vulnerability affect the optimal level of resources that should be devoted to security. For a broad class of security breach probability functions, the optimal security investment is an increasing function of the level of vulnerability (Gordon and Loeb 2002). However, extremely vulnerable information may be very expensive to protect, a firm may be better off concentrating efforts on protecting midrange vulnerabilities. The data prove the argument. Under assumptions, investment may only be justified only for a midrange of vulnerabilities. Analysis suggests that a firm should only spend a small fraction of expected losses due to a security breach. Little or no information security is economically justified for extremely high and extremely low levels of vulnerability.

**Vulnerability research**

Computer science literature on security is also irrevocably linked to vulnerability, since vulnerability is the precedent for security. Vulnerability research is a common occupation within information systems markets. Since software products often come out early before wide-scale testing can be applied, vulnerabilities are discovered on an almost ad hoc basis.

Vulnerability research occurs in five broad markets: the government market, the open market, the underground market, the auction market and the vendor market. Vulnerabilities can be discovered by internal research teams or obtained from third parties. The differences between government and commercial revenue and cost reasons for vulnerability research are on the revenue side of the
equation. While commercial entities seek vulnerability information for economic gain (to patch their software), governments are motivated by national security. On the expense side, governments must incur similar costs to their commercial counterparts for vulnerability discovery, by hiring labour (vulnerability researchers).

For vulnerability research, the underground market, vendor (open) market and the government market are important markets. The underground market has similarities to the government and open markets, however, the underground’s focus is to inflict damage or steal money: terrorism is an example. The black market for vulnerability research increases the social vulnerability, and economic security costs for governments and businesses.

The private sector undertakes vulnerability research to discover insecurity in their software, that we have shown is often released without proper security testing (Anderson 2001). Though developers make some vulnerability discoveries, many are actually found by users. Most vendors do not compensate for these vulnerability discoveries to not give incentive for blackmail and trading of discoveries on the black market. Ultimately, companies benefit from having a large pool of testers that are not on the payroll. Most companies do not compensate researchers that report vulnerabilities with their products for fear that providing compensation of any kind will open vendors up to blackmail, as individuals will demand unrealistic sums in exchange for information. If not paid what they request, the individual may publicly disclose the vulnerability or sell it to the often lucrative underground market (Sutton and Nagle 2006).

The problem caused by insecure software creates the lucrative underground market for vulnerability information. The failure of firms to ship secure software opens up a black market where holes in security are traded and can be used offensively. Since many vulnerabilities are found voluntarily by users, firms have been economizing on vulnerability discovery. Though this helps them potentially save costs, it feeds vulnerabilities for black market value. The outstanding security problem acts like an externality, whose costs are borne by users, and eventually the firm who fails to provide security, if used in an attack towards them.

Conclusion
How do we assess when we are secure or not? Well, 9/11, and threats of attack from terrorist groups, coupled with the Department of Homeland Security’s (DHS) threat level indicator has given some more information to the public pertaining to how secure they are. How can we improve security with ITS?

A main target of terrorism is the transportation sector, due to it’s relative accessibility, potential to attract significant public attention, linkage with national symbols, and ability to impact a wide number of people immediately (Palac-McMiken 2005). An incident or event can directly or indirectly result in considerable reductions or interruptions in serviceability of a road network. This can be due to several factors such as conflict from terrorist actions, but also adverse weather, accidents or road construction. The Moscow metro bombs and public commuter bombs in Madrid serve as reminders how vulnerable the transport system is, even with heightened security measures since 9/11.
We have showed that ITS can enhance productivity by replacing infrastructure improvements and expensive capital undertakings. Instead of widening a road or building more roads, a government may chose to manage congestion instead, with an ATIS, variable message signs (VMS), and variable toll (road pricing) as demand management strategies. For commercial vehicles, a host of new ITS have allowed improved predictability and reliability in meeting transportation demand: on board computers, cell phones, navigation systems and EDI. ITS equipment for keeping track of shipments and improving service quality also promotes economies of scope for the transport sector, spreads costs, permitting them to allow a variety of consumer needs and adapt quickly to volatility.

ITS also has applications to borders. Due to perceived security threats, the US has enabled several new regulations and programs to attempt to increase border security. These regulations scrutinize trucks, drivers, and cargo at the border. In this effect, border crossings have become increasingly congested and this has cost the economy millions of dollars. In order to help control congestion, and minimize economic losses that are inevitable with stringent security protocols, ITS emerges with border security applications such as smart borders, expedited freight processing and advance notification of manifest and commercial driver. These technologies can increase visibility and productivity, while providing security at the same time. These types of technologies are attractive for firms to undertake voluntarily, which makes implementation easier. In this fashion, to improve social welfare by improving security, incentives are distributed to the firm.

The main vulnerability of transportation arises from globalization. Ultimately, it is a tradeoff between security and efficiency, in terms of how much interaction with the outside world are we willing to give up for an additional increment of security. Security is in fact a public good that is not possible to have in the absolute sense because of diminishing marginal returns. However, security is also an important precedent in enjoying other values, so the “primacy” of security is emphasized in the literature. This must be approached cautiously because in IT, security is often under-produced due to perverse incentives, while internationally; it can be over-produced, exploiting public fears.

The examples from airports show the weakest link concept in security is very important. Because of it's interconnectedness, an airport is only as secure as other airports, due to heavy reliance on the network for security. IT and globalization works in much the same fashion. Since transportation is an enabler of globalization (even though it is the least researched contributor) security of the network becomes important (Janelle and Beuthe 1997).

Globalization exposes transportation to severe vulnerability, often at short notice. Since transportation is a frequent target of terrorist threats, it's use and design must be cognizant of the broader international political environment. Even the realization that global environmental problems warrant global solutions exposes transportation systems and their dependent economies to challenges, such as the implementation of global standards on fossil fuel use. The need for collaboration international collaboration on security cannot be overstated since globalization may diminish the tradeoff between security and efficiency. Piracy was only pacified due to collaboration among governments and the consensus that it simply cost businesses too much.
References


ICF Consulting and HLB Decision Economics (2004). "FHWA Freight BCA Study: Summary of Phase II Results." Under subcontract to AECOM.


Ullman "Redefining Security." pp 130, 133.

