Risk Analysis, Vol. 36, No. 4, 2016 DOI: 10.1111/risa.12362

Defense of Cyber Infrastructures Against Cyber-Physical Attacks Using Game-Theoretic Models

Nageswara S. V. Rao,[1,*] Stephen W. Poole,[1] Chris Y. T. Ma,[2] Fei He,[3] Jun Zhuang,[4] and David K. Y. Yau[5]

The operation of cyber infrastructures relies on both cyber and physical components, which are subject to incidental and intentional degradations of different kinds. Within the context of network and computing infrastructures, we study the strategic interactions between an attacker and a defender using game-theoretic models that take into account both cyber and physical components. The attacker and defender optimize their individual utilities, expressed as sums of cost and system terms. First, we consider a Boolean attack-defense model, wherein the cyber and physical subinfrastructures may be attacked and reinforced as individual units. Second, we consider a component attack-defense model wherein their components may be attacked and defended, and the infrastructure requires minimum numbers of both to function. We show that the Nash equilibrium under uniform costs in both cases is computable in polynomial time, and it provides high-level deterministic conditions for the infrastructure survival. When probabilities of successful attack and defense, and of incidental failures, are incorporated into the models, the results favor the attacker but otherwise remain qualitatively similar. This approach has been motivated and validated by our experiences with UltraScience Net infrastructure, which was built to support high-performance network experiments. The analytical results, however, are more general, and we apply them to simplified models of cloud and high-performance computing infrastructures.

KEY WORDS: Cyber infrastructures; cyber-physical networks; game theory

1. INTRODUCTION

The operation of infrastructures that provide cyber services, such as network connectivity and computing capacity, requires the continued functioning of: (i) *cyber components* such as computers, routers, and switches, and (ii) *physical components* such as fiber routes, cooling, and power systems. While these infrastructures are built to provide cyber services, their operation is "cyber-physical" in nature due to its dependence on both cyber and physical components. For example, the components may be degraded by factors such as incidental (weather-related) power failures and device fatigue failures as well as deliberate cyber attacks on computers and physical attacks on fiber routes. While cyber attacks on computing systems and networks seem to get more public media attention, in many occasions the infrastructure degradations have been due to physical factors such as power blackouts and backhoe incidents on fiber routes. Indeed, these cyber

[1] Computer Science and Mathematics Division, Oak Ridge National Laboratory, Oak Ridge, TN, USA.

[2] Advanced Digital Sciences Center, Singapore.

[3] Department of Mechanical and Industrial Engineering, Texas A&M University–Kingsville, Kingsville, TX, USA.

[4] Department of Industrial and Systems Engineering, State University of New York, Buffalo, NY, USA.

[5] Department of Computer Science, Singapore University of Technology and Design, Singapore.

[*] Address correspondence to Nageswara S. V. Rao, Computer Science and Mathematics Division, Oak Ridge National Laboratory, Oak Ridge, TN 37831, USA; raons@ornl.gov.

infrastructures can be compromised by attacks on physical components such as heating, ventilation, and air conditioning (HVAC) systems, power-supply lines, and physical fiber connections; in particular, the latter two are typically routed through long stretches of unprotected areas, making them vulnerable to physical attacks. Consequently, the design and operation of these infrastructures must strike a balance between the cost of such degradations based on estimates and empirical data, in particular attacks, and the benefits of infrastructure reinforcements on the overall performance. In this article, we present game-theoretic models that capture the interactions between an attacker and a defender to support rigorous design and analysis of a class of cyber infrastructures that consists of network and computing components. These constitute a subclass of more general infrastructures such as monitoring and control networks for the energy grid, intelligent transportation systems, nuclear plants, and hydroelectric dams; in the latter, in particular, cyber attacks can degrade physical capabilities, in addition to physical attacks degrading the cyber capabilities.

The provider of these cyber infrastructures has to account for both cyber and physical intentional degradations, namely, attacks, in addition to natural and incidental degradations. Our work is motivated by experiences with UltraScience Net (USN),[1] which is a cross-country 10 Gbps network infrastructure built in 2004 for supporting the testing of high-performance network solutions. Somewhat surprisingly, all major service outages of USN have been due to noncyber incidents, such as fiber cuts and power outages, which highlights the dependence of cyber infrastructures on physical components. There have been many attack attempts on USN cyber components, and the firewalls combined with control-plane encryption prevented them from developing into service outages. Consequently, the operation of USN required a systematic, analytical way to counter such physical incidents, in addition to cyber measures to protect the network devices and hosts. The game-theoretic models in this article encompass the cyber-physical aspects of USN infrastructure, and in addition are generally applicable to cloud computing infrastructure (CCI) and high-performance computing infrastructure (HPCI). The successful operation of USN for six years under the requirement of no more than two outages per year indicates the validity and effectiveness of rather simple game-theoretic models.

We consider a class of cyber infrastructures modeled as discrete systems of cyber and physical components, which are subject to incidental degradations, and attacks that could lead to service interruptions. The provider or defender is charged with reinforcing the infrastructure parts or components to defend against the degradations of both kinds. These infrastructures are characterized by the following considerations:

(1) Knowledge about the capabilities and locations of the infrastructure is available to the attacker, primarily from the information provided to facility users;
(2) Knowledge about incidental degradations is available to both parties, primarily from public sources;
(3) Actual costs incurred by the defender and attacker are private information and not available to the other; and
(4) Strategies used by the defender in choosing which parts to reinforce and by the attacker in choosing which parts to attack are not revealed to the other.

These considerations lead to game-theoretic models where objectives of the attacker and defender contain common terms corresponding to items (1) and (2), and private terms corresponding to items (3) and (4). We only consider the attacks that immediately disrupt the cyber services provided by the infrastructure, and do not consider those that primarily steal information, or plant malicious codes to attack others (using only a small amount of resources). Due to item (4), both defender and attacker consider that the other employs a probabilistic strategy (deterministic strategy is a special case). Our main objective is to gain an understanding of the interactions to help ensure the infrastructure survival in the presence of cyber and physical degradations within the framework of game theory.[2–4]

We consider that the attacker chooses between cyber and physical parts, and the defender reinforces both cyber and physical parts. Both attacks and reinforcements have a certain probability of success, and additionally the infrastructure is subject to incidental degradations. The utility functions of the attacker and defender are sums of cost and system terms, where the latter represents the "benefit" of the degradation and continued operation for the attacker and provider, respectively. We first consider a simplified model where the cyber and physical parts are treated as single subinfrastructures, and then consider that each consists of several discrete components. In each case, we compute the Nash equilibrium (NE) that represents the attacker and defender actions based on their utility functions, from which neither has a motivation to unilaterally deviate. Despite the probabilistic strategies, we show that NE is deterministic in that underlying probabilities are either 0 or 1, from which the survival status of the infrastructure can be inferred. Furthermore, if the costs depend only on the number of components n, NE can be computed with polynomial time complexity in n. The performance degradations of the infrastructure at NE, including a complete shutdown, depend on further details of reinforcement and attack strategies. We also incorporate the probabilities of successful attack and defense of components, and also the probabilities of their incidental failures. In the latter case, the attacker is at a certain advantage under incidental degradations, but otherwise the game-theoretic results remain qualitatively similar.

We first describe the USN infrastructure and our experiences that led to the game-theoretic analysis described in this article. We then consider CCI and HPCI, which represent two different ways of providing computing capabilities to users. In the former, computing servers are distributed at various sites over the Internet, and in the latter computing power is concentrated at specific supercomputing facilities connected over high-performance networks. We apply the above game-theoretic methods to infer conditions for the survival of these infrastructures at NE, and derive the expected performance levels under statistical independence conditions. Our results show that the cloud computing provider can hide and exploit the information about the distribution of servers at various sites to improve the expected performance against the attacker.

The organization of this article is as follows. In Section 2, we briefly compare our formulation with related works within a broad context. In Section 3, we first describe USN infrastructure, and then describe simplified models of CCI and HPCI. In Section 4, we present our game-theoretic formulation and discuss NE conditions for the subinfrastructure attack-defense model in Section 4.1 and the component attack-defense model in Section 4.2; we incorporate the probabilities of successful attacks and reinforcements in Section 4.3. In Section 5, we discuss the CCI and HPCI.

Table I presents the notation used in the article.

2. RELATED WORK AND THE CONTRIBUTION OF THIS ARTICLE

Since the terrorism attacks on September 11, 2001, there has been a growing literature on attacker-defender games; see Ref. 5 for a recent edited book and see Ref. 6 for a recent review article on this topic. This line of research starts with single-period,[7] single-target,[8] complete information[7] models, and then extends to multiple-period,[9,10] multiple-target,[7,11,12] and incomplete information[8,13–15] models.

In addition to being applied to counterterrorism literature, game theory has also been applied to study the strategic interactions in cyber security problems,[16–19] mostly between the hackers and defenders (company, system operators). For example, the hackers could steal system/customer information and plant stealthy malicious codes, while the defender could purchase antivirus software as well as use "honeypots" to track hackers.[20–22] Some strategic interactions between the third party (e.g., government who may provide subsidy) and the multiple defenders in interdependent security networks have also been studied.[23,24]

Note that most of the above works on cyber security are limited to the space of cyber infrastructure parts, not touching the space of physical parts. However, cyber infrastructures often integrate and interact with physical ones; and such integration and interaction have been documented in the literature of cyber-physical systems.[25–27] For example, Refs. 28 and 29 study the interdependence between the cyber and physical components.

To our best knowledge, none of the previous game-theoretical works explicitly study the strategic interactions between the attackers and defenders in complex cyber-physical systems, which are essential and critical in practice.[28] This article fills this gap by using a single-period, multiple-component, and complete-information game to study the optimal level of defenses on cyber, physical, and combined parts of infrastructures that provide network and computing services,[30] facing adaptive adversaries.

For tractability and simplicity, this article focuses on modeling discretized cyber and physical components. These models are simpler than some complex models used in power distribution, transportation, and telecommunication critical infrastructures,[31–33] where the systems are characterized by continuous

Table I. Notation

Notation	Explanation
Infrastructure parameters:	
$i = c, p, cp$	Index of cyber, physical, and combined part, respectively
$n_i, i = c, p$	Number of components in part i
$k_i, i = c, p$	Minimum number of components of part i needed for infrastructure
$f_U(n_c, n_p, x_c, x_p, y_c, y_p)$	robustness fraction
Defender's variables:	
N_D	Action set of defender
G^D	Gain matrix of defender
C^D	Cost matrix of defender
S^D	System matrix of defender
$x_i, i = c, p$	Number of components defended or reinforced in part i
Attacker's variables:	
N_A	Action set of attacker
G^A	Gain matrix of attacker
C^A	Cost matrix of attacker
S^A	System matrix of attacker
$y_i, i = c, p$	Number of components attacked in part i
Decision variables:	
Q_D	Defender's probability vector
Q_{SD}	Defender's probability vector with defense success probabilities incorporated
$Q_{SD-\delta}$	Defender's probability vector with defense success probabilities and incidental failure probabilities incorporated
P_A	Attacker's probability vector
P_{SA}	Attacker's probability vector with attack success probabilities incorporated
$P_{SA+\delta}$	Attacker's probability vector under attack success probabilities and incidental failure probabilities incorporated
Utilities:	
$U_D(P_A, Q_D)$	Defender's utility
$U_A(P_A, Q_D)$	Attacker's utility

parameters and dynamics, and the underlying problems may involve solving differential equations.[34] For continuous systems, the computation of optimum strategies is much more complex, and could be in the complexity class of polynomial parity arguments on directed graphs (PPAD)-complete.[35] By contrast, as a result of the uniform cost formulation, the complexity of NE computation for this article is polynomial time, which is much more effective in practice.

3. CYBER INFRASTRUCTURES

In this section, we first describe USN network infrastructure and then describe two simplified models of CCI and HPCI.

3.1. UltraScience Net

USN is a wide-area network testbed that provides suites of 10 Gbps connections of several thousands of miles in support of high-performance network tests.[1] USN infrastructure consists of a data-plane of two parallel OC192 connections with co-location sites at Oak Ridge, Chicago, Seattle, and Sunnyvale, as shown in Fig. 1.[6]

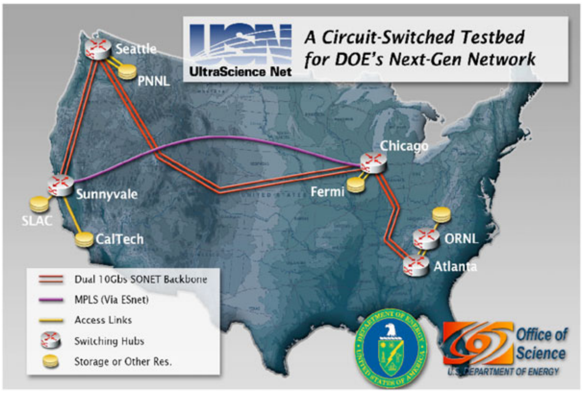


Fig. 1. USN consists of dual 10 Gbps lambdas from Oak Ridge to Chicago to Seattle to Sunnyvale.

[6] USN was commissioned by the Department of Energy in 2004, and has been supported by the Department of Defense since

At each site, a Linux host supports the users, and an additional control workstation at Oak Ridge provides remote management and configuration of the entire network via a secure control-plane, which is physically separated from the data-plane. At each site, all devices are behind a local firewall, and secure encrypted tunnels between the firewalls carry the control traffic between the sites. The hosts are restricted to execute a limited set of user transport codes, and in particular, they do not run e-mail and web service codes. USN is an experimental testbed used mainly by network researchers with a somewhat modest service requirement of no more than two service outages in a year. The small number of hosts with very limited functionality combined with highly restrictive control-plane firewall rules resulted in no service outages due to cyber incidents. However, an increasing number of intrusion attempts have been recorded by the firewall logs at all sites over the years, including port scans and login attempts. All USN service interruptions have been due to noncyber incidents, including the following incidents during 2004–2010:

(1) **Fiber Disruptions:** A small-engine airplane crashed into the fiber route between Chicago and Oak Ridge nodes, which disconnected both data- and control-planes. Also, two incidents of fiber outages between Chicago and Seattle nodes disconnected the data-plane.
(2) **Device Failures:** There have been three linecard failures that led to data-plane disruptions, and a switch failure in the control-plane at Sunnyvale node.
(3) **Power Disruptions:** There have been four power interruptions at Oak Ridge node, which disconnected the data-plane at Oak Ridge and also brought down the entire control-plane.

A careful analysis of the frequency of these incidents became necessary to ensure no more than two service outages per year, which in turn led to our game-theoretic formulation (presented in the next section). Overall, the operational performance over a period of six years at this service level justifies the utilization of the game-theoretic models and analysis, even though they are somewhat simple.

3.2. Computer Infrastructure Models

We now consider CCI and HPCI, which represent two different ways of providing computing capabilities to users. CCIs provide commodity computing capacity using servers possibly distributed over the Internet, wherein the user is typically unaware of the location of servers that execute the task. HPCIs make available supercomputers to users, who typically execute their code on specific systems.

3.2.1. Cloud Computing Infrastructure

Collections of computing servers may be deployed at multiple sites over the Internet to provide a specified level of aggregated computing capacity to users connected to the Internet. Typically, the details about the number and types of servers at any particular site are not disclosed. The tasks submitted by users are scheduled on the available servers, typically at locations unknown and not easily predictable by users. Cyber attacks could be launched remotely on the servers or gateway routers, and physical attacks could be launched on fiber connections or power lines to server sites. A physical disruption of the fiber or cyber disruption of the gateway router makes all servers at that site unavailable, and a cyber attack on all servers at this site will also have the same effect. In addition, the server sites are subject to incidental disruptions of the physical plant and power-supply systems. The provider can reinforce the cyber parts by replicating the servers and deploying fail-over gateway routers. The physical parts can be reinforced using redundant diverse fiber and power connections, and redundant HVAC systems. The total computing power of all servers that are up and connected to the Internet is the *available capacity*, and is a performance measure of this infrastructure.

3.2.2. High-Performance Computing Infrastructure

HPCIs consist of supercomputers at multiple sites, connected to high-speed networks via fiber connections. Information about such facilities deployed for open research projects, such as those by the Department of Energy and the National Science Foundation, is publicly available. Users of such facilities typically submit jobs to be executed on specific supercomputers. In general, supercomputer sites provide redundant power and HVAC systems to protect against single failures. But, targeted cyber attacks

2007. The 10 Gbps infrastructure was decommissioned in 2010, and is currently being upgraded to 40/100 Gbps with a different footprint.

on supercomputers or gateway routers can render these facilities unavailable. Also, physical attacks on fiber connections can render them unreachable, and multiple attacks on power lines can bring down these facilities (since backup power is generally utilized for smooth shutdowns rather than sustained operations). In terms of reinforcements, fiber connections and gateway routers may be replicated and configured to support fail-overs, and firewall capabilities may be reinforced to protect against cyber attacks. For a given HPCI, the number of supercomputers that are operational and connected to the network is a measure of its infrastructure performance.

Despite the apparent differences in the type of computing services provided, the underlying infrastructures of CCI and HPCI are quite similar, and they both can be studied using the game-theoretic method described in the next section. While the overall survival of these infrastructures can be inferred from NE conditions of the game-theoretic models, further details need to be taken into account to assess their performance levels, as will be described in Section 5.

4. GAME-THEORETIC ANALYSIS

In this section, we first consider the Boolean attack-defense model for cyber and physical subinfrastructures or parts, followed by the discrete case where each part consists of multiple components. We also consider that both cyber and physical parts of the system are subject to incidental degradations. An attacker is aware that both cyber and physical components are essential for the operation of the infrastructure and chooses to attack only one of them.[7] On the other hand, the provider would reinforce both cyber and physical parts.

4.1. Subinfrastructure Attack-Defense Model

We consider that the defender and attacker make Boolean choices of defending and attacking the cyber and physical subinfrastructures as individual units.

- Defender's action set is $N_D = \{cp, 0\}$, where cp represents reinforcing both cyber and physical parts, and 0 represents no reinforcement. The corresponding probability vector is $Q_D = [q_{cp} \quad 1 - q_{cp}]$, where q_{cp} is the probability that both parts are reinforced.
- Attacker's action set is $N_A = \{c, p, 0\}$, where c and p represent attacking cyber and physical parts, respectively, and 0 represents no attack. The corresponding probability vector is $P_A = [p_c \quad p_p \quad 1 - p_c - p_p]$, where $p_i, i = c, p$, is the probability that part i is attacked.

The utility function of the attacker is the sum of (i) a *cost term* representing the cost of launching an attack, and (ii) a *system performance term* representing the benefit of rendering the system nonoperational.[30,37] The utility function is expressed using a gain matrix G^A consisting of cost matrix C^A and system matrix S^A such that:

$$G^A = C^A + S^A = \begin{pmatrix} a_c & a_c \\ a_p & a_p \\ 0 & 0 \end{pmatrix} + \begin{pmatrix} \beta_{c,cp} & -\beta_{c,0} \\ \beta_{p,cp} & -\beta_{p,0} \\ \beta_{0,cp} & \beta_{0,0} \end{pmatrix}, \quad (1)$$

where (i) a_c and a_p are positive scalar costs corresponding to cyber and physical attacks, respectively, and (ii) $\beta_{i,j}$, $i = c, p, 0$ and $j = cp, 0$ is a positive scalar corresponding to the system term. Similarly, the defender's utility function is specified using a gain matrix G^D consisting of cost matrix C^D and system matrix S^D such that:

$$G^D = C^D + S^D = \begin{pmatrix} d_{cp} & 0 \\ d_{cp} & 0 \\ d_{cp} & 0 \end{pmatrix} + \begin{pmatrix} -\alpha_{c,cp} & \alpha_{c,0} \\ -\alpha_{p,cp} & \alpha_{p,0} \\ -\alpha_{0,cp} & -\alpha_{0,0} \end{pmatrix}, \quad (2)$$

where the first and second parts correspond to cost and system performance, respectively. In a zero-sum game, we have $S^A = -S^D$, indicating the opposing interests of the attacker and defender in rendering the system nonoperational and keeping it operational, respectively. NE under the specific case of $\beta_{i,j} = -\alpha_{i,j} = s$ has been derived in Ref. 37; the single scalar parameter s represents the system term for the provider and attacker, given by $-s$ and s, respectively. Here, the NE for zero-sum game in this case is deterministic in that it is achieved by p_i is 0 or 1 for $i = c, p$, and q_{cp} is 1 or 0.

We now consider an extension wherein $p_{s|i}, i = c, p$ represents the probability that an attack on part i will be successful if launched. Similarly, $q_{s|cp}$ represents the probability of successful defense given that both cyber and physical components are reinforced. The cost to the attacker is based on p_c and p_p, and that to defender is based on q_{cp}. The

[7] Extension to simultaneous cyber and physical attacks is direct as described in Ref. 36 for the case without incidental degradations.

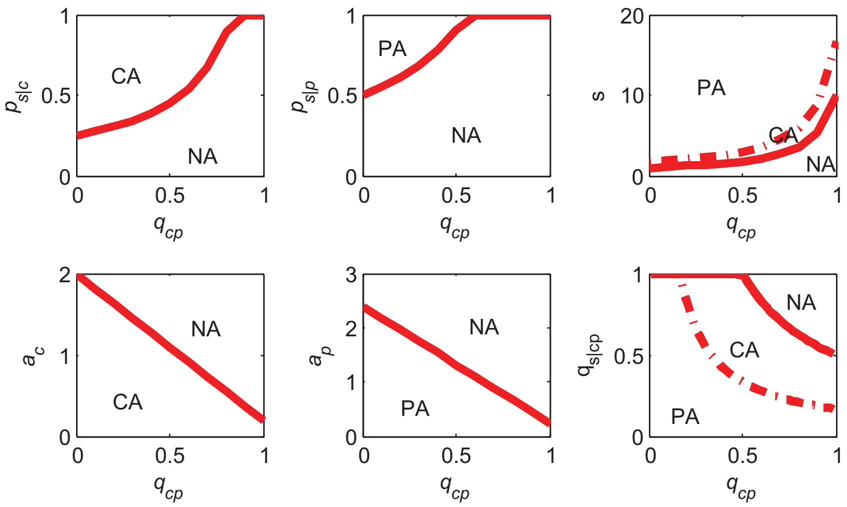


Fig. 2. Illustration of attacker's best responses with baseline values $a_c = 1$, $a_p = 2$, $s = 2$, $p_{s|c} = 0.5$, $p_{s|p} = 0.5$, $q_{scp} = 0.6$ (CA = cyber attack; PA = physical attack; NA = no attack).

system's response is based on the results of the attack and defense and hence is determined by $p_{sc} = p_{s|c}p_c$, $p_{sp} = p_{s|p}p_p$, and $q_{scp} = q_{s|cp}q_{cp}$. We incorporate the success probabilities to obtain the modified probability vectors $P_{SA} = [p_{sc} \quad p_{sp} \quad 1 - p_{sc} - p_{sp}]$ and $Q_{SD} = [q_{scp} \quad 1 - q_{scp}]$.

(1) *Attacker Strategy*: NE for the attacker is given by P_A that minimizes the attacker's utility function:

$$U_A(P_A, Q_D) = P_A C^A Q_D^T + P_{SA} S^A Q_{SD}^T,$$

where the cost term $P_A C^A Q_D^T$ is based on the probability of attack and attacker's estimated Q_D, and the second term $P_{SA} S^A Q_{SD}^T$ is based on the probability of successful attack and defense. At NE, the condition $\frac{\partial U_A}{\partial p_c} = a_c - 2s(1 - q_{scp})p_{s|c} < 0$ implies that p_c can be increased to 1 to minimize U_A, and otherwise p_c can be decreased to 0; the case of p_p is similar. Thus, the necessary conditions for the attacker to attack the cyber and physical parts are:

$$p_{s|c} > \frac{a_c}{2s(1 - q_{scp})} \quad \textit{and} \quad p_{s|p} > \frac{a_p}{2s(1 - q_{scp})},$$

respectively. Thus, the attacker will attack only if there is a certain level of probability of success. When both conditions are satisfied, the one corresponding to lower cost will be chosen. These conditions require the knowledge of s, which is decided by the provider to keep the system operational, and also the estimated state vector Q_D.

Fig. 2 illustrates the attacker's best response functions. In particular, we see that the attacker is more likely to launch a cyber attack (CA) when the defense probability q_{cp} is small, the conditional probability of successful cyber attack $p_{s|c}$ is large, the cyber attack cost a_c is small, the system payoff s is intermediate, and the conditional probability of successful defense $q_{s|cp}$ is intermediate. Similarly, the attacker is more likely to launch a physical attack (PA) when the defense probability q_{cp} is small, the conditional probability of successful physical attack $p_{s|p}$ is large, the physical attack cost a_p is small, system parameter s is large, and $q_{s|cp}$ is small.

(2) *Defender Strategy*: NE for the defender is given by Q_D that minimizes the defender's utility function:

$$U_D(P_A, Q_D) = P_A C^D Q_D^T - P_{SA} S^A Q_{SD}^T,$$

based on estimated P_A. The defender will reinforce the cyber and physical parts, that is, $q = 1$, under the condition:

$$q_{s|cp} > \frac{d_{cp}}{2s(p_{sc} + p_{sp})},$$

where $p_s = p_{sc} + p_{sp} = p_{s|c}p_c + p_{s|p}p_p$ is the probability of a successful attack on either cyber or physical part. In other words, the provider will reinforce if the attacker has a certain probability of successful attack, or if the importance level of keeping the system operational significantly outweighs the cost, i.e., $s \gg d_{cp}$. For USN, $p_{s|c}$ is small since none of the cyber attacks were disruptive. Meanwhile, p_p is small since no physical attacks were recorded. As a result, p_s is small, thereby leading to a large threshold for $q_{s|cp}$ derived above; thus, no

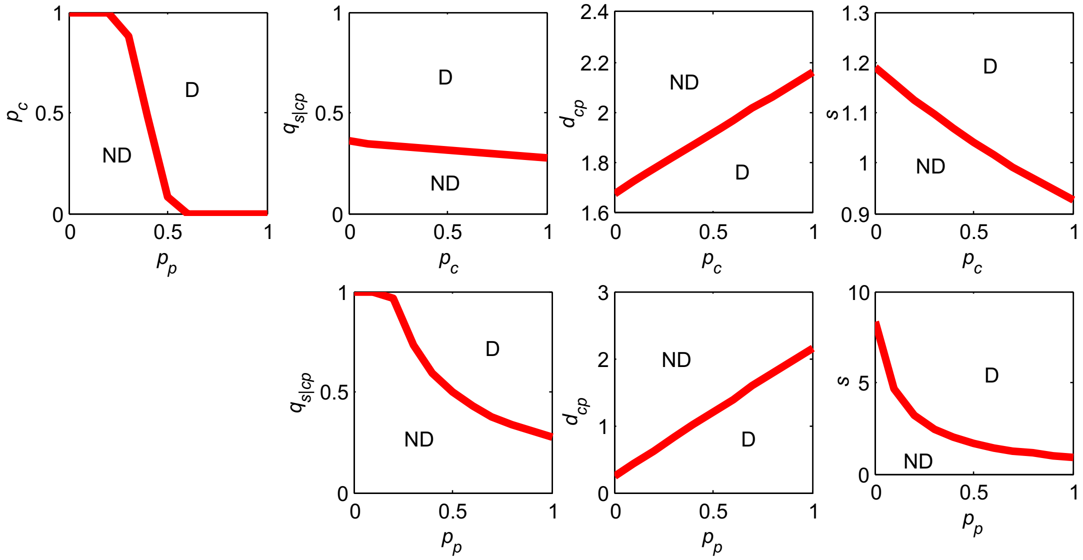


Fig. 3. Illustration of defender's best responses with baseline values $d_{cp} = 1$, $s = 2$, $p_{sc} = 0.1$, $p_{sp} = 0.8$ (D = defend; ND = not defend).

reinforcements were necessary based on these considerations.

Fig. 3 illustrates the defender's best response function. In particular, we see that the defender is more likely to defend (D) when the attacking probabilities p_p and p_c are high, the probability $q_{s|cp}$ is high, defense cost d_{cp} is low, and system parameter s is high.

NE thus is deterministic, and the outcome is determined by the cost terms, the single system term s, attacker's and defender's estimated probability vectors Q_D and P_A, respectively, and the probabilities of successful attack and defense. We note that both attacker and defender originally conjecture a mixed strategy for the other but end up employing a deterministic one.

Now consider that both cyber and physical parts are subject to incidental failures with probabilities δ_c and δ_p, respectively. We assume that cyber and physical failures are statistically independent of each other as well as the actions of attacker and defender. In this case, the probability vectors corresponding to the system term are:

$$P_{SA+\delta} = [p_{sc} + \delta_c p_{sp} + \delta_p \quad 1 - p_{sc} - p_{sp} - \delta_c - \delta_p]$$
$$Q_{SD-\delta} = [q_{scp} - \delta_c - \delta_p \quad 1 - q_{scp} + \delta_c + \delta_p].$$

Here, we notice that the degradation probabilities are added to the attack probabilities and subtracted from the defense probabilities, reflecting their net effect on the system. Proceeding as above, we have the condition for the cyber attack (namely, $p_c = 1$) given by:

$$p_{s|c} \geq \frac{a_c}{2s(1 - q_{scp} + \delta_c + \delta_p)},$$

which specifies a lower threshold for the attack compared to the above case. The case of p_p is similar. For the defender, we have the reinforcement condition (namely, $q_{cp} = 1$) given by:

$$q_{s|cp} > \frac{d_{cp}}{2s(p_{sc} + p_{sp} + \delta_c + \delta_p)},$$

which requires the reinforcement for lower values of attack success probabilities compared to the above case. For USN, this threshold is lower compared to the previous case as a result of incidental physical degradations described in Section 3.1, but is still above $q_{s|cp}$. In particular, the required outage rate of below two per year made the reinforcements unnecessary. A more stringent requirement, namely, higher s, would have made reinforcements to physical components necessary. For example, a requirement of no more than a single outage in two years would have required additional steps such as: (i) replication of control-plane host at a site other than Oak Ridge; and (ii) rerouting of one of the data-plane OC192 circuits over a physically diverse path, such as the southern U.S. route.

The formulation in this section is coarse in that it does not account for the details of various components within cyber and physical subinfrastructures but it provides an overall assessment of the need for their reinforcements. In the next section, we refine this formulation to account for the number of components within each subinfrastructure.

4.2. Component Attack-Defense Model

We consider that cyber and physical subinfrastructures or parts are composed of n_c and n_p components, respectively. Let $x_i \geq 0$, $i = c, p$, be the number of components reinforced by the defender, and $y_i \geq 0$, $i = c, p$, be the number of components attacked. The system operates at different performance levels based on the specific values of x_i and y_i, but requires that $x_i - y_i \geq k_i$ (where $k_i \geq 0$), to be operational.

A cyber infrastructure can be modeled at different levels of detail under this formulation depending on the relative importance of components. The parameters $k_i, i = c, p$ should be appropriately chosen and interpreted to achieve the required infrastructure performance. For a simplified CCI model, n_c is the total number of servers located at n_s sites, and $n_p = 2n_s$, where each site contributes to two physical components, namely, HVAC system and fiber connection. k_c represents the number of servers that are operational and connected to the Internet, and k_p represents the physical components at these operational servers. For a simplified HPCI model, $n_c = n_s$ represents the number of supercomputers, and $n_p = 2n_s$ as in the case of CCI. k_c represents the number of supercomputers that are operational and connected to the network, and $k_p = n_s + k_c$ ensures that the HVAC system and fiber connection are both operational at k_c sites. The components of USN can be modeled at various levels of abstraction; at a very coarse level, $n_c = 4$ represents four firewalls, and $n_p = 10$ represents HVAC systems at four sites and six fiber (OC192) connections. The condition that Oak Ridge site must be operational for the control-plane leads to $k_c = 1$, and that at least one fiber connection and one site must be physically operational to provide a minimum service leads to $k_p = 2$.

Let $x \in \{1, 2, \ldots, n_c n_p + 1\}$ and $y \in \{1, 2, \ldots, n_c + n_p + 1\}$ denote the variables of defender and attacker that correspond to the action sets $N_D = \{(1, 1), \ldots (n_c, n_p), (0, 0)\}$ and $N_A = \{(1, 0), \ldots (n_c, 0), (0, 1), \ldots, (0, n_p), (0, 0)\}$, respectively. We represent this game using $(n_c + n_p + 1) \times (n_c n_p + 1)$ gain matrices, G^A and G^D, where rows correspond to y, the attacker's choices, and columns correspond to x, the defender's options. The (y, x)th element, $e_{y,x}$, of a gain matrix is interpreted as follows:

(i) For the defender, $x = n_c n_p + 1$ represents defending neither cyber nor physical components, namely, $x_{cp} = 0$; $x \in [1, n_c n_p]$ represents defending $x_p = [(x - 1) \div n_c] + 1$ physical components and $x_c = [(x - 1) \bmod n_c] + 1$ cyber components. In some cases, we denote (y, x)th element $e_{y,x}$ in a more explicit form.

(ii) For the attacker, $y \in [1, n_c]$ represents attack on $y_c = y$ cyber components, and $y \in [n_c + 1, n_c + n_p]$ represents attack on $y_p = y - n_c$ physical components, and $y = n_c + n_p + 1$ represents no attack, namely, $y_c = y_p = 0$.

Each gain matrix is expressed as a sum of cost and system matrices as in the Boolean case, namely, $G^A = C^A + S^A$ and $G^D = C^D + S^D$ for the attacker and defender, respectively. The probability vectors of attacker and defender are given by:

$$P_A = [p_{c_1} \quad p_{c_2} \ldots p_{c_{n_c}} p_{p_1} p_{p_2} \ldots p_{p_{n_p}} p\prime] \text{ and}$$

$$Q_D = [q_{1:1} q_{1:2} \ldots q_{1:n_p} \ldots q_{n_c:1} \ldots q_{n_c:n_p} q\prime],$$

respectively, where $p\prime = 1 - \sum_{l=1}^{n_c} p_{c_l} - \sum_{l=1}^{n_p} p_{p_l}$ and $q\prime = 1 - \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} q_{x_c:x_p}$. For simplicity of notation, we also use the alternative notation $P_A = [p_1, p_2, \ldots, p_{n_c+n_p+1}]$, and $Q_D = [q_1, q_2, \ldots, q_{n_c n_p+1}]$ where the index x represents x_c and x_p; q_x is also denoted by $q_{x_c:x_p}$. Let $c_{y,x}$, $d_{y,x}$, and $s_{y,x}$ denote the (y, x)th entry of attacker's cost matrix C^A, defender's cost matrix C^D, and system matrix $S^A = -S^D$. The bottom row of C^A consists of 0s denoting the cost of no attack with probability $p\prime$, that is, $c_{n_c+n_p+1,x} = 0$ for $x = 1, 2, \ldots, n_c n_p + 1$. And the rightmost column of C^D consists of 0s denoting no reinforcement cost, that is, $d_{y,n_c n_p+1} = 0$ for $y = 1, 2, \ldots, n_c + n_p + 1$. As a result, we have the following cost term for the attacker:

$$P_A C^A Q_D^T = \sum_{x=1}^{n_c n_p+1} q_x \left(\sum_{l=1}^{n_c} p_{c_l} c_{l,x} + \sum_{l=1}^{n_p} p_{p_l} c_{n_c+l,x} \right),$$

where Q_D^T represents the attacker's estimate of defender's probabilities of reinforcement. The system term utilized by the attacker is given by:

$$
\begin{aligned}
P_A S^A Q_D^T = & \sum_{y=1}^{n_c+n_p+1} \sum_{x=1}^{n_c n_p+1} p_y s_{y,x} q_x \\
= & \sum_{l=1}^{n_c} p_{c_l} \left(\sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} s_{l,x_c:x_p} q_{x_c:x_p} \right) \\
& + \sum_{l=1}^{n_c} p_{c_l} \left(s_{l,n_c n_p+1} q' \right) \\
& + \sum_{l=1}^{n_p} p_{p_l} \left(\sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} s_{n_c+l,x_c:x_p} q_{x_c:x_p} \right) \\
& + \sum_{l=1}^{n_p} p_{p_l} \left(s_{n_c+l,n_c n_p+1} q' \right) \\
& + p\prime \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} s_{n_c+n_p+1,x_c:x_p} q_{x_c:x_p} \\
& + p\prime s_{n_c+n_p+1,n_c n_p+1} q\prime .
\end{aligned}
$$

At NE, attacker computes P_A^* that minimizes $P_A G^A Q_D^T$, and defender computes Q_D^* that minimizes $P_A G^D Q_D^T$. By combining the above, for the attacker we have the partial derivative for cyber components:

$$
\begin{aligned}
\frac{\partial P_A G^A Q_D^T}{\partial p_{c_l}} = & \, q'(s_{l,n_c n_p+1} - s_{n_c+n_p+1,n_c n_p+1}) \\
& + \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} q_{x_c:x_p} \left(c_{l,x_c:x_p} \right. \\
& \left. + s_{l,x_c:x_p} - s_{n_c+n_p+1,x_c:x_p} \right),
\end{aligned}
$$

and the partial derivative for physical components:

$$
\begin{aligned}
\frac{\partial P_A G^A Q_D^T}{\partial p_{p_l}} = & \, q'(s_{n_c+l,n_c n_p+1} - s_{n_c+n_p+1,n_c n_p+1}) \\
& + \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} q_{x_c:x_p} \left(c_{n_c+l,x_c:x_p} \right. \\
& \left. + s_{n_c+l,x_c:x_p} - s_{n_c+n_p+1,x_c:x_p} \right).
\end{aligned}
$$

NE is determined by computing all above partial derivatives that are negative, and assigning probability 1 to the one that minimizes $P_A G^A Q_D^T$. Since each of these terms is based on "fixed" elements of the gain matrices and no limits are imposed on the cost, the corresponding probability can be increased to 1 (as in the Boolean case). Note, however, that if the elements depend on the probabilities, this approach does not result in the minimization of utility function. If all partial derivative are nonnegative, then attacker will not attack, i.e., $p' = 1$, and the system survives. The computational complexity of this step is $O(n_c n_p (n_c + n_p))$. Due to the specific nature of these underlying game matrices, this computation is polynomial time, compared to the more complex PPAD-completeness of the general two-player NE computation.(35) This computation requires attacker's assessment of the likelihood of components being reinforced. Such information can be based on public information, general best practices in deploying the infrastructures, and results of past attacks.

For the defender, we have a cost term given by:

$$
\begin{aligned}
P_A C^D Q_D^T = & \sum_{l=1}^{n_c} p_{c_l} \left(\sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} d_{l,x_c:x_p} q_{x_c:x_p} \right) \\
& + \sum_{l=1}^{n_p} p_{p_l} \left(\sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} d_{n_c+l,x_c:x_p} q_{x_c:x_p} \right) \\
& + p' \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} d_{n_c+n_p+l,x_c:x_p} q_{x_c:x_p},
\end{aligned}
$$

and combining with the system term $P_A S^D Q_D^T = -P_A S^A Q_D^T$, we have:

$$
\begin{aligned}
\frac{\partial P_A G^D Q_D^T}{\partial q_x} = & \sum_{l=1}^{n_c} p_{c_l} (d_{l,j} - s_{l,x} + s_{l,n_c n_p+1}) \\
& + \sum_{l=1}^{n_p} p_{p_l} (d_{n_c+l,x} - s_{n_c+l,x} + s_{n_c+l,n_c n_p+1}) \\
& + p'(d_{n_c+n_p+1,x} - s_{n_c+n_p+1,x} \\
& + s_{n_c+n_p+1,n_c n_p+1}).
\end{aligned}
$$

Here, P_A represents the defender's estimate of the attacker's probabilities of attack. Since an attack will be on either cyber or physical part, only one of $\sum_{l=1}^{n_c} p_{c_l} s_{l,x}$ and $\sum_{l=1}^{n_p} p_{p_l} s_{n_c+l,x}$ will be nonzero, and the one with minimum utility value will be chosen at NE. Then, for the defender, we compute all the resultant terms that are negative, and pick the one that gives the lowest cost for $P_A G^D Q_D^T$. If no negative partial derivatives exist, no components will be reinforced, i.e., $q\prime = 1$, and the infrastructure may not necessarily survive an attack. Thus at NE, the infrastructure survival status is deterministic and is determined as follows:

system state

$$= \begin{cases} \text{survive} & \text{if } [(x_c \geq k_c) \wedge (x_p \geq k_p)] \\ & \vee[(y_c < n_c - k_c) \\ & \wedge(y_p < n_p - k_p)] \\ \text{not} & \text{else if} \\ & [(x_c < k_c) \wedge (y_c > n_c + x_c - k_c)] \\ & \vee[(x_p < k_p) \\ & \wedge(y_p > n_p + x_p - k_p)] \\ \text{either} & \text{else.} \end{cases}$$

The infrastructure survival in the third case depends on which specific components are attacked and reinforced. For $i = c, p$, there are fewer than k_i components reinforced, and no more than $n_i - y_i$ components not attacked, since $x_i < k_i$ and $n_i - k_i \geq y_i$ and $y_i \leq n_i + x_i - k_i$. There is a set $S_{n_i - y_i}$ with at least $n_i - y_i \leq k_i$ components that are not attacked, and there is a set S_{x_i} with $x_i < k_i$ components that are reinforced. The infrastructure will survive if and only if there are k_i, for $i = c, p$, components each of which is either not attacked or has been reinforced, that is, $|S_{n_i - y_i} \cup S_{x_i}| \geq k_i$, for $i = c, p$. If the infrastructure survives, its performance level is determined by x_i, y_i, n_i, and k_i, for $i = c, p$, and also the precise strategies used by the attacker and defender (as illustrated in Section 5).

The concept of survival is based on the choice and semantics of $k_i, i = c, p$, parameters. For the CCI model, the survival implies the availability of k_c servers for users over the Internet. Similarly for the HPCI model, survival implies that k_c supercomputers are available to users. In both cases, a more detailed analysis is needed to assess the effects of constraints due to k_i, as will be illustrated in Section 5 under statistical independence conditions.

4.3. Probability of Successful Attack and Defense

We now consider that when attacker launches $z_i \geq y_i \geq 0, i = c, p$, attacks, y_i of them will be successful with probability $p_{y_i|z_i}$. Then, the probabilities of y_c and y_p successful cyber and physical attacks are given by:

$$p_{sy_c} = \sum_{z_c=y_c}^{n_c} p_{y_c|z_c} p_{z_c} \text{ and} p_{sy_p} = \sum_{z_p=y_p}^{n_p} p_{y_p|z_p} p_{z_p},$$

respectively. When defender reinforces $t_i \geq x_i$ components, x_i will successfully withstand the attack with probability $q_{x_c|t_c:x_p|t_p}$. Then, the probability of successful defense of x_p physical components and x_c cyber components is given by:

$$q_{sx_c:sx_p} = \sum_{t_c=x_c}^{n_c} \sum_{t_p=x_p}^{n_p} q_{x_c|t_c:x_p|t_p} q_{t_c:t_p}.$$

The probability vectors that multiply cost matrices are P_A and P_D (same as before), and those that multiply system matrices are:

$$P_{SA} = [p_{sc_1} p_{sc_2} \ldots p_{sc_{n_c}} p_{sp_1} p_{sp_2} \ldots p_{sp_{n_p}} p_{s'}]$$

$$Q_{SD} = [q_{s1:s1} q_{s1:s2} \ldots q_{s1:sn_p} \ldots q_{sn_c:s1} \ldots q_{sn_c:sn_p} q_{s'}],$$

where $p_{s'} = 1 - \sum_{y=1}^{n_c} p_{sc_y} - \sum_{y=1}^{n_p} p_{sp_y}$ and $q_{s'} = 1 - \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} q_{sx_c:sx_p}$. For the attacker, we consider the cost $P_A C^A Q_D^T + P_{SA} S^A Q_{SD}^T$, and the partial derivatives are obtained as in the previous section. For cyber components, we have:

$$\frac{\partial P_A C^A Q_D^T}{\partial p_{c_l}} + \frac{P_{SA} S^A Q_{SD}^T}{\partial p_{c_l}} = \sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} q_{x_c:x_p} c_{l,x_c:x_p}$$

$$+ \sum_{x=1}^{c_l} \left(p_{x|c_l} \left[\sum_{x_c=1}^{n_c} \sum_{x_p=1}^{n_p} q_{x_c:x_p} \left(s_{l,x_c:x_p} - s_{n_c+n_p+1,x_c:x_p} \right) \right.\right.$$

$$\left.\left. + q'(s_{l,n_c n_p+1} - s_{n_c+n_p+1,n_c n_p+1}) \right] \right) .$$

For physical components, the partial derivative $\frac{\partial P_A C^A Q_D^T}{\partial p_{p_l}} + \frac{P_{SA} S^A Q_{SD}^T}{\partial p_{p_l}}$ can be similarly computed.

For the defender, we consider the cost $P_A C^D Q_D^T - P_{SA} S^A Q_{SD}^T$ and the partial derivative is given by:

$$\frac{\partial P_A C^D Q_D^T}{\partial q_x} - \frac{P_{SA} S^A Q_{SD}^T}{\partial q_x}$$

$$= \sum_{l=1}^{n_c} p_{c_l} d_{l,j} + \sum_{l=1}^{n_p} p_{p_l} d_{n_c+l,x}$$

$$- \sum_{x'_c=1}^{x_c} \sum_{x'_p=1}^{x_p} q_{x'_c|x_c:x'_p|x_p} \sum_{l=1}^{n_c} p_{c_l} (s_{l,n_c n_p+1} - s_{l,x})$$

$$- \sum_{x'_c=1}^{x_c} \sum_{x'_p=1}^{x_p} q_{x'_c|x_c:x'_p|x_p}$$

$$\sum_{l=1}^{n_p} p_{p_l} (s_{n_c+l,n_c n_p+1} - s_{n_c+l,x})$$

$$+ \sum_{x'_c=1}^{x_c} \sum_{x'_p=1}^{x_p} q_{x'_c|x_c:x'_p|x_p} p' (d_{n_c+n_p+1,j}$$

$$- s_{n_c+n_p+1,x} + s_{n_c+n_p+1,n_c n_p+1}).$$

We utilize the algorithm of the previous section to compute NE, and the computational complexity is $O(n_c^2 n_p^2(n_c + n_p))$. The probability of incidental failures can be handled using $P_{SA+\delta}$ and $Q_{SD-\delta}$ as in the previous section. NE is qualitatively quite similar to that of the previous section although the values of z_a and t_a could be different when incidental failures are taken into account.

For USN, the analysis is similar to the Boolean case but is carried out separately on individual cyber and physical components. The provider's estimates of p_{sc_l} is close to zero, since $p_{y_c|z_c}$ is close to zero due to unsuccessful cyber attacks on USN. And, the estimate of p_{sp_l} is close to zero for a different reason, namely, no incidents of physical attacks, which makes p_{z_p} close to zero. As a result, $p\prime$ component of provider's estimate of P_{SA} is close to 1, and others are close to zero. Then, the corresponding partial derivatives are positives, leading to provider's solution $q\prime = 1$, and as a result no additional reinforcements were needed. For incidental degradations, $\delta = 0$ for cyber components, and a value much below the target of two failures per year for physical components. Thus, the incremental terms in the partial derivatives due to δ are close to zero, which in turn leads to no additional reinforcements. Any significant increases either in the success probabilities of cyber attacks or incidents of physical attacks would render the corresponding partial derivatives negative; this condition in turn will require that the corresponding components be reinforced. Similar qualitative analysis applies to incidental degradations: increases in incidental degradation probabilities of the components will render some of the partial derivatives negative, thereby indicating that the corresponding components be reinforced. In contrast with the Boolean case, the results of this section provide a finer analysis in that they identify specific cyber and physical components to be reinforced.

If the cost of attack or reinforcement depends on the component, then the minimization of the utility function needed for NE computation depends on the choice of components for both attack and defense. Under arbitrary (possibly nonlinear) costs, the choice of picking the optimal set of components to attack by the attacker and the optimal set of components to reinforce for the defender can be shown to be versions of the bin packing problem, and hence are computationally intractable. The deterministic NE of this formulation is a result of the unbounded cost, i.e., cost terms can be arbitrarily increased to make the underlying probability 1. When finite bounds are imposed on cost terms, the NE is no longer guaranteed to be deterministic, and could consist of a mixed strategy.

The results of this section are based on ensuring that k_i, $i = c, p$, components would be operational but does not provide further information about the performance levels above these values. For example, the "spare" capacity of CCI above the minimum level of k_c servers could be a measure of robustness of the infrastructure to later degradation events. Also, this framework does not account for different sites housing different number of servers, which could influence the site-level reinforcement strategies. Such analysis requires that further details about the infrastructure be taken into account, as will be illustrated in the next section for computing infrastructures.

5. COMPUTING INFRASTRUCTURES

We now consider the details of computing infrastructures of Section 3.2 to refine the results based on NE conditions. In these computing infrastructures, the cyber components consist of computing systems and gateway routers, and the physical components consist of fiber connections, physical plant, and power supplies. The disruptions of gateway routers, fiber connections, physical plant, and power supplies all have the same net effect of disconnecting all computing systems at the site. Hence, for simplicity of discussion, we generically consider only the physical attacks on fiber to capture all such effects.

The refinement of NE results to infer the performance of cyber infrastructures requires that the elements of both cost and system matrices be suitably specified. The elements of cost matrices are specified as follows to reflect component-level details: (i) for the defender, $d_{l,x} = d_{l,x_c:x_p} = x_c d_{dc} + x_p d_{dp}$, where d_{dc} and d_{dp} are costs of reinforcing a cyber and physical component, respectively, and (b) for the attacker, $c_{y,x} = y c_{ac}$ for $y \in [1, n_c]$ and $c_{y,x} = (y - n_c)^\alpha c_{ap}$, for $\alpha \geq 1$, $y \in [n_c + 1, n_c + n_p + 1]$, where c_{ac} and c_{ap} are the costs of attacking a cyber and physical component, respectively; α could be higher than 1, indicating a higher cost of coordinating multiple physical attacks at geographically separated locations.

Then, we consider two ways of computing the elements $s_{y,x}$ of the system matrix S^A.

First, we consider further details of the system terms for the defender by taking into account the levels of reinforcement above the values specified by k_i, $i = c, p$, as follows:

$$-s_{i,j} = \begin{cases} -2s & \text{if } [(y_c = 0) \wedge (y_p = 0)] \\ 2s & \text{else if } [(x_c < k_c) \\ & \quad \wedge (y_c > n_c + x_c - k_c)] \\ & \quad \vee [(x_p < k_p) \\ & \quad \wedge (y_p > n_p + x_p - k_p)] \\ -s\left[1 + \dfrac{x_c - k_c}{x_c - k_c + y_c}\right] & \text{else if } y_p = 0 \\ -s\left[1 + \dfrac{x_p - k_p}{x_p - k_p + y_p}\right] & \text{else if } y_c = 0. \end{cases}$$

Here, the single scalar $-s$ represents the system term for the defender. In the first case, there is no attack hence the system survives at the reinforced level. In the next case, the system will not survive since the required number of cyber and physical components are not available. In the last two cases, the system operates with a degraded capacity, and the residual capacity is proportional to $1/y_i$, $y_i = 1, 2, \ldots, n_i, i = c, p$. Intuitively, this characterization reflects the vulnerability of the infrastructure in that $1/y_i$ is the probability of being a target of a uniform attack model.

Alternatively, we consider another approach to specify the system terms, where the residual capacity is proportional to $-y_i$, as follows:

$$-s^{II}_{i,j} = \begin{cases} -2s & \text{if } x_c = 0; x_p = 0; \\ & \quad y_c = 0; y_p = 0 \\ 2s & \text{else if } y_p \geq x_p - k_p \\ 2s & \text{else if } y_c \geq x_u - k_c \\ -s\left[1 + \dfrac{x_c - k_c - y_c}{x_c - k_c}\right] & \text{else if } y_p = 0 \\ -s\left[1 + \dfrac{x_p - k_p - y_p}{x_p - k_p}\right] & \text{else if } y_c = 0. \end{cases}$$

Based on NE of the game, the attacker and provider will determine values of x_i and y_i, respectively, which in turn determine if the infrastructure survives or not.

In the case the system survives, we now estimate the expected infrastructure performance when the attacker and defender pick the components to attack and reinforce, respectively, independently using the uniform distribution. We also assume that the attack and reinforcement processes that are used to choose the components are mutually statistically independent. Once x_i and y_i values are chosen, the components to reinforce and attack, respectively, could be chosen using uniform pseudo random number generators, many of which satisfy the statistical independence property to a first order. A cyber or physical component will survive if it is not attacked or has been reinforced when attack occurs; for $i = c, p$, these probabilities are given by $[1 - \frac{1}{n_i}]^{y_i}$ and $[1 - (1 - \frac{1}{n_i})^{x_i}][1 - (1 - \frac{1}{n_i})^{y_i}]$, respectively. The probability that a component will survive a specific attack is given by, for $i = c, p$,

$$1 - \left[1 - \frac{1}{n_i}\right]^{x_i}\left[1 - \left(1 - \frac{1}{n_i}\right)^{y_i}\right],$$

which is an increasing function of x_i and decreasing function of y_i. In particular, if $y_i = 0$, the infrastructure continues to operate. Under the condition that the attacker will only attack physical or cyber components but not both, the probability that the component will survive is given by:

$$f_U(n_c, n_p, x_c, x_p, y_c, y_p) = 1 - \sum_{i=c,p}\left(\left[1 - \frac{1}{n_i}\right]^{x_i}\left[1 - \left(1 - \frac{1}{n_i}\right)^{y_i}\right]\right),$$

which is called the *robustness fraction*. We next estimate the expected capacity and expected number of available supercomputers for CCI and HPCI, respectively, using this formula for $f_U(.)$.

5.1. Cloud Computing Infrastructure

We consider a CCI with different number of servers at different sites, and the attacker is not aware of this information. Let $n_{s_1}, n_{s_2}, \ldots n_{s_{n_s}}$ denote the number of servers located at n_s physical sites. The attacker will attack y_c servers based on their cyber location information, and they can be distributed across the sites since their physical locations are not known to the attacker. On the other hand, each physical attack is on a single site, and if successful will disconnect all servers at the site.

We consider two strategies for the defender: (i) uniform strategy where the components are chosen uniformly and independently, and (b) proportional strategy that assigns higher reinforcement probabilities to sites with a higher number of servers with probability $\frac{n_{s_j}}{\sum_{l=1}^{n_p} n_{s_l}}$ for a site j with n_{s_j} servers. On the other hand, the attacker will adopt a uniform strategy, being unaware of the number of servers at different sites. For the defender's uniform strategy, the expected capacity of CCI is given by:

Table II. Simulation of 1,000 Server Cloud Computing Infrastructure; *c* and *p* Denote Cyber and Physical Parts, and prop and uni Denote Proportional and Uniform Strategies

Case	k_c	k_p	c_{ac}	c_{cp}	d_{dc}	d_{dp}	Attack	Defense	Survival	Residual Capacity
A	25	1	1	1	1	1	100 (c)	25(c), 1(p)	100% (both)	50.75 (both)
B	25	1	1	10	10	1	100 (c)	25(c), 1(p)	100% (both)	50.75 (both)
C	25	2	1	10	10	1	100 (c)	25(c), 2(p)	100% (both)	50.69 (both)
D	25	1	10	1	10	1	1(p)	25(c), 1(p)	100% (both)	65.46 (prop), 58.26 (uni)
D’	25	1	10	1	10	1	1(p)	25(c), 1(p)	100% (both)	57.26 (both)
E	25	3	1	10	10	1	5(p)	25(c), 3(p)	100% (both)	66.10 (prop), 65.00 (uni)

$$\sum_{j=1}^{n_s}\left(n_{s_j}\left[1-\sum_{i=c,p}\left(\left[1-\frac{1}{n_i}\right]^{x_i}\left[1-\left(1-\frac{1}{n_i}\right)^{y_i}\right]\right)\right]\right)$$
$$=\left(\sum_{j=1}^{n_s} n_{s_j}\right)\left[1-\sum_{i=c,p}\left(\left[1-\frac{1}{n_i}\right]^{x_i}\left[1-\left(1-\frac{1}{n_i}\right)^{y_i}\right]\right)\right]$$
$$=\left(\sum_{j=1}^{n_s} n_{s_j}\right) f_U(n_c, n_p, x_c, x_p, y_c, y_p),$$

where the robustness fraction specifies the fraction of servers $\sum_{j=1}^{n_s} n_{s_j}$ that will be operational on the average.

Under the proportional strategy, the probability that any node will be selected for reinforcement and attack is given by $1-(1-\frac{n_{s_j}}{\sum_{l=1}^{n_p} n_{s_l}})^{x_i}$ and $1-(1-\frac{1}{n_i})^{y_i}$, respectively. Then, by considering cyber and physical parts, the probability that server at site j will survive is given by:

$$1-\sum_{i=c,p}\left(\left[1-\frac{n_{s_j}}{\sum\limits_{l=1}^{n_p} n_{s_l}}\right]^{x_i}\left[1-\left(1-\frac{1}{n_i}\right)^{y_i}\right]\right).$$

Then, the expected capacity of the CCI for the proportional strategy is given by:

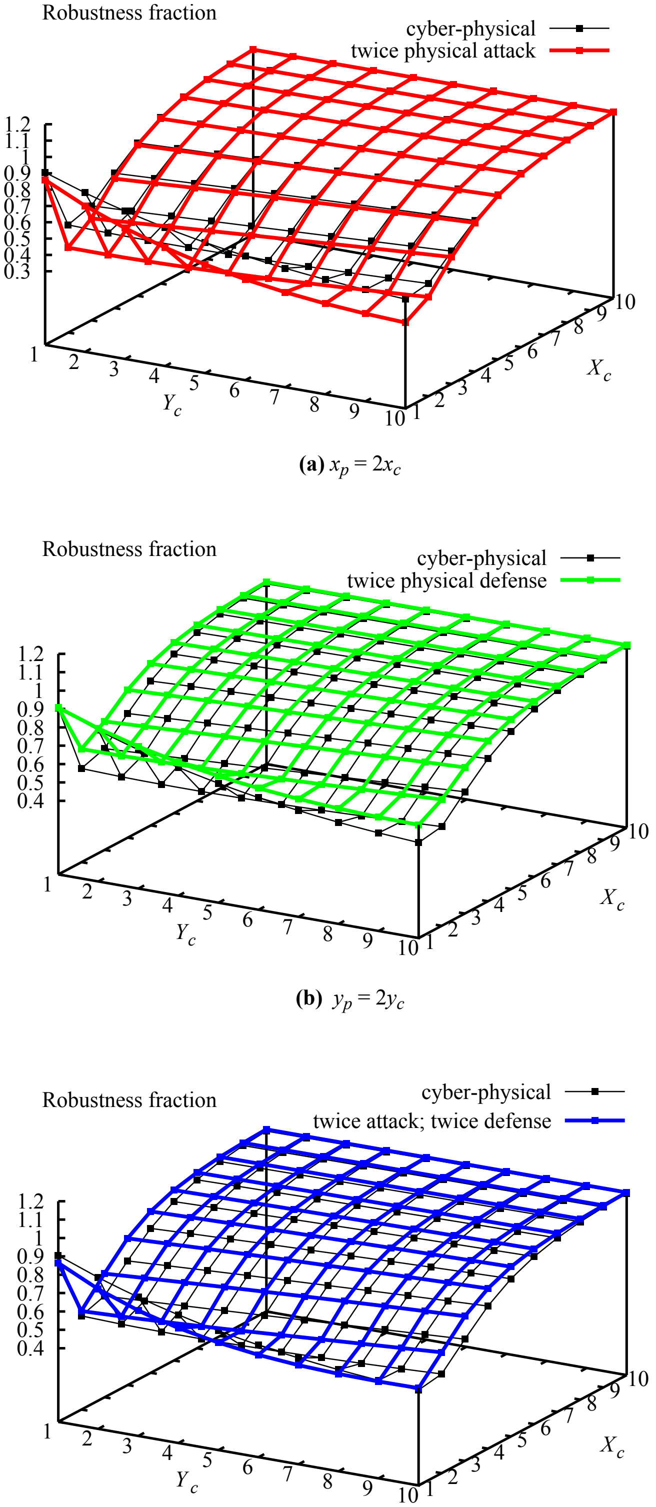
$$\sum_{j=1}^{n_s}\left(n_{s_j}\left[1-\sum_{i=c,p}\left(\left[1-n_{s_j}/\sum_{l=1}^{n_p} n_{s_l}\right]^{x_i}\right.\right.\right.$$
$$\left.\left.\left.\left[1-\left(1-\frac{1}{n_i}\right)^{y_i}\right]\right)\right]\right).$$

The expected capacity for the uniform strategy can be shown to be smaller than the above expected capacity by utilizing the inequality $(\sum_{j=1}^{n_s} n_{s_j})^2 \le n_s \sum_{j=1}^{n_s} n_{s_j}^2$. Thus, this defender’s proportional approach ensures a higher expected capacity compared to the uniform strategy. If the provider discloses n_{s_j}s, then attacker might adopt a less uniform strategy; by not disclosing this information defender gains a definite advantage.

We simulated a CCI with 100 servers distributed at five sites with various parameters. At NE, we compute the system status and available capacity by simulating 1,000 instances of the attacker and defender strategies; for the latter, we consider both uniform and proportional methods. The salient features of the simulations are summarized in Table II. We consider the server distribution of 50, 30, 10, 5, and 5 across the sites for Cases A–E, and 20 servers at each site for Case D’. In cases A–C, the attacks are on the cyber part due to its lower cost, and defender reinforces the required number of cyber and physical components, and the system survives, albeit at about half the capacity. In case D, the cost of cyber attacks becomes 10 times higher, resulting in a physical attack, where the proportional strategy leads to a higher residual capacity. The case D’ is identical except each site has 20 servers, which leads to a lower residual capacity. Case E requires three physical nodes to be operational, which leads to attacks on all physical nodes, and defender reinforces three nodes; the proportional strategy leads to a slightly higher residual capacity.

5.2. High-Performance Computing Infrastructure

We consider an HPCI represented by (i) $n_c = n_s$ cyber components each encompassing the firewall and computing system, where n_s is the number of sites, and (ii) $n_p = n_s$ physical components representing the sites that house the computing systems including fiber connections. Then, the expected number of supercomputing facilities available to users is given by $\sum_{j=1}^{n_s} E[1_j]$, where 1_j is the indicator function, which takes value 1 if the site j survives and 0 otherwise. We now consider that both attacker and defender adopt uniform random strategies, and the attacks and reinforcements are statistically independent. By noting that $E[1_j]$ is the



(a) $x_p = 2x_c$

(b) $y_p = 2y_c$

(c) $x_p = 2x_c$ and $y_p = 2y_c$

Fig. 4. Profiles of robustness fraction $f_U(20, 20, x_c, x_p, y_c, y_p)$. Case (a) illustrates the effects of doubling physical attacks, which leads to lower $f_U(.)$ values. Case (b) illustrates the effects of doubling physical reinforcements, which leads to higher $f_U(.)$ values. Case (c) shows the effects of doubling physical attacks and doubling physical reinforcements, which shows a more complex comparative performance.

probability that site j survives, the expected number of supercomputers $\hat{N}_{HPC}$ that will survive y_i uniform independent attacks is given by:

$$\begin{aligned}
&\hat{N}_{HPC}\\
&= \sum_{j=1}^{n_s} \left(1 - \sum_{i=c,p} \left[\left(1 - \frac{1}{n_i}\right)^{x_i} - \left(1 - \frac{1}{n_i}\right)^{x_i+y_i} \right] \right)\\
&= n_s \left[1 - \sum_{i=c,p} \left(\left[1 - \frac{1}{n_i}\right]^{x_i} \left[1 - \left(1 - \frac{1}{n_i}\right)^{y_i}\right] \right) \right]\\
&= n_s f_U(n_c, n_p, x_c, x_p, y_c, y_p),
\end{aligned}$$

where $f_U(n_c, n_p, x_c, x_p, y_c, y_p)$ is the same robustness fraction. As expected, the expected number of surviving supercomputers improves as x_i increases and decreases as y_i increases. In particular, under $y_i = 0$, all n_s computing systems will be available, and under $x_i = 0$, the reduction in $\hat{N}_{HPC}$ is the largest for any y_i. Due to the application of the robustness fraction $f_U(.)$ to both CCI and HPCI, we now examine its overall profiles. We show three profiles in Fig. 4 of $f_U(20, 20, x_c, x_p, y_c, y_p)$ plotted as a function of x_c and y_c. In Fig. 4(a), we plot the cases of $x_c = x_p$ and $y_c = y_p$, and $y_p = 2 \times y_c$, which illustrates that higher levels of attack lead to lower f_U values but the difference becomes quite small ($< 1\%$) for higher values of x_c. In Fig. 4(b), we plot the cases of $x_c = x_p$ and $y_c = y_p$, and $x_p = 2 \times x_c$ with all other parameters being the same; these plots illustrate that higher levels of reinforcement lead to higher f_U values but the difference becomes quite small ($<1\%$) at higher values of x_c. In Fig. 4(c), we plot the cases of $x_c = x_p$ and $y_c = y_p$, and $x_p = 2 \times x_c$ and $y_p = 2 \times y_c$, which illustrates somewhat more complex relative performance and the difference is quite significant ($>10\%$) for most values of x_c.

6. CONCLUSIONS

Cyber infrastructures rely on both cyber and physical components for their operation, which are subject to natural, incidental, or intentional degradations. We presented a systematic analysis and design framework for such infrastructures based on two game-theoretic models that capture different levels of detail. We studied the strategic interactions between an attacker and a defender using this game-theoretic approach. When the utility functions of the attacker and provider consist of sums of individual cost and system terms, NE is deterministic, and is polynomial-time computable under uniform costs. We utilized these results to analyze USN network infrastructure and simplified models of CCI and HPCI.

This formulation only provides a basic game-theoretic analysis of cyber infrastructures, and could be extended in several ways. The simplified models of CCI and HPCI considered here can be refined by explicitly modeling the correlations and differences between the cyber and physical components. Also, the uniform attack and defense models considered here represent only a starting point of the game-theoretic analysis, and more informed models based on statistical correlation and measurement data could lead to more practically useful results. In terms of game theory, formulations that bound the total costs of reinforcements and attacks would be of future interest, and they are likely to lead to more complex NE computations. It would also be interesting to study the sequential game formulations of this problem, and the cases where different levels of knowledge are available to the attacker and provider. More detailed simulations with system-specific details of CCI and HPCI would be of future interest.

ACKNOWLEDGMENTS

This work was funded by the Mathematics of Complex, Distributed, Interconnected Systems Program, Office of Advanced Computing Research, U.S. Department of Energy, and by Extreme Scale Systems Center, sponsored by U. S. Department of Defense, and performed at Oak Ridge National Laboratory managed by UT-Battelle, LLC for U.S. Department of Energy under Contract No. DE-AC05-00OR22725.

REFERENCES

1. Rao NSV, Hicks SE, Poole SW, Newman P. Testbed and experiments for high-performance networking. Tridentcom: Proceedings of International Conference on Testbeds and Research Infrastructures for the Development of Networks and Communities, 2010.
2. Fudenberg D, Tirole J. Game Theory. Cambridge, MA: MIT Press, 2003.
3. Myerson RB. Game Theory: Analysis of Conflict. Cambridge, MA: Harvard University Press, 1991.
4. Nisan N, Roughgarden T, Tardos E, Vazirani VV (eds). Algorithmic Game Theory. New York: Cambridge University Press, 2007.
5. Bier VM, Azaiez MN (eds). Game Theoretic Risk Analysis of Security Threats. New York: Springer, 2009.
6. Hausken K, Levitin G. Review of systems defense and attack models. International Journal of Performability Engineering, 2012; 8(4):355–366.

7. Zhuang J, Bier VM. Balancing terrorism and natural disasters—Defensive strategy with endogenous attack effort. Operations Research, 2007; 55(5):976–991.
8. He F, Zhuang J. Modelling "contracts" between a terrorist group and a government in a sequential game. Journal of the Operational Research Society, 2012; 63(6):790–809.
9. Jose VRR, Zhuang J. Technology adoption, accumulation, and competition in multi-period attacker-defender games. Military Operations Research, 2013; 18(2):33–47.
10. Zhuang J, Bier VM, Alagoz O. Modeling secrecy and deception in a multiple-period attacker-defender signaling game. European Journal of Operational Research, 2010; 203(2):409–418.
11. Shan X, Zhuang J. Cost of equity in homeland security resource allocation in the face of a strategic attacker. Risk Analysis, 2013; 33(6):1083–1099.
12. Shan X, Zhuang J. Hybrid defensive resource allocations in the face of partially strategic attackers in a sequential defender-attacker game. European Journal of Operational Research, 2013; 228(1):262–272.
13. Jenelius E, Westin J, Holmgren ÄJ. Critical infrastructure protection under imperfect attacker perception. International Journal of Critical Infrastructure Protection, 2010; 3(1):16–26.
14. Nikoofal M, Zhuang J. Robust allocation of a defensive budget considering an attacker's private information. Risk Analysis, 2012; 32(5):930–943.
15. Zhuang J, Bier VM. Secrecy and deception at equilibrium, with applications to anti-terrorism resource allocation. Defence and Peace Economics, 2011; 22(1):43–61.
16. Alpcan T, Basar T. Network Security: A Decision and Game Theoretic Approach. Cambridge University Press, 2011.
17. Lye KW, Wing J. Game strategies in network security. International Journal of Information Security, 2005; 4:71–86.
18. Roy S, Ellis C, Shiva S, Dasgupta D, Shandilya V, Wu Q. A survey of game theory as applied to network security. In Proceedings of the 37th Hawaii International Conference on System Sciences, 2010.
19. Ten CW, Manimaran G, Liu CC. Cybersecurity for critical infrastructures: Attack and defense modeling. IEEE Transactions on System, Man and Cybernectics: Part A: Systems and Humans, 2010; 40(4):853–865.
20. Honeynet Project. Know Your Enemy: Learning About Security Threats, 2nd ed. Boston, MA: Addison-Wesley Professional, May 2004.
21. Spitzner L. Honeypots: Tracking Hackers. Boston, MA: Addison-Wesley Professional, September 2002.
22. Zhuang J, Bier VM. Reasons for secrecy and deception in homeland-security resource allocation. Risk Analysis, 2010; 30(12):1737–1743.
23. Zhuang J. Impacts of subsidized security on stability and total social costs of equilibrium solutions in an n-player game with errors. Engineering Economist, 2010; 55(2):131–149.
24. Zhuang J, Bier VM, Gupta A. Subsidies in interdependent security with heterogeneous discount rates. Engineering Economist, 2007; 52(1):1–19.
25. Lee EA. Cyber physical systems: Design challenges. In Proceedings of International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing (ISORC), 2008.
26. Sridhar S, Hahn A, Govindarasu M. Cyber–physical system security for the electric power grid. Proceedings of the IEEE, 2011; (99):1–15.
27. Wu FJ., Kao YF, Tseng YC. From wireless sensor networks towards cyber physical systems. Pervasive and Mobile Computing, 2011; 7(4):397–413.
28. He F, Zhuang J, Rao NSV, Ma CY, Yau DK. Game-theoretic resilience analysis of cyber-physical systems. Pp. 90–95 in Proceedings of the IEEE 1st International Conference on Cyber-Physical Systems, Networks, and Applications (CPSNA), 2013.
29. Rinaldi SM. Modeling and simulating critical infrastructures and their interdependencies. In Proceedings of the 37th Hawaii International Conference on System Sciences, 2004.
30. Rao NSV, Ma CYT, Yau DKY. On robustness of a class of cyber-physical network infrastructures. In Proceedings of Workshop on Design, Modeling and Evaluation of Cyber Physical Systems, 2011.
31. Altman E, Boulogne T, El-Azouzi R, Jiménez T, Wynter L. A survey on networking games in telecommunications. Computers & Operations Research, 2006; 33(2):286–311.
32. Brown T, Sarioz D, Bar-Noy A, LaPorta T, Verma D, Johnson M, Rowaihy H. Geometric considerations for distribution of sensors in ad-hoc sensor networks. Technical Report, City Universiy of New York, November 2006. Computer Science Technical Reports, TR-2006014.
33. Zhang P, Peeta S, Friesz T. Dynamic game theoretic model of multi-layer infrastructure networks. Networks and Spatial Economics, 2005; 5(2):147–178.
34. Novak AJ, Feichtinger G, Leitmann G. A differential game related to terrorism: Nash and Stackelberg strategies. Journal of Optimization Theory and Applications, 2010; 144(3):533–555.
35. Papadimitriou CH. The complexity of finding Nash equilibrium. In Nisan N, Roughgarden T, Tardos E, Vazirani VV (eds). Algorithmic Game Theory. Cambridge, MA: Cambridge University Press, 2007.
36. Rao NSV, Ma CYT, He F, Zhuang J, Yau DKY. Cloud computing infrastructure robustness: A game theory approach. In Proceedings of International Conference on Computing, Networking and Communications, 2012.
37. Ma CYT, Rao NSV, Yau DKY. A game-theoretic study of attack and defense in cyber-physical systems. In Proceedings of International Workshop on Cyber-Physical Networking Systems, 2011.