Role of Intelligence Inputs in Defending against Cyber Warfare and Cyber Terrorism

Aniruddha Bagchi
Coles College of Business
Kennesaw State University
Kennesaw, GA 30144

Tridib Bandyopadhyay
Coles College of Business
Kennesaw State University
Kennesaw, GA 30144

Last Revised: March 30, 2016

Abstract

This article examines the role of espionage in defending against cyber-attacks on infrastructural firms. We analyze the problem using a game between a government, an infrastructural firm and an attacker. If the attacker successfully breaches the IT security defenses of the infrastructural firm, primary losses accrue to the victim firm while widespread collateral losses accrue to the rest of the economy. The government assists the infrastructural firm by providing intelligence inputs about an impending attack. We find that expenditure on intelligence adds value only when its amount exceeds a threshold level. Also, the nature of the equilibrium depends on the level of government expenditure in intelligence. We find that the optimal level of intelligence expenditure can change in seemingly unexpected ways in response to shift in parameters. For example, reduced vulnerability of the infrastructural firm does not necessarily imply a reduction in intelligence gathering effort. We also exhibit circumstances under which a system of centralized security in which the government regulates both intelligence gathering as well as the system inspection regime of the infrastructural firm may not always be desirable because of strategic interactions between the players.

1 Introduction

As cyberspace takes an overarching role in the mainstream economic activities, cyber-attack has emerged as a major area of concern in the USA (Carter et al. 2013). Some of the most concerning types of cyber attacks are of the nature of warfare or terrorism, known as acts of Cyber Warfare and Cyber Terrorism, henceforth CWCT. It is now known with reasonable degree of certainty that cyber actors are assessing the information system vulnerabilities of our national infrastructure networks (e.g., facilities and assets that deal with chemical and electrical energy production and distribution) and creating strategic cyberattack vectors to exploit those vulnerabilities (U.S. Department of Defense 2012). As a result, Cyber Warfare and Cyber Terrorism (CWCT) are seen as a real threat at all levels (Wheatcroft 2010).

As such, CWCT is widely different from usual cybercrime in terms of the motivation of the perpetrator. Unlike criminally motivated cybercrime where the attacker attempts to receive some form of pecuniary gain, CWCT attacks are premeditated, politically motivated, executed by national entities, sub national groups or clandestine agents, intended to impact the lives of citizens and deliver a strong political message (Pollitt 1997). As a result, different type of installations, often the infrastructural services become attractive targets for CWCT attacks. In order to appreciate the target selection, please recall a parallel in the 2008 US-Israel CWCT attack where Stuxnet computer worm was injected in the control circuitry of an Iranian nuclear facility (Nakashima and Warrick 2012), which eventually destroyed 20% of all downstream centrifuges and seriously debilitated Iran's overall ability to create nuclear arsenal.

In this paper, we conceptualize and model a game of CWCT defense against an attack on industrial control (SCADA, an abbreviation that stands for Supervisory Control and Data Acquisition Systems) of an infrastructural firm such as an electrical power generation system which results in widespread power outages to downstream economic and civic activities (Ingersoll and Kelley 2013). SCADA is well documented to be a prime target for CWCT (Nicholson et al. 2012). A successful attack on the infrastructural firm will have ripple effects on other sectors of the economy that depend upon the service provided by the infrastructural firm. As a result, the government has a major role to play in defending against CWCT.

Broadly speaking, there are two kinds of processes involved in defending against CWCT. The

first process is gathering intelligence about impending attacks. The next stage requires a defender to take an optimal action based upon this information. In this paper, we call this process as alert activation; in other contexts, this process can similarly be referred to as inspection. The literature has tended to ignore the role of intelligence gathering in defending against attacks. One of the major features of our work is that we model espionage as a centerpiece of the security architecture. A pertinent question therefore is to know the exact role of the government. This issue is far from settled. Should the government be involved in both of these processes as is commonly done in airports or ports? Or should it be involved only in intelligence gathering and leave it to the private sector to act upon that information?

In this paper, we consider both of these scenarios. We call the former system (when the government is in charge of both processes) as *Centralized Security,* and the latter *as Decentralized Security.* Centralized Security is common in many domains such as airport or port security and has been discussed in Bagchi and Paul (2014). However, decentralized security seems to be more relevant to the case of information security. Under decentralized security, there is a concern that the infrastructural firm will underutilize the intelligence inputs because it will not internalize the loss to other sectors in the economy. It is natural to expect that centralized security is a better defensive mechanism because the government would take into account the damage to the entire economy. We show in this paper that this intuition is false. In particular, we identify circumstances in which social welfare is higher under decentralized security (and to be fair, there are other circumstances where welfare is higher under centralized security). Hence, there is no clear ranking between these two defensive systems that applies for all parameter values. We discuss circumstances in which one dominates the other.

Below, we summarize a few other interesting results that we derive. We find that spending nothing on intelligence is better than spending an extremely low amount on intelligence. Additionally, when a government spends a sufficiently large amount on intelligence, then such expenditure enhances welfare. Interestingly, we provide a lower bound on the value addition from intelligence in such cases. We also investigate how the optimal intelligence expenditure varies with changes in certain parameters. For example, suppose there is an improvement in technology that results in a lessening of the degree of vulnerability of the infrastructural firm's controls. A natural conjecture is that such a change will reduce the importance of intelligence gathering and should therefore reduce

the optimal expenditure on intelligence. We show in the paper that this conjecture is not true.

The plan of the paper is as follows: We discuss the literature in Section 2. In the analytical part of the paper, we first discuss the decentralized system in detail in Sections 3-6. In Section 7, we present the results on centralized system. The discussion of this system is concise because the method used is similar to our discussion of decentralized security. We conclude in Section 8.

2 Literature Review

There is considerable research (such as Pollitt 1997, Denning 2000 and 2001, etc.) attempting to provide exact definition of cyber terrorism and delving to qualify and distinguish the exact nature of cyber terrorism as opposed to hacking, cyber-squatting, hacktivism etc. In this research, we adopt the common definition of cyber terrorism proposed by Pollitt (1997) and Denning (2001) as stated in the introduction.

Researchers have investigated strategies to counter acts of cyber terrorism and cyber warfare (CWCT). For example, Scully (2011) differentiates CWCT as an advanced persistent threat (APT) - sophisticated and targeted (as against opportunistic) attacks - and exhorts private-public participation including information sharing - a conceptual novelty that we have modeled in this paper. Our research integrates the role of the sovereign government as a collaborator in defense against cyber terrorism, who extends support by providing intelligence on the spectrum of APT (advanced persistent threat) of CWCT to the private entities that directly face such attacks. Rollins and Wilson (2007) provide guidance for an adequate set of government policies that could effectively counter the capabilities of cyber terrorists. Likewise, our work provides government policies towards an optimal regime of intelligence sharing with the private firms that in turn effectively deters attacks and minimizes overall losses from cyber terrorism.

Supervisory control and data acquisition systems (SCADA) of industrial systems which are at the forefront of CWCT have attracted attention among scholars such as Dacey (2003), Patel et al. (2009) and Nicholson et al. (2012) who have looked at objective issues around technological, architectural and engineering aspects of industrial instrumentation networks. Galloway et al. (2013) provides an abridged yet comprehensive description of SCADA systems, compare these systems with standard networks and point out how security aspects of modern SCADA systems differ from the

usual IT systems. Zhu et al. (2011) provide an excellent taxonomy of cyber-attacks on SCADA that takes into account the escalated vulnerability from de-isolation of SCADA networks owing to increased use of open standard protocols like IP and 802.11 - a reality that we assume as the backdrop of this work.

Miller and Rowe (2012) provide a survey on SCADA incidents of cyber terrorism and categorize them in a taxonomy of 4 characteristics, viz. source, target, modus operandi and impact. In this research we comprehensively integrate each of these 4 aspects of the taxonomy. On one hand, we model the sovereign goverment as responsible for analyzing the cyber terrorists (source) and providing intelligence in a manner that minimizes the loss (impact) to the overall society. On the other hand, we model the infrastructural firm (target) as the responsible entity to neutralize the unfolding attack signature (modus operandi) of the cyber terrorists.

Research in cyber security can be roughly dichotomized between technical and managerial (including behavioral, systemic and economic aspects of cyber security) streams. Of the later, one prominent thread is that of the economics of information security, which is also the area where this research broadly lies. We now briefly review the literature on the economics of cyber security.

The literature on the economics of cyber security has taken two main paths. The first one relates to the overall governance of IT security that encompasses product market dynamics between the vendors, user firms, governing agencies as well as other institutional stakeholders. For example, while Arora et. al. (2006) analyze the impact of software patching on the quality of software and provide optimal patching strategies, Choi et al. (2010) isolate conditions under which a software vendor discloses product vulnerabilities and later show that a regulatory policy that enforces mandatory vulnerability disclosure does not always improve overall welfare.

The other flow - where this work lies - centers on user centric firm level research and deals with optimality of firms' investment in information security; impact and externalities of interdependent investments; information sharing between user firms; systemic optimality of security regimes (prevention, detection and loss control) including their combinatorial arrangements and efficacies.

In this flow, Gordon and Loeb (2002) show that the vulnerability of target and the potential loss from a successful attack affect the optimal level of expenditure on IT security and suggest that not all information assets may justify protection. In contrast, our research focuses only on the SCADA networks as the collective information asset, which is widely known for its overarching

importance in operations of modern infrastructural firms. Campbell et al. (2003), Garg et al. (2003) and Cavusoglu et al. (2004) take a reflective perspective and calculate the impact of information security breaches on firms' stock valuation with the help of event studies. In our research, such reflective impacts are assumed integrated in the overall loss to the infrastructural fitrm and not isolated separately.

Bringing the strategic interplay in cyber defense, Gal-Or and Ghose (2005) and Hausken (2007) show how information sharing between defenders optimize expenditure on information security specific conditions. In contrast, the framework of strategic informaton sharing in our research is modeled through the intelligence sharing relationship of the defender with the sovereign goverment, who has *ex ante* access to classified information in the cyberterrorism space. Cavusoglu et al. (2008) demonstrate the superiority of game theoretic approaches for firms to achieve strategically optimal level of information security, a methodology that we have implemented in this paper to tease out the strategic aspects of CWCT defense. Png and Wang (2009) allow for strategic interaction between defenders and attackers and compare IT security policies of 'user precaution facilitation' and 'enforcement against attackers' under varied backdrops of 1-1 and 1-many cyberattacks. In comparison, our work is more focused in that we only consider CWCT, where the attack vectors are known to be typically of APT (advanced persistent threat) in nature and are 1-1 in nature (Scully 2011). It is important to note that none of the works in either of the two flows of of the economics of information security literature integrates the specifics of CWCT where the attacker is a sub national or terrorist entity where the infrastructural installations are the prime target.

Model based research on CWCT defense is handful and is in an early stage of development. Bandyopadhyay and Mattord (2008) explain how game theoretic modeling can help capture the nuances of cyber terrorism including those of citizens' probability neglect and regulators' bias. However, their research exemplifies the niceties of game theory based modeling approach rather than attempting to provide optimal solutions for CWCT defense. Hua and Bapna (2013) propose a game theoretic model and utilize a simulation approach to investigate the impacts of attacker preference, sensitivity of breach function and degree of deterrence on the optimal level of expenditure on countering cyber terrorism. The closest to our study is that of Hua and Bapna (2013), yet ours is a significant extension on multiple fronts. While Hua and Bapna (2013) consider perfect information, exogenous characterization of cyber terrorists, and linearity of deterrence function to

derive simulated solutions employing assigned numerical values, we present a game theoretic model of imperfect information, where the government provides imperfect signals of plausible cyber attacks to the defenders of SCADA systems and thus effectively coordinates CWCT defense. We provide closed form solution of this game without functional specifications, thus yielding generalized insights across all APT (advanced persistent threat) vectors that may emanate from cyber terrorists.

3 The Model

Consider a game between an attacker (A), an infrastructural firm (D) that is the defender and a government (G). The notations used in the analysis of this game are summarized in Table 1. We begin our description of the game by describing the role of each player.

3.1 Players

The attacker: An attacker is either a state agent (case of cyber warfare) or a sub-state agent (case of cyber terrorism), invested in planning and executing an attack on the defender D. In order to attack, an attacker has to first hatch an executable plan of attack in period 1. It is not guaranteed that the attacker will always be able to develop a viable plan of attack. There are at least two ways to think about this issue. First, being able to develop a viable plan of attack depends only stochastically on the effort. It is possible that an attacker may not be able to develop a plan because of bad luck. Second, all attackers are not equally capable. Assume that an attacker incurs a cost of developing a plan. An attacker with a low cost of developing a plan will have a higher incentive of expending effort for this purpose. This is not the case if the cost of developing the plan is high. It is also important to note that a plan can be a serendipitous outcome as well, e.g., chance meeting with other terrorists or emergence of ad-hoc alliances between terrorists. Hence, the result of the attacker's effort (to develop a plan) remains private information to that person, and from the perspective of others (such as the defender or the government) can be viewed as stochastic.

Let θ be an indicator variable that takes a value 1 if the attacker has an executable plan of attack and 0 otherwise. If $\theta = 1$, the attacker has two possible options - "Attack" and "Do Not Attack." However, if $\theta = 0$, then the attacker does not even have the option to attack because he

does not even have a plan.

The defender: The defender operates in the infrastructure sector and provides services (e.g., electrical energy) to other firms in the general economy. An attack, when successful, debilitates the defender's ability to operate and cuts off its services to the downstream firms. That is, a cyber attack can harm the whole network of firms that depend on the services provided by D. The defender can activate a private and costly state of alert (alternatively known as an inspection regime). A state of alert is a regime of additional inspections and cross validation of data from SCADA logs, annunciation charts of control commands at RTUs, control actuators and field probes; shift overlaps as well as elevating conditions for hot start up of stand by plants including maintainance of stand-by auxiliaries in hot idling mode. An attack is assumed to incur no major losses when the state of alert is activated because all system reduncies deploy quickly. On the other hand, if an attack occurs when the state of alert is not activated, the attack succeeds and the defender suffers loss from missed production as well as recovery and other charges. When infrastructural services are interrupted, collateral losses accrue to the downstream economy, which is serviced by the infrastructural firm.

The Government: The government of the country is mandated to ensure normal services from infrastructural as well as other sectors of the economy. To that end, it spends resources on intelligence gathering. In other words, it institutes a costly cyber terrorism threat signaling system (CTTSS) that can imperfectly estimate the type of the attacker. The purpose of intelligence gathering is to learn the value of θ. A higher level of provisioning results in higher fidelity of CTTSS, ceteris paribus. The signal $s = 1$ (resp., $s = 0$) informs the infrastructural firm whether the government estimates that an executable plan of attack exists or not, *i.e.*, whether government estimates $\theta = 1$ (resp., $\theta = 0$). The government privately delivers signal s to the infrastructural firm.

TABLE 1 ABOUT HERE

3.2 Assumptions

We denote the joint probability distribution of (s, θ) by

$$\{\Pi_{ij}(k)\}_{i,j=1}^{2}$$

where $\Pi_{ij}(k)$ is $\Pr(s = i \text{ and } \theta = j)$, given an expenditure k on intelligence gathering. By the definition of a probability distribution, it must be the case that

$$\Pi_{ij}(k) \geq 0;\ i, j = 0, 1 \text{ and } \sum_{i=0}^{1}\sum_{j=0}^{1}\Pi_{ij}(k) = 1.$$

The degree of association between s and θ increases with the expenditure on intelligence k. In particular, if the expenditure on intelligence increases, then the chance that the government makes a mistake in its assessment is lower. In the model, this is captured by the following assumption:

$$\Pi'_{ii}(k) > 0 \tag{1}$$

and

$$\Pi'_{ij}(k) < 0 \text{ for } i \neq j. \tag{2}$$

We can use the above assumption to determine the change in the posterior probabilities when k increases. Suppose the government observes a signal $s = 1$. Then, it estimates the probability of the attacker having an executable plan as

$$\Pr(\theta = 1 | s = 1; k) = \frac{1}{1 + \frac{\Pi_{10}(k)}{\Pi_{11}(k)}}.$$

It follows from (1) and (2) that

$$\frac{\partial}{\partial k}\Pr(\theta = 1 | s = 1; k) > 0,$$

that is, an increase in the expenditure on intelligence enables the government to assess that there is a greater chance of the attacker having an executable plan when the government itself observes a signal of 1. Following similar steps, it can be shown that

$$\frac{\partial}{\partial k}\Pr(\theta = i | s = i; k) > 0 \tag{3}$$

and

$$\frac{\partial}{\partial k}\Pr(\theta = j | s = i; k) < 0. \tag{4}$$

Note that (3) and (4) means that the True (Positive/Negative) Rates (TR) increase and the False (Positive/Negative) Rates (FR) decrease when the expenditure on intelligence increases.

The order of the moves is as follows: In period 1, the value of θ is realized. Therefore, in this period, either the attacker hatches a plan or fails to do so. In period 2, G spends k to gather intelligence. The purpose of intelligence is to guess the value of θ.[1] In period 3, the government reports its intelligence assessment to the firm. The intelligence assessment is the government's estimate of θ. Based upon the report, the infrastructural firm selects the probability $\beta(s)$ of activating the state of alert. At the same time, the attacker determines to attack the firm with probability α. Note that an attacker can attack only when a plan has been hatched. In other words, $\alpha = 0$ whenever $\theta = 0$. An important point to note is that the attacker is assumed to be *opportunistic* in this model. In other words, the attacker does not necessarily attack even when $\theta = 1$. Instead, the attacker carries out an attack only if it makes sense for him to do so. The normal form of the game in period 3 is given by Table 2.

3.3 Payoff Structure

First, consider the attacker's payoff. If the attacker does not attack, then his payoff is 0. Let τ be the cost of attack that is incurred by the attacker. There are several factors that explain this cost. An attacker bears the risk of being convicted irrespective of the success of the attack, and the expected punishment is one of the components of τ. Apart from this, there is an opportunity cost of the time spent in designing a plan of attack and that is also included in the term τ. We assume that the benefit from an attack is greater than the cost, that is,

$$b > \tau > 0. \tag{5}$$

Next, consider the firm's payoff in period 3. If the firm activates the state of alert, then it is assumed to stop an attack with certainty. This is a simplifying assumption and is used to keep the model tractable. In principle, it is possible to design a model in which an attack is stopped with probability $z < 1$. However, that model is equivalent to our model. To see this, notice that what matters for the results is the detection probability, and the detection probability can be equated in the two models by appropriately calibrating the probability of alert activation.

The marginal cost of activating the state of alert (that is, of inspecting) is a constant and is denoted by $c > 0$. Thus, the payoff of the firm is $-c$ when it activates the state of alert (and this is regardless of the attacker's action). Next, suppose the firm does not activate a state of alert. In this case, if the attacker does not attack, then the firm's payoff is 0 because the firm neither incurs any activation cost nor suffers any damage. Finally, suppose the firm does not activate a state of alert and the attacker attacks. In this case, the firm suffers a loss of $L(b) > c > 0$ from the attack. Since the loss to the firm increases with the gain to the attacker, therefore, we assume that $L'(b) > 0$.

In the next section, we discuss the attacker's optimal action. However, it is important to recognize that an attacker's decision to attack depends upon his perceived probability of a successful attack. In order to derive this, the attacker has to estimate the probability of the government observing either kind of signal. For this purpose, we need conditions similar to (3) and (4) and these are given below:

$$\frac{\partial}{\partial k}\Pr(s = i|\theta = i; k) > 0 \text{ and } \frac{\partial}{\partial k}\Pr(s = j|\theta = i; k) < 0.$$

We assume that

$$\Pr(\theta = 1|s = 1; k) \geq \Pr(\theta = 1|s = 0; k). \tag{6}$$

The above inequality implies that there is a greater likelihood that a plan has been developed when the government observes a signal of $s = 1$ rather than a signal of $s = 0$. Further, we assume that

$$\Pr(\theta = 1|s = 0; k = 0) > \frac{c}{L(b)}. \tag{7}$$

The cost to activate a state of alert c will usually be small in comparison to the damage from a successful attack $L(b)$. Thus, the ratio $\frac{c}{L(b)}$ will be a small number. When there is no expenditure on intelligence, the government can at best observe a noisy signal. The above assumption requires that in such a case, the False Negative Rate (FNR) or the False Clear Rate is sufficiently high. Notice that (6) and (7) together imply that

$$\Pr(\theta = 1|s = 1; k) > \frac{c}{L(b)}$$

for all k.

TABLE 2 ABOUT HERE

4 Alert Activation Stage

First we determine the optimal action of the attacker in period 3 if $\theta = 1$. This is presented in Lemma 1 below.

Lemma 1 *Suppose $\theta = 1$. Then, in period 3, the optimal action of the attacker is as follows:*

$$\begin{array}{rll} \textit{Attack} & \textit{if} & \left\{ \begin{array}{lll} \Pr(s=0|\theta=1;k)\beta(0) + \Pr(s=1|\theta=1;k)\beta(1) & < & \left(\frac{b-\tau}{b}\right) \quad , \\ & = & \quad , \\ & > & \quad . \end{array} \right. \\ \textit{Indifferent} & \textit{if} & \\ \textit{Do not Attack} & \textit{if} & \end{array} \tag{8}$$

Proof. See the Appendix. ■

The left hand side in (8) is the probability of alert activation, while the right hand side is net benefit of the attacker. It follows from Lemma 1 that the attacker chooses to attack only when the probability of alert activation is sufficiently low. Notice that the left hand side of (8) is conditioned on k. Therefore, the optimal action of the attacker depends on the government's expenditure on intelligence. One might want to know if this is a reasonable assumption.

There are two ways to justify this assumption. First, in many democratic countries, information is available about the magnitude of k. For example, it follows from a press release from the Office of the Director of National Intelligence (2013) that the United States spent around $49 billion in the National Intelligence Program in 2013. Similarly, it is reported in the Spending Review (2013) submitted by the Chancellor of the Exchequer in UK that the budget for intelligence agencies is £1.9 billion during 2014-15. The British government will also spend £210 million during this year on cybersecurity. The second justification is theoretical. As we discuss in the next section, the government selects k to maximize a social welfare function (given by (22)). The parameters of the welfare function are common knowledge. Therefore, the attacker can also solve the government's maximization problem and determine the optimal value of k just like the government. Essentially, any attacker can make a reasonable guess about k, as is assumed in our model. This implies that

the attacker can make a reasonable estimate of the quality of the government's intelligence before deciding whether or not to attack. However, it is important to clarify that the exact content of the intelligence report is a secret and the attacker does not observe it; the attacker is only assumed to be aware of the quality of the report.

Next, we determine the firm's optimal action in the alert activation stage. This can be derived in a similar way as above and is presented in Lemma 2 below. Hence, we have the following lemma.

Lemma 2 *Given an intelligence report s, the firm' s optimal action in the alert activation stage is as follows:*

$$\begin{array}{rcl} \textit{Activate state of alert} & \textit{if} & \Pr(\theta=1|s)\alpha > \frac{c}{L(b)}, \\ \textit{Indifferent} & \textit{if} & = , \\ \textit{Do not activate state of alert} & \textit{if} & < . \end{array} \tag{9}$$

Proof. See the Appendix. ■

In (9), the right hand side captures the cost to benefit ratio of activating the state of alert, while the left-hand side captures the probability of an actual attack. For the left hand side, it is important to understand that in the model, *(i)* an attack can take place only if a plan is hatched, and *(ii)* because of imperfect signals, it is possible for an attack to occur even when $s = 0$.

Below, we derive the equilibria in the alert activation subgame. In principle, this subgame can have four kinds of equilibria and these are discussed below.

4.1 Type 1 Equilibrium: Large expenditure on Intelligence

This equilibrium occurs when the following condition is satisfied:

$$\frac{c}{L(b)} = \Pr(\theta=1|s=1;k)\alpha > \Pr(\theta=1|s=0;k)\alpha. \tag{10}$$

This equilibrium is described using Proposition 1 below.

Proposition 1 *In the type* 1 *equilibrium, the following results hold:*

(i) If a plan is hatched, then the attacker attacks with probability

$$\alpha = \frac{1}{\Pr(\theta = 1|s = 1; k)} \frac{c}{L(b)}. \tag{11}$$

(ii) If the firm receives a signal of $s = 0$, then it does not activate state of alert, that is,

$$\beta(0) = 0. \tag{12}$$

(iii) If the firm receives a signal of $s = 1$, then its alert activation probability is

$$\beta(1) = \frac{1}{\Pr(s = 1|\theta = 1; k)} \left(\frac{b - \tau}{b} \right).$$

(iv) The ex ante expected payoff of the firm when the government spends k in intelligence gathering is given by

$$V(k) = -\frac{\Pr(\theta = 1)}{\Pr(\theta = 1|s = 1; k)} c. \tag{13}$$

(v)The ex ante probability of a successful attack is given by

$$\Lambda(k) = \Pr(\theta = 1) \frac{1}{\Pr(\theta = 1|s = 1; k)} \frac{c}{L(b)} \frac{\tau}{b}. \tag{14}$$

Proof. See the Appendix. ■

If the equilibrium is of type 1, then the firm does not always activate state of alert even when the government warns it of a high risk of attack, nor does the attacker always attack even if the plan is hatched. For what levels of intelligence expenditure does this equilibrium arise? We investigate this below. It must be the case that $\beta(1) \leq 1$ and this occurs if

$$\Pr(s = 1|\theta = 1; k) \geq 1 - \frac{\tau}{b}. \tag{15}$$

Notice that (15) requires that k is high enough. Let k_1 be defined as follows:

$$k_1 = \min \left\{ k | \Pr(s = 1|\theta = 1; k) \geq 1 - \frac{\tau}{b} \right\}. \tag{16}$$

Then the equilibrium is of Type 1 if $k \geq k_1$, that is, the type 1 equilibrium arises only when the expenditure on intelligence is large enough.

4.2 Type 2 Equilibrium: Moderate expenditure on Intelligence

This equilibrium occurs when the following condition is satisfied:

$$\Pr(\theta = 1|s = 1; k)\alpha > \frac{c}{L(b)} > \Pr(\theta = 1|s = 0; k)\alpha. \tag{17}$$

This equilibrium is described using Proposition 2 below.

Proposition 2 *In the type* 2 *equilibrium, the following results hold:*

(i) If a plan is hatched, then the attacker attacks with probability $\alpha = 1$.

(ii) If the firm receives a signal of $s = 0$, *then it never activates the state of alert, that is,* $\beta(0) = 0$.

(iii) If the firm receives a signal of $s = 1$, *then it always activates the state of alert, that is,* $\beta(1) = 1$.

(iv) The ex ante expected payoff of the firm when the government spends k *in intelligence gathering is given by*

$$V(k) = -\left[\Pi_{01}(k)(L(b) - c) + \Pi_{10}(k)c + \Pr(\theta = 1)c\right]. \tag{18}$$

(v)The ex ante probability of a successful attack is given by

$$\Lambda(k) = \Pi_{01}(k). \tag{19}$$

Proof. See the Appendix. ■

Compared to the type 1 equilibrium, the values of α and $\beta(1)$ are both higher in the type 2 equilibrium, while the value of $\beta(0)$ remains the same. The intuition is that in the type 2 equilibrium, the quality of the intelligence report is lower. Hence, the chance of an attack increases. Consequently, the infrastructural firm is forced to activate the state of alert more often.

4.3 Type 3 Equilibrium: Low expenditure on Intelligence

This equilibrium occurs when the following condition is satisfied:

$$\Pr(\theta = 1|s = 1; k)\alpha > \frac{c}{L(b)} = \Pr(\theta = 1|s = 0; k)\alpha. \tag{20}$$

Since this equilibrium is not used much in the paper, therefore it is discussed in detail in the Appendix (see Proposition 8). It can be shown that the type 3 equilibrium occurs if $k \leq k_3$ where

$$k_3 = \max\left\{k|\Pr(\theta = 1|s = 0; k) \geq \frac{c}{L(b)},\ \Pr(s = 1|\theta = 1; k) \leq 1 - \frac{\tau}{b}\right\}. \tag{21}$$

An important point that is shown in the Appendix is that $k_3 \leq k_1$. It will be shown later that Type 3 equilibrium will never occur because it is in the government's interest to spend an amount greater than k_3 on intelligence gathering.

It can also be shown that the equilibrium of type 2 occurs for $k \in (k_3, k_1)$.

4.4 Other Candidate Equilibria

In principle, there is a fourth case possible in which the following chain of inequalities hold:

$$\Pr(\theta = 1|s = 1; k)\alpha > \Pr(\theta = 1|s = 0; k)\alpha > \frac{c}{L(b)}.$$

However, it can be shown that this is not consistent with an equilibrium.

5 Optimal Expenditure on Intelligence

In this section, we derive the government's optimal expenditure on intelligence. The government's objective is to maximize the overall social welfare. There are three components of the social welfare function. The first is the payoff of the firm, $V(k)$. This term is derived from the alert activation subgame. Note that $V(k)$ is negative.

The second is the expected negative externality (collateral damage) of an attack on the rest of the economy as services from the infrastructural firm D is disrupted from the cyber attack. Each successful attack imposes a cost of ω on the rest of the economy. Therefore, the expected negative

externality (collateral damage) is given by

$$\omega\Lambda(k)$$

where $\Lambda(k)$ is the probability of a successful attack. The third part of the social welfare is the cost of gathering intelligence, k. Therefore, the social welfare function is given by

$$W(k) = V(k) - \omega\Lambda(k) - k.$$

The social welfare function therefore takes into account the benefit as well as the cost of providing security. Hence, in equilibrium, the government is assumed to achieve an optimum balance between these two objectives when choosing k. This is an important point because the literature (and in our opinion, public policy also) has tended to focus too much on the benefits of security. This results in excessive diversion of funds from other productive purposes to security.

Using the analysis of the section above, we have the following proposition.

Proposition 3 *The social welfare function takes the following form after accounting for the equilibria in the alert activation subgame:*

$$W(k) = \begin{cases} -\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k)}\left[1+\omega\frac{1}{L(b)}\frac{\tau}{b}\right]c - k & \text{if} \quad k \geq k_1, \\ -\Pi_{01}(k)\left[L(b)+\omega-c\right] - \Pi_{10}(k)\,c - \Pr(\theta=1)\,c - k & \text{if} \quad k_3 \leq k < k_1, \\ -\left[1+\omega\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=0;k)}\frac{1}{L(b)}\frac{\tau}{b}\right]c - k & \text{if} \quad k < k_3. \end{cases} \tag{22}$$

Proof. See the Appendix. ■

The government's objective is to maximize the social welfare function $W(k)$ by optimally choosing k. Let k^* denote the optimal level of intelligence. We first show in the lemma below that $k^* > k_3$.

Lemma 3 *The social welfare function $W(k)$ decreases in k for $k < k_3$. Hence, k^* is either 0 or greater than k_3.*

Proof. See the Appendix. ■

The implication of Lemma 3 is that if the government spends only a small amount $0 < k < k_3$

instead of 0, then it will reduce social welfare. Hence, in order for intelligence inputs to add value, the government must spend at least k_3 in intelligence gathering, and refrain from providing signals that are too noisy.

In general, the social welfare function $W(k)$ can have a local maximum in either the range $k \in (k_3, k_1)$ or in the range $k \in (k_1, \infty)$, or both. Let $\widehat{\hat{k}}$ be the local maximizer in (k_3, k_1), while let $\hat{k}$ be the local maximizer in (k_1, ∞). Suppose the parameters are such that spending 0 on intelligence is sub-optimal; this is discussed in detail below. The global maximizer is then defined as follows:

$$k^* = \arg\max W(k)$$

and the implication is that

$$k^* = \begin{cases} \hat{k} & \text{if} \quad W\left(\hat{k}\right) \geq W\left(\widehat{\hat{k}}\right), \\ \widehat{\hat{k}} & \text{otherwise.} \end{cases}$$

In principle, the optimal k can belong to either range. If k^* belongs to the intermediate range (k_3, k_1), then in the alert activation subgame the equilibrium is of type 2. On the other hand, if k^* is greater than k_1, then in the alert activation subgame the equilibrium is of type 1. Thus, the government acts as the coordinator of the alert activation subgame. Finally, as we have already discussed, the equilibrium of type 3 does not occur in equilibrium.

5.1 Value of Intelligence

It is important to determine the value of intelligence in the context of cybersecurity. To do so, let us examine the social welfare function if the government does not spend on intelligence. In this case, the infrastructural firm will have to defend itself without the benefit of any intelligence input.

Proposition 4 *When the government does not spend any money on intelligence gathering, then the following results hold in the alert activation subgame:*

(i) If a plan is hatched, then the attacker attacks with probability $\alpha = \frac{1}{\Pr(\theta=1)} \frac{c}{L(b)}$.

(ii) The firm activates the state of alert with probability $\beta = 1 - \frac{\tau}{b}$.

(iii) The ex ante expected payoff of the firm is $-c$.

(iv)The ex ante probability of a successful attack is $\frac{c}{L(b)} \frac{\tau}{b}$.

Using the results above, it can be shown that social welfare is

$$W(0) = -\left[1 + \omega \frac{1}{L(b)} \frac{\tau}{b}\right] c$$

when the government does not spend on intelligence gathering.

What is the value of intelligence? This is discussed in the corollary below.

Corollary 1 *(a) If the government spends at least k_3 on intelligence instead of 0, then welfare changes by at least*

$$\left[1 - \frac{\Pr(\theta = 1)}{\Pr(\theta = 1 | s = 1; k_1)}\right] |W(0)| - k_1. \tag{23}$$

(b) This amount is positive if

$$\Pi_{11}(k_1)\,\Pi_{00}(k_1) > \Pi_{10}(k_1)\,\Pi_{01}(k_1) \tag{24}$$

and

$$|W(0)| > \frac{k_1}{1 - \frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k_1)}}. \tag{25}$$

Proof. See the Appendix. ■

If the government spends at least k_3 on intelligence instead of 0, then the change in welfare is at least equal to the expression in (23). In general, the lower bound on welfare improvement can be negative. However this expression is positive if (24) and (25) hold. Therefore, intelligence is guaranteed to add value as long as these two sufficient conditions hold.

6 Sensitivity Analysis

In this section, we examine the impact of a change in parameter values on the optimal expenditure on intelligence and the optimum social welfare. For this analysis, we need the first order conditions which are as follows:

$$W'(k^*) = -\Pi'_{01}(k^*)\,[L(b) + \omega - c] - \Pi'_{10}(k^*)\,c - 1 = 0 \tag{26}$$

if $k^* = \widehat{\hat{k}}$ and by

$$W'(k^*) = \frac{\Pr(\theta = 1)}{[\Pr(\theta = 1|s = 1; k^*)]^2} \left[1 + \omega \frac{1}{L(b)} \frac{\tau}{b}\right] c \times \frac{\partial}{\partial k} \Pr(\theta = 1|s = 1; k^*) - 1 = 0$$

if $k^* = \hat{k}$.[2] The second order condition is that $W''(k^*) < 0$.

First, we consider the impact of a change in the degree of vulnerability of the SCADA system.

6.1 Improvements in SCADA equipment and control

The Original Equipment Manufacturer (OEM) who supply SCADA equipment provides for the requisite qualities of the system. Improvements in design and processes involving hardware and software as well as better implemention of redundancy and validation management in the command and control architecture of RTUs and PLCs reduce the vulnerability of a SCADA system.[3] A higher degree of vulnerability implies that cyber terrorists would have higher likelihood of success in developing a plan of attack. In our model, the degree of system vulnerability of SCADA is captured by the probability that an attacker succeeds in developing an executable plan, that is by

$$p \equiv \Pr(\theta = 1).$$

A lowering of vulnerability is associated with a reduction in p. In this subsection, we examine how the equilibrium in the model is affected when there is a reduction in p. One would expect that a reduction in p would reduce the expenditure on intelligence, since better security features of SCADA equipment likely reduces the need for good intelligence. One would also expect that social welfare would increase with a reduction in p. Below, we demonstrate that there are circumstances in which these conjectures do not hold.

One important feature to keep in mind is that a change in the degree of vulnerability changes k_1 (defined in 16), which is the boundary between the levels of government spending in intelligence k segregating the type 1 equilbrium from the type 2 equilibrium. A direct consequence of this is that the equilibrium may shift from one type to another in response to a reduction in p. We simply denote such a change a "large" change in p. In contrast, when there is a "small" change in p, the equilibrium remains of the same type both before and after the reduction in p. We discuss the

impact of the small changes first.

6.1.1 Equilibrium is of type 2 before and after the reduction in p

In this case, a reduction in p affects the optimal intelligence expenditure and welfare in the following way:

Proposition 5 *Suppose there is a small change in the degree of vulnerability p such that the nature of the equilibrium is type* 2 *(moderate intelligence expenditure) both before and after the change. In this case, a decrease in p (a) can change the optimal intelligence expenditure either way, and (b) increases welfare if*

$$\Pi_{11}(k)\,\Pi_{00}(k) > \Pi_{10}(k)\,\Pi_{01}(k) \tag{27}$$

for $k \in (k_3, k_1)$.

Proof. See the Appendix. ■

The important point to note is that a reduction in p does not always result in a reduction in k as one would expect. This is because of the interaction of two counteracting forces. A reduction in vulnerability initially provides an incentive to the government to reduce its intelligence expenditure. However, when the equilibrium is of type 2, the fidelity of intelligence is low anyway. Any further reduction in k now makes the intelligence report so noisy that it forces the firm to search unnecessarily on many occasions. This increases the inspection cost. If this second effect is the larger one, then it is not socially optimal to reduce intelligence expenditure.

6.1.2 Equilibrium is of type 1 before and after the reduction in p

Following similar steps as above, it can be shown that in this case, a lowering of vulnerability unambiguously leads to a decrease in the optimal expenditure on intelligence. Also, it can be shown that in this case, social welfare unambiguously increases when there is a lowering of vulnerability (*i.e.*, reduction in p).

6.1.3 Equilibrium is of type 2 initially and is of type 1 after the reduction in p

In the discussion above, we considered situations in which the character of the equilibrium did not change. However, when there is a change in p, then the character of the equilibrium can also change and it can lead to counter-intuitive results. The following proposition summarizes the key result in this case.

Proposition 6 *Suppose there is a large change in the degree of vulnerability p such that the nature of the equilibrium changes from type* 2 *(moderate intelligence expenditure) to type* 1 *(large intelligence expenditure). In this case, there are parameter values for which a decrease in system vulnerability p leads to (a) an increase in the optimal expenditure on intelligence k and (b) a decrease in welfare.*

Proof. See the Appendix for a sketch of the proof. ■

The implication of this result (along with the results on small changes in p) is that the optimal expenditure on intelligence does not change monotonically with p. The intuition for the above proposition is as follows: Suppose there is a reduction in the system vulnerability. Everything else remaining constant, this acts as a deterrent to the attacker, and as a result, the attacker reduces his probability of attack. The firm therefore reduces its alert activation rate in order to save on the alert activation cost. This in turn enhances the chance of a successful attack. To counter that, the government spends more on intelligence to ensure that the decision to reduce the rate of alert activation is better supported by higher quality intelligence.

Finally, note that in this situation, there is also a reduction in welfare in response to a decrease in vulnerability. This result is also counter to what one might expect.

6.2 Decrease in negative externality (collateral damage)

In this subsection, we consider the impact of a decrease in the external cost ω. The external cost measures the damage to other firms in the network when the attacker successfully breaches the security of the infrastructural firm. The external cost can be lessened if other firms in the network set up IRDR (Incidence Response and Disaster Recovery) and BC (Business Continuity) plans in the event of a damage to the network.

Let us first examine the change in k^* when the external cost ω decreases. In this case, k_1 does not change and hence there will be no switch from one type of equilibrium to another. It can be shown that $\frac{\partial k^*}{\partial \omega} > 0$, that is a decrease in the external cost leads to a decrease in the optimal expenditure on intelligence. Further, social welfare unambiguously increases when there is a reduction in the external cost. Both of these results are along expected lines.

6.3 Decrease in the cost of alert activation

In this subsection, we consider the impact of a reduction in the alert activation cost c. One would expect that such a reduction would reduce the optimal expenditure on intelligence, since the firm can increase the rate of alert activation. This should also increase welfare. However, as we show in the analysis below, such a conjecture is not correct. For the analysis, it is important to recognize that a change in c can change k_3 (defined in 21). This is the lower bound of the set of k in which the equilibrium is of type 2 in the alert activation subgame. This can result in a switch of the equilibrium from type 2 to type 1 when c decreases. We focus on this case in our discussion because this is more interesting.[4]

6.3.1 Equilibrium is of type 2 initially and is of type 1 after the reduction in c

The following proposition summarizes the key result in this case.

Proposition 7 *Suppose there is a reduction in the marginal cost of alert activation c such that the nature of the equilibrium changes from type 2 (moderate intelligence expenditure) to type 1 (large intelligence expenditure). In this case, there are parameter values for which a decrease in the alert activation cost c leads to (a) an increase in the optimal expenditure on intelligence k, and (b) a decrease in welfare.*

Proof. See the Appendix for a sketch of the proof. ■

This result (along with the results on small changes in c) implies that the expenditure on intelligence does not change monotonically with c. The intuition is similar to the case when there is a reduction in p.

6.4 Increase in loss to the infrastructural firm

This can be discussed along similar lines as above. The discussion is in the Appendix.

6.5 Discussion on coordinated CWCT defense

We have presented a game theoretic model of CWCT and analyzed the strategic actions of the players in the game. We now discuss the public policy implications that emerge from the strategic actions of the players in the coordinated game.

The infrastructure sector faces the frontal impact of CWCT, yet the secondary losses ripple through the general economy. This negative externality argues for sovereign intervention and support system in defense against CWCT. Our research demonstrates that sovereign support is beneficial when such commitment exceeds a threshold level of expenditure on intelligence. An adequate level of expenditure on intelligence determines the equilibrium of the game and coordinates actions of the strategic adversaries. For example, by adjusting the expenditure on intelligence, the government can moderate the attacking propensity of the attacker (α) and also influence the alert activation regime (β) of the infrastructural firm, thereby ensuring an overall desirable state of assurance in cyber defense.

Over the last two decades, open standard IP protocols have been increasingly implemented to interconnect SCADA systems with other corporate and business information systems. This has advantaged the hacker community who are generally not familiar with the proprietary protocols of industrial SCADA systems. The OEMs and the system integrators of SCADA systems now attempt to provide immunity of the RTUs and PLCCs from rogue access with the help of innovative system layouts and design considerations in addition to standard firewall and IDS protections. An attack of cyber terrorism cannot be conceived unless the vulnerabilities in the SCADA systems and its interconnectivity with the corporate networks can be identified and exploited. This reality is modeled with the indicator variable θ. An intelligently integrated SCADA network reduces these vulnerabilities (that is, p falls), making it less likely that an executable plan for a cyber attack can be hatched.

As the vulnerabilities of a specific SCADA system and its interconnectivity are extensively researched and discussed between the potential perpetrators, it becomes opportune for the intel-

ligence community to identify and monitor such excitement ("chatter" in intelligence parlance). In turn, this makes the signaling system (s) amenable to predict the state variable θ. As more resources and assets are pulled in by the government to monitor the chatter, the signaling system more closely mirrors the reality of whether a viable, executable plan for cyber attack has indeed been hatched or not. We have shown that unless the signaling system achieves at least a threshold level of fidelity, the economy does not stand to benefit from the signaling system at all. In other words, half hearted and inadequately supported sovereign help in defense against cyber terrorism is not productive and should be avoided.

An adequately resourced and properly implemented mechanism of cyber terrorism threat signaling system (CTTSS) predicts whether a credible threat exists or not. This refines the information set of the defender who must decide whether to activate a costly state of alert (β), which among other activities include manual inspections of the RTUs and PLCCs in the SCADA system.[5] Such specialized regime, when activated, successfully identifies and foils an attack.

The default vulnerability level of the SCADA systems (θ) in the infrastructure sector influences the mechanism of CTTSS at the optimal level of resourcing (k) by the government in varied degrees. When the OEMs are able to reduce SCADA vulnerability, the government can reduce its resources for CTTSS if the fidelity of the signal is high enough. While this may lead someone to argue that government should consider subsidizing R&D efforts of the OEMs to reduce SCADA vulnerabilities, such an action is not certain to yield positive results. First, there are plausible circumstances in which the optimal expenditure on espionage increases in response to a reduction in SCADA vulnerability. If this reduction in vulnerability is a result of government subsidy on the R&D of OEMs, then the government will have to bear the burden of the subsidy as well as the additional intelligence expenditure. This may not be feasible given the government's budgetary constraints. And second, infrastructural firms optimally procure SCADA technologies from global markets, whereas such R&D subsidization can only create minor impact in the local market.

The collateral damage (ω) from a stalled and incapacitated SCADA system in an infrastructural firm can be reduced when fault tolerant, redundant or parallel services are available or when the secondary firms have effective business continuity plans (BCP) to sustain the interruption in service. If there is a reduction in the magnitude of collateral damage from a successful attack, then the government can afford to reduce its support for CTTSS.

In essence, our analysis shows that the government should create and adequately support a robust mechanism to collect and disseminate CWCT threat outlook to the infrastructure sector. Now we investigate whether government should also consider managing the trigger for alert activation regime in the CWCT firms.

7 Is Centralized Security More Desirable?

In this paper so far, the government is assumed to be in charge of intelligence gathering and the infrastructural firm is allowed to determine its alert activation strategy. Such a system is known as a decentralized system of security. This system may not be socially optimum since the alert activation strategy is determined by considering only the infrastructural firm's interests (and therefore ignoring the spillover effects of an attack on the non-infrastructural sector). Therefore, it is of interest to know if social welfare can be improved by internalizing the externality. One way to achieve this is to let the government take over the responsibility of alert activation (that is, inspection). In many industries such as the airline industry and shipping, the government is in charge of both intelligence gathering as well as alert activation. Will such a move necessarily improve welfare? We now examine the effect of having centralized security, as opposed to decentralized security that was considered so far. Surprisingly, we find that such a move does not necessarily improve welfare.

Our solution strategy is as follows. Assume that before the game begins (say in period 0), the government has to decide whether to adopt a system of centralized security or a system of decentralized security. Once it makes a selection, it is locked into that decision. This decision is also publicly observable. The rest of the game then unfolds. Which one is then the best system? In period 0, the government can anticipate the future outcomes. Therefore, in the spirit of backward induction, it can compare the anticipated outcomes and select whichever system yields a higher level of welfare.

With decentralized security, the payoffs in the alert activation stage are given by Table 2. With centralized security, we need to make one change in the payoff structure. The change is that if there is a successful attack, then the payoff of the defendant is $-\left(L\left(b\right)+\omega\right)$, instead of $-L\left(b\right)$. In this case Lemma 1 still holds, but in Lemma 2 the expression in the right hand side changes from $\frac{c}{L(b)}$ to $\frac{c}{L(b)+\omega}$.

An analysis of equilibrium in the alert activation subgame can be done along similar lines as in the case of decentralized security. The payoff of the government in the equilibrium of the alert activation subgame (for a given k) is denoted by $U(k)$ and is as follows:

$$U(k) = \begin{cases} -\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k)}c & \text{if} \quad k > k_1, \\ -\left[\Pi_{01}(k)(L(b)+\omega-c)+\Pi_{10}(k)c+\Pr(\theta=1)c\right] & \text{if} \quad k_4 < k < k_1, \\ -c & \text{if} \quad k < k_4. \end{cases}$$

In the above expression, k_4 is defined as follows:

$$k_4 = \max\left\{k|\Pr(\theta=1|s=0;k) \geq \frac{c}{L(b)+\omega},\ \Pr(s=1|\theta=1;k) \leq 1-\frac{\tau}{b}\right\}.$$

Since $\Pr(\theta=1|s=0;k)$ is a decreasing function of k, therefore it follows that

$$k_4 \geq k_3.$$

Social Welfare in this case is the payoff of the government in the alert activation stage and its payoff in the intelligence gathering stage. Consequently, the welfare function under centralized security is as follows:

$$W^{CE}(k) = U(k) - k. \tag{28}$$

7.1 Centralized vs. Decentralized Security

In order to compare the two systems, we need to examine separately four possible ranges of k as follows: $(0, k_3)$, (k_3, k_4), (k_4, k_1) and (k_1, ∞) (illustrated in Figure 1). Note that the intelligence expenditure is "small" under both systems in the first case when $k \in (0, k_3)$. Under both systems, the intelligence expenditure is moderate in the third case, and it is large in the fourth case. The most interesting case is the second one in which the intelligence expenditure is moderate in a decentralized system but only small in a centralized system. This case plays an important role in the results that we present below.

How does the optimal expenditure on intelligence under centralized security compare with the one under decentralized security? Let k^{CE} be the optimal expenditure on intelligence under

centralized security and let k^{DE} be the optimal expenditure on intelligence under decentralized security. By comparing the first order conditions under the two systems, the following conclusions can be drawn:

(1) If $k^{DE} > k_1$, then $k^{CE} < k^{DE}$. In other words, if the equilibrium is of type 1 (large expenditure on intelligence) under the decentralized system, then the expenditure on intelligence is lower under the centralized system. (2) Under the centralized system, if it is optimal to spend a positive amount, then this amount should be at least k_4. (3) If $k^{DE} \in (k_3, k_4)$, then $k^{CE} > k^{DE}$. In this case, a centralized security system requires a higher expenditure on intelligence. (4) If k^{CE} and k^{DE} both belong to the range (k_4, k_1), then $k^{CE} = k^{DE}$.

Next, we compare welfare under the two different systems. By comparing (28) with (22), it follows that for a fixed k,

$$W^{CE}(k) \geq W(k)$$

except when $k \in (k_3, k_4)$. It is then easy to show that there are several cases in which social welfare is higher under centralized security. For example this result holds if $k^{CE} > k_1$ and $k^{DE} > k_1$. The fact that welfare may be higher under centralized security is not surprising. *However, what is interesting is the observation that there are circumstances in which welfare is lower under centralized security.*

To see this, consider Figure 1. Notice that the welfare function under centralized security lies above the welfare function under decentralized security when $k < k_3$ or when $k > k_1$. Further, these two functions coincide when $k \in (k_4, k_1)$. Under decentralized security, welfare is maximized at X. However, this is not the case under centralized security since X lies to the left of k_4. Hence, under centralized security, welfare is maximized at Y. Thus, welfare is lower under centralized security. The insight from this analysis is that a government controlled security system need not be more desirable under all circumstances. In other words, when the the government's optimal intelligence expenditure lies between k_3 and k_4 (such that it is considered moderate in the decentralized system but small in the centralized system), then the optimal mechanism of the government is NOT to dictate the alert activation policy of the firm. Only when the government optimally spends more on intelligence, it becomes appropriate to dictate the alert activation regime of the firm.

Two important policy matters are apparent from the overall analysis in this article. We have

already shown that unless the government spends enough on intelligence gathering to create an intelligence mechanism that is at least as good as the threshold level of fidelity, the government should refrain from collecting and disseminating intelligence at all. Now, in this section, we again observe a similar extension of the idea that unless the intelligence expenditure is high enough, the government should not attempt to dictate the alert activation regime of the CWCT firms!

FIGURE 1 ABOUT HERE

8 Concluding Remarks

In this paper, we focus on efficient ways of providing security against cyber warfare and cyber terrorism (CWCT) to the infrastructure sector. There are two processes involved in defending against CWCT. The first is through intelligence gathering about CWCT attacks and the second one is the state of alert that involves specailized command, annunciation and data inspection at the RTU and PLCC units of SCADA systems and mainitain the system redundancy arrangements in hot rolling mode. Intelligence gathering is done by the government, while the SCADA alert activation remains the role of the private sector. Our model captures the dynamics of these strategic roles and analyzes the outcome levels of CWCT security. We also consider the collateral losses to the non-infrastructure sector that occur as a result of cyber attacks on infrastructural firms. Our analysis shows: *(i)* The government can change the nature of the equilibrium in the game between the infrastructural firm and the attacker, *(ii)* expenditure on intelligence adds value only when its amount exceeds a threshold level, and *(iii)* the optimal level of intelligence can change in seemingly unexpected ways in response to parametric changes. For example, lowering vulnerability of SCADA systems by the OEM may not always imply a reduction in intelligence gathering efforts. We also investigate whether government should initiate direct involvement in SCADA security and create strict guidelines and mandatory procedures akin to what we see in the case of TSA in the airline industry. Our analysis suggests that such centralization ensures higher welfare only when the intelligence outlay is high and does not lie within a certain range. In other words, government policy of implementing centralized guidelines and procedures must precede cautious estimation of the current state of decentralized provisioning of CWCT security and avoid those scenarios where a system of centralized guidelines and procedures become counterproductive in presence of low

fidelity intelligence.

As we have mentioned in the Introduction, undeniable instances of CWCT are now increasingly evident. Clearly, efforts to defend against such attacks is a meaningful allocation of resources in todays time rather than later. To use an analogy, the methods of the hijackers on September 11, 2001 would have seemed impossible before that date but not so much in the post 9/11 era! Likewise, exact threat vectors and modus operandi of cyber terrorists may not be known with any degree of certainty unless well provisioned intelligence, signaling and coordination mechanisms are put in place beforehand. The game analyzed in this paper demonstrates the need and benefit of having a governmental intelligence system as an integral part of defense against CWCT attacks on the critical infrastructure sector of our nation.

Spectacular CWCT attacks have been rare, covert or even suppressed. However, these attacks tend to leave a lasting mark on the human psyche, much more than the general crimes that occur regularly. CWCT has the potential to magnify the damage from a physical attack as well, and therefore there is a higher need to design systems to prevent these incidents. Added to the concern are the obvious vulnerability issues in our aging infrastructure assets which are now experiencing large scale open standard network connectivity with other business systems. We position and purpose our work to aid the current evolution of IT security architecture in the infrastructure sector - the backbone of all economic activites.

Notes

[1] One question we were asked in a seminar is the following: Suppose G spends k on intelligence gathering in period 1 and the attacker hatches a plan in period 2. What would be the effect of that alternate sequence?

In our model, the purpose of intelligence gathering is to learn the value of θ. So, it cannot be done before the value of θ is realized. Also, the attacker is not under any kind of compulsion to attack even if $\theta = 1$. Note that the decision to attack or not to attack is taken in period 3 after the government collects intelligence (in period 2), exactly as suggested by the question.

[2] For (26), it is important to recognize that the value of θ does not depend on k. In other words, whether or not an attacker hatches a plan depends on the characteristics of the equipment and his own skills. The purpose of intelligence gathering is to find out if the attacker has been successful in this attempt or not.

[3] For technical details, see Shaw (2013).

[4] It is also possible that the character of the equilibrium does not change. The results in this case can be derived

easily and are excluded from the discussion.

[5] Rogue implements and memory devices were utilized to initiate Stuxnet attack on the Iranian uranium centrifuges.

References

Arora, A., J. P. Caulkins and R. Telang. 2006. Sell First, Fix Later: Impact of Patching on Software Quality. Management Science 52(3): 465-471.

Bagchi, A. and J. A. Paul. 2014. Optimal Allocation of Resources in Airport Security: Profiling vs. Screening. Operations Research 62(2): 219-233.

Bandyopadhyay, T. and H. R. Mattord. 2008. Defending Cyber Terrorism – A Game Theoretic Approach. Proceedings of the American Conference on Information Systems, Toronto, Canada.

Campbell, K., L. A. Gordon, M. P. Loeb and L. Zhou. 2003. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security 11(3): 431-448.

Carter, C. J., P. Benson and M. Castillo. 2013. "Official: Cyberattacks, N. Korea, Jihadist Groups Top U.S. Threats," retrieved December 9, 2015, from

http://www.cnn.com/2013/03/12/us/threat-assessment/.

Cavusoglu, H., B. Mishra and S. Raghunathan. 2004. The Effect of Internet Security Breach Announcements on Market Value: Capital Market Reaction for Breached Firms and Internet Security Developers. International Journal of Electronic Commerce 9(1): 69-105.

Cavusoglu, H., S. Raghunathan and W. T. Yue. 2008. Decision-theoretic and game-theoretic approaches to IT security investment. Journal of Management Information Systems 25(2): 281-304.

Chancellor of the Exchequer HM Treasury. 2013. Spending Review. Retrieved March 20, 2014, from https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/

209036/spending-round-2013-complete.pdf.

Choi, J. P., C. Fershtman and N. Gandal. 2010. Network Security: Vulnerabilities and Disclosure Policy. Journal of Industrial Economics 58(4): 868-894.

Dacey, R. 2003. Critical infrastructure protection: Challenges in securing control systems, United States General Accounting Office

Denning, D. E. 2000. Cyberterrorism. Retrieved June 27, 2013, from

http://www.cs.georgetown.edu/~denning/infosec/cyberterror-GD.doc.

Denning, D. E. 2001. Activism, Hactivism, and Cyberterrorism: The Internet as a Tool for

Influencing Foreign Policy. Networks and Netwars. J. Arquilla and D. Ronfeldt, Rand Publications, USA. (Document # MR-1382-OSD).

Galloway, B. and G. P. Hancke. 2013. Introduction to Industrial Control Networks. Communications Surveys & Tutorials, IEEE 15(2): 860-880.

Gal-Or, E. and A. Ghose. 2005. The Economic Incentives for Sharing Security Information. Information Systems Research 16(2): 186-208.

Garg, A., J. Curtis and H. Halper. 2003. Quantifying the Financial Impact of IT Security Breaches. Information Management and Computer Security 11(2): 74-83.

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

Hausken, K. 2007. Information Sharing among Firms and Cyber Attacks. Journal of Accounting and Public Policy 26(6): 639–688.

Hua, J. and S. Bapna. 2013. The economic impact of cyber terrorism. Journal of Strategic Information Systems 22(2): 175-186.

Ingersoll, G. and M. B. Kelley. 2013. There's Only One Thing Stopping Enemy Nations From Smashing America's Power Grid. Business Insider Retrieved February 14, 2015,
from http://www.businessinsider.com/nations-had-electric-wmd-for-years-2013-2.

Miller, B. and D. Rowe. 2012. A survey SCADA of and critical infrastructure incidents. Proceedings of the 1st Annual conference on Research in information technology. Calgary, Alberta, Canada, ACM.

Nakashima, E. and J. Warrick. 2012. Stuxnet was work of U.S. and Israeli experts, officials say. Washington Post Retrieved February 14, 2015, from http://www.washingtonpost.com/world/
national-security/stuxnet-was-work-of-us-and-israeli-
experts-officials-say/2012/06/01/gJQAlnEy6U_story.html.

Nicholson, A., S. Webber, S. Dyer, T. Patel and H. Janicke. 2012. SCADA security in the light of Cyber-Warfare. Computers & Security 31(4): 418-436.

Office of the Director of National Intelligence. 2013. DNI Releases Budget Figure for 2013 National Intelligence Program. Retrieved March 18, 2014, from http://www.dni.gov/index.php/
newsroom/press-releases/191-press-releases-2013/957-dni-
releases-budget-figure-for-2013-national-intelligence-program?tmpl=component&format=pdf.

Paget, F. 2013. Hacking Summit Names Nations With Cyberwarfare Capabilities. Retrieved November 11, 2013, from http://blogs.mcafee.com/mcafee-labs/hacking-summit-names-nations-with-cyberwarfare-capabilities.

Patel, S. C., G. D. Bhatt and G. H. Graham. 2009. Improving the Cyber Security of SCADA Communication Networks. Communications of the ACM 52(7): 139-142.

Png, I. P. L. and Q.-H. Wang. 2009. Information Security: Facilitating User Precautions Vis-Ã -Vis Enforcement Against Attackers. Journal of Management Information Systems 26(2): 97-121.

Pollitt, M. M. 1997. Cyberterrorism: Fact or Fancy? Proceedings of the 20th National Information Systems Security Conference: 285-289.

Rollins, J. and C. Wilson. 2007. Terrorist Capabilities for Cyberattack: Overview and Policy Issues, Foreign Affairs, Defense and Trade Division, US Government.

Scully, T. 2011. The Cyber Threat, Trophy Information and the Fortress Mentality. Journal of Business Continuity & Emergency Planning 5(3): 195-207.

Shaw, W. T. 2013. SCADA System Vulnerabilities to Cyber Attack. Retrieved August 23, 2013, from http://www.electricenergyonline.com/?page=show_article&article=181.

U.S. Department of Defense. 2012. "Remarks by Secretary Leon E Panetta on Cybersecurity to the Business Executives for National Security, New York City," retrieved December 9, 2015, from http://archive.defense.gov/transcripts/transcript.aspx?transcriptid=5136.

Wheatcroft, P. 2010. "Cyber Terrorism is a real threat now," Wall Street Journal, retrieved December 9, 2015, from http://www.wsj.com/articles/SB10001424052748704103904575336703726142746.

Zhu, B., A. Joseph and S. Sastry. 2011. A Taxonomy of Cyber Attacks on SCADA Systems. Internet of Things (iThings/CPSCom), 2011 International Conference on and 4th International Conference on Cyber, Physical and Social Computing.

LIST OF TABLES AND FIGURES

NOTATION	DESCRIPTION
θ	Indicator variable that takes a value of 1 when the attacker hatches a plan, 0 otherwise
α	Probability of an attack (An attack is not feasible for $\theta = 0$)
p	Probability of hatching the plan, that is $\Pr(\theta = 1)$
s	Indicator variable that is a signal of θ: $s = 1$ when the government estimates that the attacker has hatched a plan, 0 otherwise
$\beta(s)$	Probability that the infrastructural firm will activate a state of alert reaching the RTU of its SCADA system given the signal s
b	Benefit received by the attacker from a cyber attack
c	Marginal cost of alert activation incurred by the infrastructual firm (defender)
k	expenditure made by the government to collect intelligence about the attacker's plans and activities
τ	cost incurred by the attacker for an attack
$\Pi_{ij}(k)$	Probability that $s = i$ and $\theta = j$, as a function of the expenditure k on intelligence
$\Lambda(k)$	Probability of a successful attack, as a function of the expenditure k on intelligence
A	The attacker
D	The infrastructural firm - the defender
G	The government of the country where D is situated
$L(b)$	Loss to D from an attack of cyber terrorism
T_i	Conditional payoff to the defender D subject to receiving signal $s = i$
$V(k)$	*Ex ante* expected payoff to the defender D as a function of the expenditure k on intelligence
ω	Cost imposed on the rest of the economy from each successful attack
$W(k)$	Social Welfare as a function of the expenditure k on intelligence
$U(k)$	*Ex ante* expected payoff to the government in the inspection stage under centralized security

Table 1: List of Notations

		Attacker ($\theta = 1$)		Attacker ($\theta = 0$)
		Attack	Do Not Attack	Do Not Attack
Firm	Activate alert	$-c,\ -\tau$	$-c,\ 0$	$-c,\ 0$
	Do not activate alert	$-L(b),\ b-\tau$	$0,\ 0$	$0,\ 0$

Table 2: The ex post payoffs in Period 3. The left panel shows the payoffs if $\theta = 1$ and the right panel shows the payoffs if $\theta = 0$.

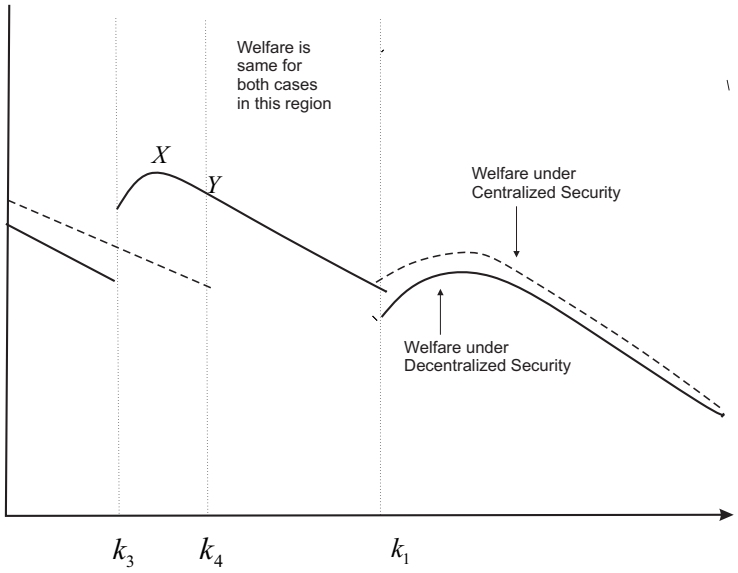

Figure 1: In the above diagram, the solid line depicts welfare under decentralized security and the dashed line depicts welfare under centralized security. Under decentralized security, welfare is maximized at X, while under centralized security, it is maximized at Y. Therefore, welfare is lower under centralized security.

Electronic Appendix

A Proof of Lemma 1

Conditional on having hatched a plan of attack, the chance of a successful attack is given by

$$\Pr(s=0|\theta=1;k)\{1-\beta(0)\}+\Pr(s=1|\theta=1;k)\{1-\beta(1)\}.$$

Noting that irrespective of success or failure, cost of attack τ accrues whenever the attacker chooses to attack, the expected payoff from an attack is given by

$$-\tau+b[\Pr(s=0|\theta=1;k)\{1-\beta(0)\}+\Pr(s=1|\theta=1;k)\{1-\beta(1)\}].$$

Further, the attacker gets a payoff of 0 if he does not attack. Hence, we have the result.

B Proof of Lemma 2

When the firm activates alert, then it always stops an attack, and consequently has a payoff of $-c$. When it does not activate a state of alert, then the firm suffers a loss $L(b)$ when the attack is launched. An attack will be launched if the attacker has a plan and chooses to use that plan to attack. Given the government's report s, the firm's estimate of the probability that the attacker has a plan is $\Pr(\theta=1|s)$. Hence, the firm estimates that the chance of an attack is $\Pr(\theta=1|s)\alpha$. Consequently given the firm's information, its expected payoff from not activating the state of alert is

$$-\Pr(\theta=1|s)\alpha L(b);\ i=1,2.$$

Hence, the result follows.

C Proof of Proposition 1

(i) The attack probability α follows from (10).

(ii) Suppose D receives the signal $s = 0$. By using (6) and (11), it follows that the left hand side of (9) is less than its right hand side, and hence the firm prefers not to activate alert. Therefore, we have the result.

(iii) Consider the firm's alert activation decision when $s = 1$. By applying a similar argument, it follows that the firm is indifferent between activating and not activating in this case. The result follows by substituting (12) into (8).

(iv) Suppose the government reports that the signal is $s = 0$. In this case, we already know that the firm never activates state of alert *i.e.*, $\beta(0) = 0$. Hence, the expected payoff to the infrastructural firm conditional on having observed a signal of 0 is

$$T_0 = \Pr(\theta = 0|s = 0; k)\, 0 - \Pr(\theta = 1|s = 0)\, \alpha L(b).$$

By substituting (11) in the above expression and then simplifying, we obtain the following:

$$T_0 = -\frac{\Pr(\theta = 1|s = 0; k)}{\Pr(\theta = 1|s = 1; k)} c.$$

When $s = 1$, the firm plays a mixed strategy. Therefore the firm is indifferent between activating and not activating state of alert. Since the payoff of the firm from activating state of alert is $-c$, therefore its *ex post* payoff must be $-c$. Hence, for the Type 1 Equilibrium,

$$T_1 = -c.$$

The *ex ante* expected payoff of the firm when the government spends k in intelligence gathering is therefore given by

$$V(k) = \Pr(s = 0; k)\, T_0 + \Pr(s = 1; k)\, T_1$$

which, upon simplification, can be re-written as (13).

(v) An attack is successful if *(a)* the terrorist has a plan (that is, $\theta = 1$), *(b)* and chooses to

attack using that plan and *(c)* the firm does not activate the state of alert. Hence,

$$\Lambda(k) = \Pr(\theta = 1)\alpha[\Pr(s = 1|\theta = 1; k)(1 - \beta(1)) + \Pr(s = 0|\theta = 1; k)(1 - \beta(0)]$$

which upon simplification can be re-written as (14).

D Proof of Proposition 2

(i) Suppose $k > k_1$. By the definition of k_1, it must be the case that

$$\Pr(s = 1|\theta = 1; k) > 1 - \frac{\tau}{b}.$$

Given the values of $\beta(1)$ and $\beta(0)$, it follows that the left hand side of (8) is $\Pr(s = 1|\theta = 1; k)$ while the right hand side is $\left(1 - \frac{\tau}{b}\right)$. Hence for $k > k_1$, the left hand side is greater than the right hand side. Therefore, it follows from Lemma 1 that $\alpha = 0$. However, in that case, $\Pr(\theta = 1|s = 1; k)\alpha = 0 < \frac{c}{L(b)}$ and that violates (17). Therefore, we cannot have an equilibrium of type 2 when $k > k_1$.

When $k < k_1$, then the following inequality holds:

$$\Pr(s = 1|\theta = 1; k) < 1 - \frac{\tau}{b}.$$

In such a case, it follows from Lemma 1 that

$$\alpha = 1.$$

(ii) and *(iii)*: Follows from Lemma 2 and (17).

(iv) The expected payoff conditional on having observed a signal of 0 is

$$T_0 = -\Pr(\theta = 1|s = 0) L(b).$$

When $s = 1$, the firm always activates the state of alert. Therefore, for the Type 2 Equilibrium,

$$T_1 = -c.$$

Hence, the *ex ante* expected payoff of the firm when the government spends k in intelligence gathering is given by

$$V(k) = \Pr(s = 0; k)\, T_0 + \Pr(s = 1; k)\, T_1$$

which upon simplification reduces to (18).

(v) The probability of a successful attack $\Lambda(k)$ can be calculated as follows:

$$\begin{aligned} & \Lambda(k) \\ = \; & \Pr(\theta = 1)[\Pr(s = 1|\theta = 1; k)(1 - \beta(1)) + \Pr(s = 0|\theta = 1; k)(1 - \beta(0)] \\ = \; & \Pr(\theta = 1)\Pr(s = 0|\theta = 1; k) \end{aligned}$$

and this upon simplification yields (19).

E Statement and Proof of Proposition 8

Proposition 8 *In the type* 3 *equilibrium, the following results hold:*

(i) If a plan is hatched, then the attacker attacks with probability

$$\alpha = \frac{1}{\Pr(\theta = 1|s = 0; k)} \frac{c}{L(b)}. \tag{29}$$

(ii) If the firm receives a signal of $s = 0$*, then its alert activation probability is*

$$\beta(0) = \frac{\left(\frac{b-\tau}{b}\right) - \Pr(s = 1|\theta = 1; k)}{\Pr(s = 0|\theta = 1; k)}.$$

(iii) If the firm receives a signal of $s = 1$*, then it always activates the state of alert, that is,*

$$\beta(1) = 1.$$

(iv) The ex ante expected payoff of the firm when the government spends k in intelligence gathering is given by

$$V(k) = -c. \tag{30}$$

(v)The ex ante probability of a successful attack is given by

$$\Lambda(k) = \Pr(\theta = 1)\frac{1}{\Pr(\theta = 1|s = 0; k)}\frac{c}{L(b)}\frac{\tau}{b}. \tag{31}$$

Proof. *(i)* The attack probability of the terrorist follows from (20).

(iii) The result follows from (9) and (20).

(ii) Using (20), it follows that the left hand side of (9) is equal to its right hand side. Hence, the firm is indifferent between activating and not activating the state of alert when it receives a report of $s = 0$ from the government. The result then follows from (8).

(iv) Suppose the government reports that the signal is $s = 0$. In this case, the firm plays a mixed strategy. Therefore the firm is indifferent between activating and not activating the state of alert. Since the payoff of the firm from activating the state of alert is $-c$, therefore its *ex post* payoff must be $-c$. Hence, for the Type 3 Equilibrium,

$$T_0 = -c.$$

On the other hand, when $s = 1$, the firm always activates the state of alert. Hence, for the Type 3 Equilibrium,

$$T_1 = -c.$$

Hence, the result follows.

(v) The probability of a successsful attack when equilibrium is of Type 3 is given by,

$$\Lambda(k) = \Pr(\theta = 1)\alpha[\Pr(s = 1|\theta = 1; k)(1 - \beta(1)) + \Pr(s = 0|\theta = 1; k)(1 - \beta(0)]$$

which simplifies to (31). ■

Now, let us examine the parametric conditions under which this equilibrium occurs. The at-

tacker's probability of attack cannot exceed 1. Hence, we must have the following restriction:

$$\Pr(\theta = 1|s = 0; k) \geq \frac{c}{L(b)}.$$

Further, it must be the case that $\beta(0) \leq 1$, and this is satisfied if (5) holds. Finally, it must be the case that $\beta(0) \geq 0$ and therefore, the following inequality must be satisfied:

$$\Pr(s = 1|\theta = 1; k) \leq 1 - \frac{\tau}{b}.$$

Combining all of these inequalities, it follows that the equilibrium is of type 3 if

$$\Pr(\theta = 1|s = 0; k) \geq \frac{c}{L(b)} \text{ and } \Pr(s = 1|\theta = 1; k) \leq 1 - \frac{\tau}{b} \tag{32}$$

are both satisfied. By comparing (16) and (32), it follows that $k_3 \leq k_1$.

F Proof of Proposition 3

Suppose $k > k_1$. Substitute (13) and (14) into the expression for $W(k)$ to obtain the following:

$$\begin{aligned} W(k) &= V(k) - \omega\Lambda(k) - k \\ &= -\frac{\Pr(\theta = 1)}{\Pr(\theta = 1|s = 1; k)} c - \omega \frac{\Pr(\theta = 1)}{\Pr(\theta = 1|s = 1; k)} \frac{c}{L(b)} \frac{\tau}{b} - k \\ &= -\frac{\Pr(\theta = 1)}{\Pr(\theta = 1|s = 1; k)} \left[1 + \omega \frac{1}{L(b)} \frac{\tau}{b}\right] c - k. \end{aligned}$$

Now suppose $k_3 < k < k_1$. Substitute (18) and (19) into the expression for $W(k)$ to obtain the following:

$$\begin{aligned} W(k) &= V(k) - \omega\Lambda(k) - k \\ &= -\Pi_{01}(k)(L(b) - c) - \Pi_{10}(k) c - \Pr(\theta = 1) c - \Pi_{01}(k) \omega - k \\ &= -\Pi_{01}(k)(L(b) + \omega - c) - \Pi_{10}(k) c - \Pr(\theta = 1) c - k. \end{aligned}$$

Finally suppose $k < k_3$. Substitute (30) and (31) into the expression for $W(k)$ to obtain the

following:

$$\begin{aligned} W(k) &= V(k) - \omega\Lambda(k) - k \\ &= -c - \omega\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=0;k)}\frac{c}{L(b)}\frac{\tau}{b} - k \\ &= -\left[1 + \omega\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=0;k)}\frac{1}{L(b)}\frac{\tau}{b}\right]c - k. \end{aligned}$$

G Proof of Lemma 3

It follows from (22) that for $k < k_3$,

$$W'(k) = \omega\frac{\Pr(\theta=1)}{[\Pr(\theta=1|s=0;k)]^2}\frac{c}{L(b)}\frac{\tau}{b} \times \frac{\partial}{\partial k}\Pr(\theta=1|s=0;k) - 1.$$

Using (4), it follows that $W'(k) < 0$ for $k < k_3$. Hence the result follows.

H Proof of Corollary 1

Let us first compare $W(k_1)$ with $W(0)$. Note that

$$\begin{aligned} & W(k_1) - W(0) \\ = & -\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k_1)}\left[1 + \omega\frac{1}{L(b)}\frac{\tau}{b}\right]c - k_1 - W(0) \\ = & \frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k_1)}W(0) - k_1 - W(0) \\ = & \left[1 - \frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k_1)}\right]|W(0)| - k_1. \end{aligned} \tag{33}$$

It can be shown that $\frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k_1)} < 1$ when (24) is satisfied. Hence if (24) and (25) hold, then (33) is positive.

Now observe the following chain of inequalities:

$$\begin{aligned} W(k^*) - W(0) &\geq W(k_1) - W(0) \\ &= \left[1 - \frac{\Pr(\theta=1)}{\Pr(\theta=1|s=1;k_1)}\right]|W(0)| - k_1. \end{aligned}$$

Hence the result follows.

I Proof of Proposition 5

By the implicit function theorem, it follows that

$$\frac{\partial k^*}{\partial p} = -\frac{\frac{\partial^2 W(k^*)}{\partial k \partial p}}{\frac{\partial^2 W(k^*)}{\partial k^2}}.$$

Since $W''(k) < 0$, therefore,

$$sign\left(\frac{\partial k^*}{\partial p}\right) = sign\left(\frac{\partial^2 W(k^*)}{\partial k \partial p}\right).$$

In order to evaluate $\frac{\partial^2 W(k^*)}{\partial k \partial p}$, note that

$$\Pi_{01}(k) = \Pr(s = 0|\theta = 1; k) \Pr(\theta = 1),$$

$$\Pi_{10}(k) = \Pr(s = 1|\theta = 0; k) \Pr(\theta = 0)$$

and

$$\Pr(\theta = 0) = 1 - \Pr(\theta = 1).$$

Using the above relationships, it follows from (26) that

$$\begin{aligned}\frac{\partial^2 W(k^*)}{\partial k \partial p} &= -\frac{\partial}{\partial k} \Pr(s = 0|\theta = 1; k) [L(b) + \omega - c] \\ &\quad + \frac{\partial}{\partial k} \Pr(s = 1|\theta = 0; k) c\end{aligned}$$

for $k^* \in (k_3, k_1)$. In the above expression, the first term is positive while the second term is negative. Hence, $\frac{\partial^2 W(k^*)}{\partial k \partial p} > 0$ if the first term dominates. However, it is also possible that $\frac{\partial^2 W(k^*)}{\partial k \partial p} < 0$ if the second term dominates. In the former case $\frac{\partial k^*}{\partial p} > 0$, while in the latter case, $\frac{\partial k^*}{\partial p} < 0$.

Now consider the effect of a reduction in p on welfare. Notice that

$$\frac{dW(k^*)}{dp} = \frac{\partial W(k^*)}{\partial p} + W'(k^*) \frac{\partial k^*}{\partial p}.$$

However, by the first order condition, $W'(k^*) = 0$. Therefore, it follows from (22) that

$$\begin{aligned}\frac{dW(k^*)}{dp} &= -\Pr(s=0|\theta=1;k^*)[L(b)+\omega-c] \\ &\quad -\Pr(s=1|\theta=0;k^*)c-c \\ &= -\Pr(s=0|\theta=1;k^*)[L(b)+\omega] \\ &\quad -\{\Pr(s=1|\theta=1;k^*)-\Pr(s=1|\theta=0;k^*)\}c\end{aligned}$$

for $k^* \in (k_3, k_1)$. The first term is negative, while the second term has an ambiguous sign. If (27) holds, then it can be shown that

$$\Pr(s=1|\theta=1;k^*) > \Pr(s=1|\theta=0;k^*).$$

In this case, the second term is also negative. Hence $\frac{dW(k^*)}{dp} < 0$ if (27) holds.

J Proof of Proposition 6

We provide a sketch of the proof here. First, note from (16) that the following equality holds at k_1:

$$\Pi_{11}(k_1) = \left(1 - \frac{\tau}{b}\right)p.$$

Since $\Pi'_{11}(k) > 0$, therefore a decrease in p decreases k_1. Consider Figure 2. Suppose $k_1 = k_1^0$ initially. In the alert activation subgame, the equilibrium is of type 1 for $k > k_1^0$ and is of type 2 for $k < k_1^0$. Therefore, the welfare function is given by AB for $k < k_1^0$ and CD for $k > k_1^0$. Notice that welfare is maximized at X and thus the equilibrium will be of type 2 in the alert activation subgame.

Now consider the effect of a lowering of vulnerability, that is, a decrease in p. This reduces k_1 to k_1^1. Now the welfare function is given by $A'E'$ for $k < k_1^1$ and $F'D'$ for $k > k_1^1$. As a result, welfare is now maximized at Y' and in the alert activation subgame, the equilibrium switches to type 1. Therefore, a lowering of vulnerability can change the nature of the equilibrium from type 2 to type 1.

This means that in such a situation, the expenditure on intelligence increases (from X to Y')

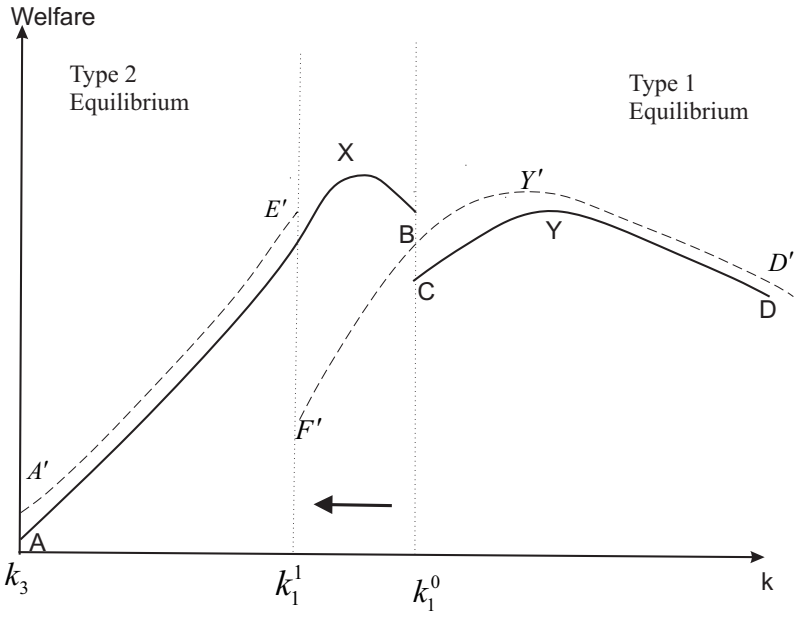

Figure 2: At the initial level of vulnerability, the welfare function is drawn using the solid lines. After the reduction in vulnerability, the welfare function is drawn using the dashed lines. The major takeaway from the diagram is the following: At the initial level of vulnerability, welfare is maximized at X. After a decrease in the degree of vulnerability, X is no longer feasible and welfare is instead maximized at Y'.

in response to decreased system vulnerability. Finally, note that in this situation, there is also a reduction in welfare in response to a decrease in vulnerability.

K Proof of Proposition 7

We provide a sketch of the proof here. Suppose $\frac{\tau}{b}$ is low enough such that $\Pr(s=1|\theta=1;k) < 1-\frac{\tau}{b}$ at $k=k_3$. Then, note from (21) that the following equality holds at k_3:

$$\Pr(\theta=1|s=0;k_3) = \frac{c}{L(b)}.$$

Since $\Pr(\theta=1|s=0;k)$ is a decreasing function of k, therefore a decrease in c increases k_3. Consider Figure 3. Suppose $k_3 = k_3^0$ initially. In the alert activation subgame, the equilibrium is of type 1 for $k > k_1$ and is of type 2 for $k_3^0 < k < k_1$. Therefore, the welfare function is given by AB for $k_3^0 < k < k_1$ and CD for $k > k_1$. Notice that welfare is maximized at X and thus the equilibrium is of type 2 in the alert activation subgame.

Now consider the effect of a decrease in the alert activation cost c. This increases k_3 to k_3^1. Now the welfare function is given by $E'B'$ for $k_3^1 < k < k_1$ and $C'D'$ for $k > k_1$. As a result, welfare is now maximized at Y' and in the alert activation subgame the equilibrium switches to type 1. Therefore, a decrease in the alert activation cost can change the nature of the equilibrium.

This means that in such a situation, the expenditure on intelligence increases in response to a decrease in the alert activation cost. Finally, note that in this situation, there is also a reduction in welfare in response to a decrease in the alert activation cost.

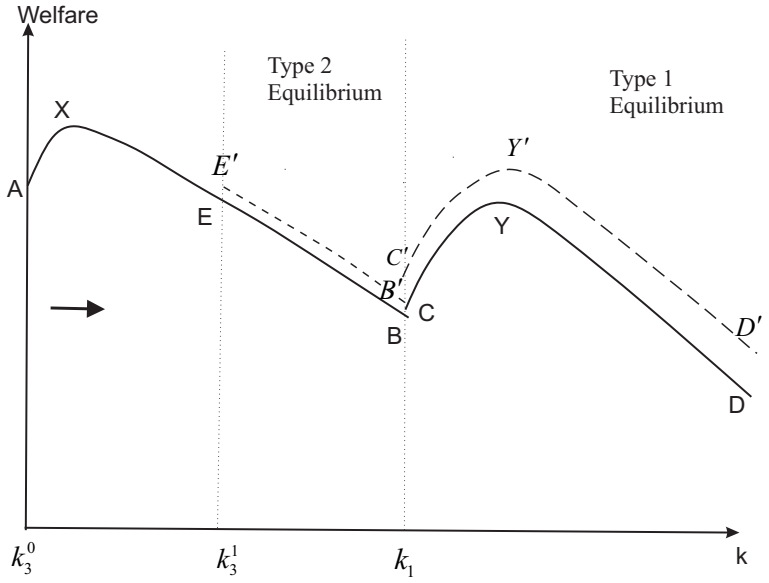

Figure 3: At the initial level inspection cost, the welfare function is given by the solid line. After the reduction in inspection cost, the welfare function is given by the dashed line. The major takeaway from the diagram is the following: Initially, welfare is maximized at X. After a decrease in the cost of inspection, X is no longer feasible and welfare is instead maximized at Y'.

L Increase in loss to the infrastructural firm

Below, we consider the impact of an increase in the infrastructural firm's loss function $L(b)$. That is, we now consider a scenario in which the loss L to the infrastructural firm is greater for the same benefit b to the terrorist.

L.0.1 Equilibrium is of type 2 before and after the increase in $L(b)$

Notice from (26) that

$$\frac{\partial^2 W(k^*)}{\partial k \partial L(b)} = -\Pi'_{01}(k) > 0$$

for $k^* \in (k_3, k_1)$. Therefore, when the equilibrium is of type 2, then an increase in the infrastructural firm's loss from a successful attack increases the optimal level of expenditure on intelligence. It also follows from (22) that

$$\frac{dW(k^*)}{dL(b)} = -\Pi_{01}(k) < 0$$

for $k^* \in (k_3, k_1)$. Thus, welfare decreases in this case.

L.0.2 Equilibrium is of type 1 before and after the increase in $L(b)$

The key result in this case is summarized in the proposition below.

Proposition 9 *Suppose there is an increase in the loss function $L(b)$ of the infrastructural firm such that the equilibrium is type 1 (large expenditure on intelligence) both before and after the increase. This leads to a decrease in the expenditure on intelligence and an increase in welfare.*

Proof. Following the same steps as above, it can be shown that when the equilibrium is of type 1, then $\frac{\partial k^*}{\partial L(b)} < 0$, that is an increase in the loss of the infrastructural firm from a cyber-attack leads to a decrease in the optimal expenditure on intelligence.

Further,

$$\frac{dW(k^*)}{dL(b)} = \frac{\Pr(\theta = 1)}{\Pr(\theta = 1 | s = 1; k)} \omega \frac{1}{[L(b)]^2} \frac{\tau}{b} c > 0$$

for $k^* \in (k_1, \infty)$. Thus in this case, social welfare increases when there is an increase in the loss of the infrastructural firm. ■

Both of these results are counter to what one might expect. One might think that these results hold because of an increase in the alert activation probability following higher loss. However, that intuition is not correct. Indeed, in this equilibrium, the probability of alert activation (given a signal) does not change in response to an increase in $L(b)$. The correct intuition instead is as follows: In the mixed strategy equilibrium, the attacker makes the infrastructural firm indifferent between activating and not activating the state of alert when the reported signal is 1. When there

is an increase in the loss to the firm, then everything else remaining constant, the firm prefers to activate the state of alert. Knowing this, the attacker then responds by reducing the probability of attack in order to restore indifference.

L.0.3 Equilibrium is of type 2 initially and is of type 1 after the increase in $L(b)$

Following similar steps as in the discussion of the reduction in c, it can be shown that an increase in $L(b)$ increases k_3. Hence using a similar argument as in Proposition 7, it can be shown that in such a situation, it is possible for the expenditure on intelligence to increase and welfare to reduce in response to an increase in $L(b)$.