Abstract—We consider a class of infrastructures composed of discrete components that can be disrupted by either cyber or physical attacks, and are protected by cyber and physical reinforcements. We formulate a game between the provider and attacker, wherein their utility functions are in the form of sum of two terms, an infrastructure survival probability term and a cost term. We present a novel formulation that accounts for the cyber-physical interactions in two ways: (i) the conditional survival probabilities of cyber and physical sub-infrastructures are specified by multiples of marginal probabilities at the structure-level, and (ii) the survival probabilities of components are determined by cyber and physical component attacks as well as component reinforcements. We derive Nash Equilibrium conditions in terms of cost terms and component survival probabilities, and obtain provider strategies by combining the cyber and physical parameters. We propose sensitivity functions that highlight the dependence of infrastructure survival probability on cost parameters and component probabilities, under statistical independence conditions. This analysis shows a rather seemingly counter-intuitive qualitative behavior at NE that high costs and lower rewards lead to high infrastructure survival probability. We apply this approach to simplified models of cloud computing infrastructures and energy grids, both with a large number of components.

I. INTRODUCTION

The operation of infrastructures such as smart grids and cloud computing, requires the continued functioning of cyber components such as Supervisory Control And Data Acquisition (SCADA) systems, servers, routers and switches, and also physical components such as power or fiber routes, and cooling and power systems. The components may be disabled and/or disconnected by cyber and physical attacks, which will degrade the infrastructure performance. To counter such disruptions, infrastructure providers are required to adopt strategies that ensure the required levels of operation and availability of both cyber and physical components by taking into account the strategies used by the attacker.

In this paper, we consider a class of infrastructures consisting of discrete cyber and physical components, which must be operational as individual units and also be available such as being connected to the network. These components are subject to individual attacks in that cyber (physical) attacks will disable cyber (physical) components that have not been reinforced. For example, a cyber attack on a server may bring it down, or a physical attack on a fiber route of a network may destroy it. In addition to these direct impacts, there are cyber-physical interactions that make a component unavailable to the infrastructure even though the component by itself is operational, that is, not disabled. For example, a physical attack on a fiber connection to a site that houses servers of a cloud computing infrastructure, will render them unavailable over the network. In addition to the component-level characterization, we consider that all cyber components form the cyber sub-infrastructure, and all physical components form the physical sub-infrastructure. The cyber and physical sub-infrastructures can be separately identified, and are typically operated by different domain experts. For example, SCADA systems of a power grid are maintained by operations staff, whereas the physical power routes are maintained by power engineering staff. A complete disruption of either sub-infrastructure will lead to that of the entire infrastructure, and we consider that conditional probability of failure or unavailability of one sub-infrastructure given the failure of the other can be estimated as a scalar multiplier, which is derived using the underlying structure information.

We consider infrastructures that consist of a large number of uniform components, for example, servers and SCADA systems, such that the overall performance level of the infrastructure is adequately characterized by the number of components that are operational and available. The attacker is expected to launch a certain number of cyber or physical attacks but not both. But, the provider needs to reinforce certain numbers of both cyber and physical components. Thus, there is a basic level of asymmetry between them, although, in some sense, the infrastructure appears as a “uniform” collection of components to both. This characterization is coarser than those that account for specific components, and is intended for infrastructures with a large number of components such as cloud computing infrastructure with thousands of servers or a power grid with hundreds to thousands of SCADA systems. In these systems, the sheer number of components makes it much too complex to account for the individual components, and it is more manageable to deal in terms of the number of components being attacked or reinforced. We focus mainly on the provider who is charged with reinforcing a certain number of cyber and physical components of the infrastructure to defend against the degradations of both kinds (which are specified by the number

1A finer model might require taking into account the specific details of the individual components.
of components attacked). We consider that a component can be reinforced so that it cannot be disabled by a direct attack, but it can be made unavailable as an indirect result of attack on another component, as in the case of a server in the cloud computing infrastructure example.

These infrastructures are characterized by the following considerations:

(a) knowledge about the capabilities and certain locations of the infrastructure is available to the attacker, primarily from public sources;

(b) costs incurred by the provider and attacker are private information and not available to the other;

(c) strategies used by the provider in choosing which parts to reinforce, and by the attacker in choosing which parts to attack are not revealed to the other;

(d) results of attacks are known to the provider and attacker.

These considerations lead to game-theoretic models where information in items (a) and (d) is available to both defender and attacker, and information in items (b)-(c) is private. Both defender and attacker consider that the other utilizes a probabilistic strategy.

Our objective is to gain a qualitative understanding of the interactions between the provider and attacker by utilizing a simultaneous game model. This model is simpler than those used in critical infrastructures such as power distribution, transportation and agriculture [3], since it does not model the dynamics of the underlying phenomena, for example, using partial differential equations to model traffic dynamics. We study methods that are designed to ensure the infrastructure survival in presence of cyber and physical degradations within the framework of game theory [4], [7], [8]. Such characterizations that address system reliability and robustness aspects using a game-theoretic formulation have been considered recently in several applications [2], for example, smart grids [6], cloud computing infrastructures [9], and power systems [5]. Our approach is based on the Stackelberg formulation wherein the infrastructure provider chooses options based on instantaneous information and may re-derive the actions as new information becomes available. This formulation is more reactive and sensitive to dynamic disruptions compared to long-term strategies used in Markov game models [1], [6].

We present a formulation of a game between the provider and attacker, wherein their utility functions are in the form of sum of two terms: (a) infrastructure survival probability term, and (b) cost term. The infrastructure survival probability accounts for cyber-physical aspects in two ways: (i) the conditional survival probabilities of cyber and physical sub-infrastructures are specified by a multiple of marginal probabilities derived at the structure-level, and (ii) component survival probabilities are derived based on the number of cyber or physical attacks, and the number of cyber and physical components reinforced. Nash Equilibrium (NE) represents the attack and reinforcement actions that optimize the utility of attacker and provider based on their individual information, from which neither has a motivation to unilaterally deviate [4]. We derive the Nash Equilibrium conditions in terms of cost terms and the component survival probabilities, typically expressed in terms of number of cyber and physical attacks and reinforcements. The infrastructure provider strategy is derived by combining both cyber and physical parameters. We also estimate the partial derivatives that indicate the sensitivities of infrastructure survival probability with respect to cost parameters and conditional success and failure probabilities of components, under statistical independence conditions. This analysis shows a rather seemingly counter-intuitive qualitative behavior that high costs and lower rewards lead to NE with high infrastructure survival probability.

We apply this approach to simplified models of cloud computing infrastructure and smart energy grid. We first consider the cases where both cyber and physical components are uniform in Section II-B, namely, servers and fiber connections for cloud infrastructures, and SCADA systems and power lines for power grid. Then, we consider two different types of cyber components, namely servers and routers, for cloud infrastructure in Section IV-A, and SCADA systems and power meters in the smart grid in Section IV-B. In these application scenarios we explicitly derive NE conditions and sensitivity functions.

In Section II, we present our discrete component model for the infrastructure and derive survival probabilities at structure- and component-levels. We present our game theoretic formulation in Section III, and derive NE conditions and sensitivity estimates. We apply our analytical results to cloud infrastructure and smart grid applications in Section IV.

II. DISCRETE SYSTEM MODELS

We consider that the infrastructure consists of \( N_C \) cyber components that constitute the cyber sub-infrastructure, and \( N_P \) physical components that constitute the physical sub-infrastructure. Each cyber and physical component must be operational and available to contribute to the infrastructure operation. A component may be unavailable in two ways: it may be operationally disabled, or it is operational but disconnected from the infrastructure. Typically, a component may be disabled by a direct attack, and may be disconnected as an indirect effect of an attack on another component. In particular, a cyber attack may render a physical component unavailable even if it is physically operational, for example, an attack on a SCADA system might disable power flow on a line. And, a physical attack on a component might render cyber components unavailable, for example, fiber cuts to a server site would make all servers unavailable even though they are up and running. We capture these cyber-physical interactions using survival probabilities at two levels: (i) at the structure-level, we utilize the abstractions of cyber and physical sub-infrastructures, and (ii) at the component-level, we consider that cyber attacks affect the availability of physical components, and vice versa. We consider that the number of components of the system to be large so that we abstract out the individual component differences by using probabilities that capture generic cyber and physical components.

A. Cyber-Physical Structural Interactions

The probability that the infrastructure is operational is denoted by \( P_{CP} \). At the structure-level, the probabilities that
the cyber and physical subinfrastructures are operational are denoted by \( P_C \) and \( P_P \), respectively, and their failure probabilities are denoted by \( P_C = 1 - P_C \) and \( P_P = 1 - P_P \), respectively. For the infrastructure to be operational both cyber and physical subinfrastructures must necessarily be operational (and available), and the failure of one in general effects the availability of the other due to component-level cyber-physical interactions. The attacker can disable the infrastructure by bringing down either cyber or physical subinfrastructures. Since the costs of attacking individual subinfrastructures are additive, typically, there is no particular advantage in attacking both parts simultaneously in our formulation. Thus we have

\[
P_{CP} = 1 - [P_C + P_P - P_{CP}] = P_C + P_P - 1 + P_{CP}. \hspace{1cm} (2.1)
\]

The joint probability \( P_{CP} \) is expressed in terms of conditional failure probabilities as: \( P_{CP} = P_{C|P} P_P \) and \( P_{CP} = P_{P|C} P_C \). Using the structural properties of infrastructure, we utilize cyber and physical multipliers, denoted by \( a_C \) and \( a_P \) respectively, to capture the relative importance of cyber and physical parts. The failure probability of cyber sub-infrastructure given that physical sub-infrastructure is disabled is \( P_{C|P} = a_C P_C \). For example, in a cloud computing infrastructure with 100 servers per site, disabling the fiber connection would disconnect all servers at the site, which can be reflected by choosing \( a_C = 100 \). Similarly, we have \( P_{P|C} = a_P P_P \). The cyber-physical multiplier \( a_{CP} = a_C \) or \( a_{CP} = a_P \) captures the effects of cyber and physical multipliers, respectively, which is appropriately chosen based on the details of the infrastructure.

**Condition 2.1:** The probability that infrastructure is operational is expressed in terms of those of cyber and physical subinfrastructures as

\[
P_{CP} = P_C + P_P - 1 + a_{CP}(1 - P_C)(1 - P_P),
\]

where \( a_{CP} = a_C \) or \( a_{CP} = a_P \).

If \( a_C > 1 \), the cyber failures are positively correlated to physical failures, that is, they occur with higher probability following physical failures, since \( P_{C|P} > P_C \). If \( a_C < 1 \) means that cyber failures are negatively correlated to physical failures. The special case \( a_C = 1 \) means that the cyber failures are independent of physical failures. The conditions on \( a_P \) are similarly interpreted. If \( a_{CP} > 1 \), then either cyber failures are positively correlated, or physical failures are positively correlated with the other. Similarly, if \( a_{CP} < 1 \), the failures are negatively correlated with the other.

### B. Component Survival Probabilities

Let \( p_{CR} \) and \( p_{CN} \) denote the probability of survival of a cyber component with and without reinforcement, respectively. Under the assumption of statistical independence of component failures, the probability that the cyber and physical parts survive the attacks are given by

\[
P_C = \frac{1}{\beta_C} \left( \frac{N_C}{x_c} \right)^{p_{CR} N_C - x_c},
\]

and

\[
P_P = \frac{1}{\beta_P} \left( \frac{N_P}{x_p} \right)^{p_{CR} N_P - x_p},
\]

respectively, where \( \beta_C \) and \( \beta_P \) are the corresponding normalization constants. Let \( p_R \) denote the probability that a component is reinforced, such that \( p_{CR} = p_{CR} p_R \) where \( p_{CR} \) is the conditional probability that a reinforced component will survive direct and indirect attacks. Similarly \( p_{CN} = p_{CN} p_R \) is probability that a component is not reinforced, and \( p_{CN} = p_{CN} p_R \) where \( p_{CN} \) is the probability that a non-reinforced component will survive direct and indirect attacks.

We apply normalization by using the probability one event that exactly \( x_c \) cyber components and \( x_p \) physical components are reinforced such that

\[
\left( \frac{N_C}{x_c} \right)^{p_{R}} (1 - p_R)^{N_C - x_c} = \beta_C
\]

and

\[
\left( \frac{N_P}{x_p} \right)^{p_{R}} (1 - p_R)^{N_P - x_p} = \beta_P,
\]

where \( p_R \) is specific to cyber and physical components. By applying this normalization factor, we have the following simpler expression for component survival probabilities:

\[
P_C = p_{CR}^{x_c} p_{CN}^{N_C - x_c} \hspace{1cm} \text{and} \hspace{1cm} P_P = p_{CR}^{x_p} p_{CN}^{N_P - x_p},
\]

**Condition 2.2:** The component failures are statistically independent such that the survival probabilities of cyber and physical subinfrastructures are given by

\[
P_C = p_{CR}^{x_c} p_{CN}^{N_C - x_c} \hspace{1cm} \text{and} \hspace{1cm} P_P = p_{CR}^{x_p} p_{CN}^{N_P - x_p},
\]

respectively.

We now describe two simplified illustrative examples for which we can derive estimates for \( p_{B|R} \) and \( p_{B|N} \), for \( B = C, P \). We will expand further on these examples in Section IV by taking additional details into account.

**Example:** Cloud Computing Infrastructure: We consider a simplified model of a cloud computing infrastructure which consists of several sites each of which houses 100 servers. The servers constitute cyber components which may be disabled by cyber attacks if not cyber-reinforced. The physical fiber connections constitute the physical components of our model, and they can be disrupted by physical attacks; reinforcements in this case could be in the form of redundant, physically separate fiber runs. A physical fiber attack will disconnect all servers at the site from the network, making them unavailable. We assume that both attacker and provider choose the components according to uniform distribution. Thus, the probability that a cyber-reinforced component survives fiber attacks is given by

\[
p_{CR} = \frac{f_{C}}{1 + 100(y_p - x_p)+},
\]

where \( 0 \leq f_{C} \leq 1 \) is appropriately chosen, and \([x]+\) is the non-negative part, that is \([x]+ = x\) for \( x > 0 \), and \([x]+ = 0\) otherwise. This estimate reflects the fact that there is a minimum of \([y_p - x_p]+\) non-reinforced fiber connections, and a cyber component is more likely to be disconnected for higher values of \([y_p - x_p]+\). There is no dependence on \( y_b \) since a cyber attack will not be able to disable a cyber-reinforced component. If the cyber component is not reinforced, it will be brought down by a direct cyber attack, or indirectly by fiber attack but the latter will have a higher impact. Thus, we use the estimate of survival probability as

\[
p_{CN} = \frac{f_{C}}{1 + y_c + 100(y_p - x_p)+},
\]
which reflects the additional lowering of survival probability inversely proportional to the level of cyber attack \( y_c \).

**Example 2: Power Grid Infrastructure:** We consider a simplified model of a power grid controlled by a (cyber) network of SCADA systems, where each system controls the power flow on 5 lines. The SCADA systems constitute the cyber components and the power lines constitute the physical components. A SCADA system may be disabled by cyber means, and we assume that such an event will disrupt the power flow on all 5 associated lines. By using the reasoning analogous to Example 1, we estimate the survival probability of a reinforced power line in presence of \( y_c \) cyber attacks, as

\[
P_{P|R} = \frac{f_p}{1 + 5[y_c - x_c]+}
\]

where \( 0 \leq f_p \leq 1 \) is appropriately chosen. Each power line can be directly disrupted by physical means such that it can be brought down if not reinforced, and a component is more likely to be unavailable if there are more physical attacks, namely, higher \( y_p \). Thus, an attack on a SCADA system will have an amplified effect on power lines compared to direct physical attacks such that

\[
P_{P|N} = \frac{f_p}{1 + y_p + 5[y_c - x_c]+}
\]

provides an estimate of the probability of survival of a non-reinforced power line. □

### III. Game Theoretic Formulation

Consider that the provider chooses to reinforce \( x_c \) cyber components and \( x_p \) physical components, and the attacker attacks \( y_c \) cyber components and \( y_p \) physical components. The provider’s objective is to keep the infrastructure operational and available, which involves selecting a number of components to reinforce at certain costs. We express the provider utility function as a sum of system probability and cost terms

\[
U_D = [P_{CP}(x_c, x_p, y_c, y_p)]g_D - C_D(x_c, x_p),
\]

where \( g_D \) represents the reward of keeping the infrastructure available and \( C_D(\cdot) \) represents the cost incurred in reinforcing the components. When the component reinforcement costs are uniform, we use \( C_D(x_c, x_p) = c_{CD}x_c + c_{PD}x_p \), where \( c_{CD} \) and \( c_{PD} \) are reinforcement costs of cyber and physical components, respectively.

Similarly, the attacker’s utility function is given by

\[
U_A = [1 - P_{CP}(x_c, x_p, y_c, y_p)]g_A - C_A(y_c, y_p)
\]

where \( g_A \) represents the reward of disabling the infrastructure and \( C_A(\cdot) \) represents the cost of attacking the components. When the attack costs are uniform, we use \( C_A(y_c, y_p) = c_{CA}y_c + c_{PA}y_p \), where \( c_{CA} \) and \( c_{PA} \) are the attack costs of cyber and physical components, respectively, and only one of \( y_c \) and \( y_p \) is non-zero.

#### A. Nash Equilibrium Conditions

We consider large numbers of cyber and physical components so that the qualitative behavior of the system can be described using derivatives of \( x_a \) and \( y_a \), \( a = c, p \). Then, Nash Equilibrium conditions are derived by equating the corresponding derivatives to zero, which yields

\[
\begin{align*}
\frac{\partial U_D}{\partial x_a} &= \frac{\partial P_{CP}}{\partial x_a}g_D - \frac{\partial C_D}{\partial x_a} = 0 \\
\text{for } a = c, p &\text{ for the provider, and} \\
\frac{\partial U_A}{\partial y_a} &= -\frac{\partial P_{CP}}{\partial y_a}g_A - \frac{\partial C_A}{\partial y_a} = 0 \\
\text{for } a = c, p &\text{ for the attacker.}
\end{align*}
\]

where \( (z, a, E, B) = (x, c, C, D), (x, p, P, D), \) and \( m_D = 1 \) correspond to the provider, and \( (z, a, E, B) = (y, c, C, A), (y, p, P, A) \) and \( m_A = -1 \) correspond to the attacker.

We define the cyber-physical differential

\[
\frac{\partial z_c}{\partial x_p} = \frac{\partial P_{CP}}{\partial x_p}/\frac{\partial P_{CP}}{\partial z_c} = \frac{\partial P_{CP}}{\partial x_p}/\frac{\partial P_{CP}}{\partial z_x} = \theta_B(x_c, x_p, y_c, y_p)
\]

which indicates the relative importance of cyber and physical parts such that \( z = x \) and \( B = D \) for the provider, and \( z = y \) and \( B = A \) for the attacker. When component costs are used, we have

\[
\theta_B(x_c, x_p, y_c, y_p) = \frac{c_{PB}}{c_{CB}},
\]

for \( B = A \) for the attacker and \( B = D \) for the provider, which solely depends on component costs.

We now consider that the effects of reinforcement and attacks on cyber and physical sub-infrastructures can be separated such that most of the interactions are captured at the component level, more precisely, \( \frac{\partial P_c}{\partial z_x} \approx 0 \) and \( \frac{\partial P_c}{\partial z_x} \approx 0 \) for \( z = x, y \). Intuitively, these conditions indicate that at the structure-level, only direct impacts are dominant, for example, cyber reinforcements contribute to improving the cyber sub-infrastructure but not directly to physical sub-infrastructure. Consequently, we have for the defender the following condition.

**Condition 3.1:** For \( P_C \) in Condition 2.1, we have

\[
\frac{\partial P_{CP}}{\partial x_c} \approx [1 - a_{CP}(1 - P_{P})]\frac{\partial P_{CP}}{\partial x_c}
\]

\[
\frac{\partial P_{CP}}{\partial x_p} \approx [1 - a_{CP}(1 - P_{C})]\frac{\partial P_{CP}}{\partial x_p}
\]

for the defender. □

#### B. OR Systems

Before we present the general result in the next section, we first consider a special case where the probability of simultaneous failures of cyber and physical sub-infrastructures is negligible. Consequently, the infrastructure will fail if either of the physical or cyber sub-infrastructures fails such that \( P_{CP} = P_C + P_P \), and such infrastructures are called OR Systems. In this case, the dependence of \( P_{CP} \) on system parameters at NE is easier to derive and interpret, since it will turn out to be determined entirely by component-level
cyber-physical interactions without requiring the structure-level interactions.

**Condition 3.2:** The probability of simultaneous failures of cyber and physical sub-infrastructures is low, $P_{CP} = 1 - (P_C + P_P)$, such that $P_{CP} = 1 - (P_C + P_P) ≈ 0$.

Under this condition, we have a much simpler form of Condition 3.1 given by $\frac{\partial P_C}{\partial x_c} \approx \frac{\partial g_C}{\partial x_c}$ and $\frac{\partial P_P}{\partial x_p} \approx \frac{\partial g_P}{\partial x_p}$. At NE, we have

$$\frac{\partial P_C}{\partial x_c} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_c} \quad \text{and} \quad \frac{\partial P_P}{\partial x_p} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_p}.$$  

We now estimate the partial differentials on the left hand side for these terms by using the specific forms $P_C = P_{C|R}^N P_{C|N}$ and $P_P = P_{P|R}^N P_{P|N}$ from Condition 2.2. For this estimation, we utilize the following general formula.

**Lemma 3.1:** For $f(x) = a^x b^{N-x}$, we have $\frac{\partial}{\partial x} f(x) = \ln(a/b) f(x)$.

**Proof:** We take ln on both sides of $f(x)$, and differentiate them with respect to $x$. Then, an algebraic manipulation yields the above formula. □

By applying the above formula from Lemma 3.1 to $\frac{\partial P_C}{\partial x_c}$ and $\frac{\partial P_P}{\partial x_p}$, we obtain the following estimates for the survival probabilities of cyber and physical sub-infrastructures:

$$\tilde{P}_{P:D}(x_p, y_c, y_p) = \frac{\partial C_D}{\partial x_p} \frac{g_D}{\ln \left( \frac{p_{P|R}^{x_p}}{p_{P|N}} \right)}$$

$$\tilde{P}_{C:D}(x_c, y_c, y_p) = \frac{\partial C_D}{\partial x_c} \frac{g_D}{\ln \left( \frac{p_{C|R}^{x_c}}{p_{C|N}} \right)}$$

which provide sensitivity estimates within a “small” locality of NE. These estimates are based on first-order partial derivatives $\frac{\partial P_C}{\partial x_c}$ and $\frac{\partial P_P}{\partial x_p}$, wherein the component probabilities $p_{P|R}, p_{P|N}, p_{C|R}, p_{C|N}$ are assumed to be constant. Consequently, the conclusions are valid only within the corresponding NE locality, and, in particular, further dependencies of component probabilities must be taken into account to derive global trends. When component costs are used, these will be further simplified to

$$\tilde{P}_{P:D}(x_p, y_c, y_p) = \frac{c_{P:D}}{g_D \ln \left( \frac{p_{P|R}^{x_p}}{p_{P|N}} \right)}$$

$$\tilde{P}_{C:D}(x_c, y_c, y_p) = \frac{c_{C:D}}{g_D \ln \left( \frac{p_{C|R}^{x_c}}{p_{C|N}} \right)}.$$  

These estimates provide qualitative information about the sensitivity of survival probabilities of cyber and physical parts in terms of costs and component-level survival probabilities. First observation is that these estimates involve only component-level probabilities of the same type, namely $\tilde{P}_{P:D}$ and $\tilde{P}_{C:D}$ depend only on the probabilities of physical and cyber components, respectively. In particular, they do not involve structure-level interactions but the component probabilities capture the cyber-physical interactions since they depend on both cyber and physical component attacks and reinforcements.

For both cyber and physical parts, the survival probabilities are proportional to component costs and inversely proportional to reward terms $g_D$. At a first look, this looks counter intuitive, but this characterization applies to the set of Nash equilibria and not to system behavior as a whole. In part, it is an artifact of the multiplicative term $g_D$ in the provider’s utility function, instead of just being $P_{CP}$ alone. Because of the maximization of the additive utility term, at NE, a higher utility indeed can be achieved at lower $P_C$ or $P_P$ for a given gain term $g_D$. Qualitatively, at NE, the partial derivative of $P_C$ is directly proportional to the cost and inversely proportional to the reward term $g_D$. But under Lemma 3.1, the partial derivative is indeed proportional to $P_C$ itself with the multiplication term $\ln \left( \frac{p_{C|R}}{p_{C|N}} \right)$, and hence has the same qualitative behavior as its partial derivative. In addition, both $\tilde{P}_{P:D}$ and $\tilde{P}_{C:D}$ depend on the component survival probabilities in a qualitatively similar way: (a) higher survival probability of reinforced component leads to lower infrastructure survival probability, and (b) higher survival probability of non-reinforced component leads to higher infrastructure survival probability.

From the provider’s perspective, qualitative information about the dependence of $P_{CP}$ can be inferred using the estimate

$$\tilde{P}_{C:P,D}(x_c) = \int \frac{\partial P_{CP}}{\partial x_c} dx_c = \frac{c_{CD}}{g_D} x_c$$

that utilizes the partial derivative as a linearized approximation of $\frac{\partial P_{CP}}{\partial x_c}$. It shows that the system survival probability at NE is inversely proportional to $g_D$ and directly proportional to component cost $c_{CD}$ and level of reinforcement $x_c$.

**C. Statistical Independence of Cyber and Physical Sub-Infrastructures**

We consider the special case $a_{CP} = 1$ such that $P_{C|P} = P_C$, or $P_{P|C} = P_P$, or both, such that the cyber sub-infrastructure failures are statistically independent of physical sub-infrastructure failures, and vice versa. Under this condition, the survival probabilities of the cyber and physical sub-infrastructures are also statistically independent such that $P_{CP} = P_C P_P$.

At NE we have

$$\frac{\partial P_C}{\partial x_c} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_c} \quad \text{and} \quad \frac{\partial P_P}{\partial x_p} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_p}.$$  

We now substitute expressions for $\frac{\partial P_C}{\partial x_c}$ and $\frac{\partial P_P}{\partial x_p}$ based on Lemma 3.1, and obtain the system of equations:

$$\tilde{P}_{C:D} \tilde{P}_{P:D} = \frac{\partial C_D}{\partial x_p} \frac{g_D}{\ln \left( \frac{p_{P|R}}{p_{P|N}} \right)}$$

$$\tilde{P}_{P:D} \tilde{P}_{C:D} = \frac{\partial C_D}{\partial x_c} \frac{g_D}{\ln \left( \frac{p_{C|R}}{p_{C|N}} \right)}.$$  

Qualitatively, at NE, the survival probabilities of cyber and physical sub-infrastructures have an inverse relationship, but
their product is determined by cost terms and component survival probabilities in a manner similar to individual probabilities $\hat{P}_{C,D}$ and $\hat{P}_{P,D}$ of previous section.

**D. NE Sensitivity Functions**

We now estimate approximations of $P_C$ and $P_P$ under Conditions 2.1, 2.2 and 3.1, to obtain qualitative information about their sensitivities to different parameters from the provider’s perspective.

**Theorem 3.1:** Under Conditions 2.1-2.2 and 3.1, for $a_{CP} \neq 1$, an estimate of the survival probability of physical sub-infrastructure is

$$\hat{P}_{P,D}(x_c, x_p, y_c, y_p) = \frac{d_{PD} - d_{CD}}{2(1 - a_{CP}) - \frac{1}{2a_{CP}}} \pm \frac{1}{2a_{CP}} \sqrt{\left(\frac{a_{CP}(d_{PD} - d_{CD})}{1 - a_{CP}} - (1 - a_{CP})\right)^2 + 4a_{CP}d_{PD}},$$

and an estimate of the survival probability of cyber sub-infrastructure is

$$\hat{P}_{C,D}(x_p, x_c, y_c, y_p) = \frac{d_{CD} - d_{PD}}{2(1 - a_{CP}) - \frac{1}{2a_{CP}}} \pm \frac{1}{2a_{CP}} \sqrt{\left(\frac{a_{CP}(d_{CD} - d_{PD})}{1 - a_{CP}} - (1 - a_{CP})\right)^2 + 4a_{CP}d_{CD}},$$

where

$$d_{PD}(x_p, y_c, y_p) = \frac{\partial C_D}{\partial x_p} \ln \left(\frac{p_{P|R}}{p_{P|N}}\right),$$

$$d_{CD}(x_c, y_c, y_p) = \frac{\partial C_D}{\partial x_c} \ln \left(\frac{p_{C|R}}{p_{C|N}}\right).$$

**Proof:** At NE, we have $\frac{\partial P_{C,D}}{\partial x_c} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_c}$ and $\frac{\partial P_{P,D}}{\partial x_c} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_c}$. By using the formulae in Condition 3.1, we have

$$[1 - a_{CP}(1 - P_C)] \frac{\partial P_C}{\partial x_c} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_c},$$

$$[1 - a_{CP}(1 - P_P)] \frac{\partial P_P}{\partial x_c} = \frac{1}{g_D} \frac{\partial C_D}{\partial x_c}.$$

We now substitute expressions for $\frac{\partial P_{C,D}}{\partial x_c}$ and $\frac{\partial P_{P,D}}{\partial x_c}$ based on Lemma 3.1, and obtain the system of equations:

$$P_C [1 - a_{CP}(1 - P_C)] = \frac{\partial C_D}{\partial x_c} \ln \left(\frac{p_{P|R}}{p_{P|N}}\right),$$

$$P_P [1 - a_{CP}(1 - P_P)] = \frac{\partial C_D}{\partial x_c} \ln \left(\frac{p_{C|R}}{p_{C|N}}\right).$$

Then, we have

$$P_C - P_P = \frac{d_{CD} - d_{PD}}{1 - a_{CP}},$$

where we represent $d_{PD}(x_p, y_c, y_p)$ and $d_{CD}(x_c, y_c, y_p)$ by simply $d_{PD}$ and $d_{CD}$, respectively. By using $P_C$ from this equation in

$$P_P [1 - a_{CP}(1 - P_C)] \frac{\partial P_P}{\partial x_c} = d_{PD}$$

we obtain the quadratic equation

$$a_{CP}P_P^2 - \left[\frac{d_{PD} - d_{CD}}{1 - a_{CP}} - (1 - a_{CP})\right] P_P - d_{PD} = 0.$$

Solution to this equation provides $\hat{P}_{P,D}(x_c, x_p, y_c, y_p)$, which in turn yields $\hat{P}_{C,D}(x_c, x_p, y_c, y_p)$. □

Compared to the case of OR Systems described in the previous section, there is a significant level of cyber-physical interactions in $\hat{P}_{P,D}(x_c, x_p, y_c, y_p)$ and $\hat{P}_{C,D}(x_c, x_p, y_c, y_p)$, which both depend on $d_{PD}(x_p, y_c, y_p)$ and $d_{CD}(x_c, y_c, y_p)$. In particular, they both are affected by survival probabilities of cyber and physical components, each of which in turn depends on the number of both cyber and physical component attacks and reinforcements.

The cyber-physical multiplier $a_{CP}$ affects these quantities in much more complicated manner than its multiplier role in Condition 2.1. Since $0 \leq P_C \leq 1$, we have $0 \leq a_{CP} \leq \frac{1}{\max\{P_C, P_P\}}$, which implies $a_{CP}$ can take values both higher and lower than 1. Both $\hat{P}_{P,D}(x_c, x_p, y_c, y_p)$ and $\hat{P}_{C,D}(x_c, x_p, y_c, y_p)$ depend on the difference of components costs, as opposed to depending on components of the same type as in the case or OR Systems. Furthermore, the nature of dependence reverses as $a_{CP}$ crosses 1, reflecting the effects of positive and negative correlations between the cyber and physical parts. For $a_{CP} < 1$, $\hat{P}_{P,D}$ and $\hat{P}_{C,D}$ are directly proportional to cyber and physical component costs, respectively, and this relationship reverses for $a_{CP} > 1$. Similarly, for $a_{CP} < 1$, $\hat{P}_{P,D}$ and $\hat{P}_{C,D}$ depend on components of the corresponding type, namely physical and cyber component survival probabilities, respectively, as follows: (a) higher survival probability of reinforced component leads to lower sub-infrastructure survival probability, and (b) higher survival probability of non-reinforced component leads to higher sub-infrastructure survival probability. And, $\hat{P}_{P,D}$ and $\hat{P}_{C,D}$ depend on components of other type, namely cyber and physical component survival probabilities, respectively, in the opposite way. For $a_{CP} > 1$, the qualitative behavior reverses in the cases above, which illustrates the significant impact of the structure-level cyber-physical correlation on the overall behavior of the infrastructure.

E. Survival Probabilities of Cyber and Physical Sub-Infrastructures

It is instructive to compare the two survival probabilities of cyber and physical sub-infrastructures, $P_C$ and $P_P$, respectively, since minimum of the two determines the survival of the infrastructure. We have

$$P_C - P_P = \frac{d_{CD} - d_{PD}}{1 - a_{CP}}.$$
Then the relationship between $P_C$ and $P_P$ is determined as follows:

(a) $d_{CD} > d_{PD}; a_{CP} > 1$: $P_C = P_P - \Delta_a$ for $\Delta_a \geq 0$
(b) $d_{CD} > d_{PD}; a_{CP} < 1$: $P_C = P_P + \Delta_b$ for $\Delta_b \geq 0$
(c) $d_{CD} < d_{PD}; a_{CP} > 1$: $P_C = P_P + \Delta_c$ for $\Delta_c \geq 0$
(d) $d_{CD} < d_{PD}; a_{CP} < 1$: $P_C = P_P - \Delta_d$ for $\Delta_d \geq 0$

It shows that both relative component costs and cyber-physical multiplier $a_{CP}$ can independently determine which part has the higher probability of survival. The difference in the survival probabilities of cyber and physical parts depends on the difference in component costs, as expected. But, the exact nature depends on the 1-crossing point of $a_{CP}$; in particular, the dependence reverses as the cyber and physical parts are switched from being positively correlated to negatively correlated.

IV. APPLICATION EXAMPLES

In this section, we incorporate additional details into Examples 1 and 2 described in Section II-B. We consider that there are different types of cyber and physical components such that $x_a^a$, $a \in A_C$, corresponds to cyber components of type $a$, and $x_b^b$, $b \in A_P$, corresponds to physical components of type $b$. Thus, we have $x_c = \sum_{a \in A_C} x_a^a$ and $x_p = \sum_{b \in A_P} x_b^b$. Now we generalize Condition 3.1 as follows.

Condition 4.1: The component failures are statistically independent such that

$$P_C = \prod_{a \in A_C} \left(\frac{p_{C|R}^a}{p_{P|N}^a}\right)^{x_a^a} \frac{N_C - x_c}{1 + 100 \left[ y_c + y_c^R \right] + 100 \left[ y_c - x_c^R \right] + y_c^R},$$

$$P_P = \prod_{b \in A_P} \left(\frac{p_{P|R}^b}{p_{P|N}^b}\right)^{x_b^b} \frac{N_P - x_p}{1 + 100 \left[ y_p - x_p \right] + y_p^R}.$$

By proceedings as in Section II-B, we obtain the following conditions using Lemma 3.1: for $a \in A_C$, $b \in A_P$

$$\frac{\partial P_C}{\partial x_c^a} = P_C \ln \left(\frac{p_{C|R}^a}{p_{P|N}^a}\right)$$

and

$$\frac{\partial P_P}{\partial x_p^b} = P_P \ln \left(\frac{p_{P|R}^b}{p_{P|N}^b}\right),$$

where $p_{C|R}^a$ and $p_{P|R}^b$ denote the probabilities of reinforced cyber component of type $a$ and reinforced physical component of type $b$, respectively. These estimates can be used for evaluating $F_B$ and $F_B$, for $B = C, P$ as described in previous sections, when there are different types of cyber and physical components. The overall conclusions are qualitatively quite similar to the simpler cases of uniform components.

A. Cloud Computing Infrastructure

We now consider that in the cloud computing infrastructure of Example 1 all servers at a site are connected via a single gateway router to the network. A physical fiber attack will disconnect all servers at the site from the network, making them unavailable, and a cyber attack on the gateway router will also have the same effect. The multiplier $a_{CP}$ would be computed appropriately at the structure-level to reflect it, and the component survival probabilities are computed using more detailed formulae derived above. Now, we separate the cyber components into two classes, namely, server and routers, and $x_c = x_c^S + x_c^R$ such that $x_c^S$ and $x_c^R$ denote the number of reinforced servers and routers, respectively. Similarly, $y_c = y_c^S + y_c^R$ such that $y_c^S$ and $y_c^R$ denote the number of servers and routers attacked, respectively. The cyber component probabilities are computed separately for servers and routers, denoted by $P_{C|R}^S$ and $P_{C|R}^R$, respectively. The probability that a cyber-reinforced server survives fiber or router attacks is given by

$$P_{C|R}^S = \frac{f_C}{1 + 100 \left[ y_c^S + y_c^R \right] + 100 \left[ y_c^S - x_c^R \right] + y_c^R},$$

which now depends on both physical attacks on fiber and cyber attack on routers. Then an estimate of the probability that cyber-reinforced router survives a fiber attack is given by

$$P_{C|R}^R = \frac{f_C}{1 + \left[ y_p - x_p \right] + y_p^R},$$

since a cyber attack on a reinforced router has no impact and a fiber attack will disconnect only one router. If the router is not cyber-reinforced, then we have

$$P_{C|N}^R = \frac{f_C}{1 + \left[ y_p - x_p \right] + y_p^R}.$$

By using these estimates for the router, we have

$$d_{CD}^R = \gamma \ln \left(\frac{1 + 100 \left[ y_p - x_p \right] + 100 \left[ y_c^S - x_c^R \right] + y_c^S}{1 + y_p^R}\right),$$

which increases in the number of attacks on non-reinforced fiber routes and decreases in the number of cyber router attacks. If the cyber component, server or router, is not reinforced, it will be brought down by a direct cyber attack, or indirectly by fiber attack but the latter will have more impact. However, cyber attacks on servers and routers will have different impacts on the availability of the infrastructure, namely a server attack will just bring it down but a router attack will make all 100 servers unavailable. Thus, for server that is not cyber-reinforced, we use the estimate

$$P_{C|N}^S = \frac{f_C}{1 + 100 \left[ y_p - x_p \right] + 100 \left[ y_c^S - x_c^R \right] + y_c^S},$$

which reflects the additional lowering of survival probability inversely proportional to the level of cyber attack $y_p^S$, and to $y_c^R$ but amplified by a factor 100. Thus for servers we have,

$$d_{CD}^S = \gamma \ln \left(\frac{1 + 100 \left[ y_p - x_p \right] + y_p^S}{1 + 100 \left[ y_p - x_p \right] + y_p^R}\right),$$

which increases in the number of attacks on non-reinforced fiber connections but decreases in the number of cyber attacks on non-reinforced routers multiplied by 100 and also in the total number of cyber attacks on servers. The survival probabilities of physical fiber components depend on $x_p$ and $y_p$ such that

$$p_{P|R} = \frac{f_P}{1 + \left[ y_p - x_p \right] + y_p^R}$$

and

$$p_{P|N} = \frac{f_P}{1 + y_p^R}.$$
which increases in the number of physical attacks but decreases in the number of attacks on non-reinforced fiber components. By combining the two formulae for fiber, we have

\[ d_{PD} = \frac{c_{PD}}{g_D \ln \left( \frac{1 + [y_p - x_p]_+}{1 + y_p} \right)} , \]

which increases in the number of physical attacks but decreases in the number of attacks on non-reinforced fiber components. In addition to \( d_{PD} \) and \( d_{PD}^B \), for \( B = S, R \), the survival probabilities of cyber and physical sub-infrastructures are determined by the correlation multiplier \( a_{CP} \) as described in Section III-E.

B. Smart Grid Infrastructure

The power grid model described in Example 2 is enhanced with smart meters on the lines that provide demand information to the generation and distribution control systems. The smart meters can be attacked by cyber means so that the demand information can be manipulated, for example, to make it zero. Now, we separate the cyber components into two classes, namely, SCADA systems and smart meters, and \( x = x_c + x_m \) such that \( x_c \) and \( x_m \) denote the number of reinforced SCADA systems and meters, respectively. Similarly, \( y = y_c + y_m \) such that \( y_c \) and \( y_m \) denote the number of SCADA systems and meters attacked, respectively. The survival probabilities of the power supply lines with and without reinforcement are denoted by \( p_{P|R} \) and \( p_{P|N} \), respectively. A SCADA system or a meter may be disabled by cyber means, which will disrupt the power flow on the lines so that

\[ p_{P|R} = \frac{1}{1 + 5[y_c - x_c]_+ + [y_m - x_m]_+}, \]

for physically-reinforced power lines; notice that cyber attacks on SCADA systems are amplified 5 times compared to attacks on smart meters. Each power line can be directly disrupted by physical means such that it can be brought down if not reinforced, and thus we have

\[ p_{P|N} = \frac{1}{1 + [y_p - x_p]_+ + 5[y_c - x_c]_+ + [y_m - x_m]_+}, \]

which reflects the amplified effect of cyber attacks on SCADA systems compared to physical line attacks. Combining the two formulae we have

\[ d_{PD} = \frac{c_{PD}}{g_D \ln \left( 1 + \frac{[y_p - x_p]_+}{[y_p - x_p]_+ + [y_m - x_m]_+} \right)} , \]

which decreases in the number of attacks on non-reinforced power lines, and increases in the number of attacks on non-reinforced SCADA systems and non-reinforced meters but the former effect is amplified 5 times. The survival probabilities of cyber components are given by

\[ p_{C|R}^B = \frac{1}{1 + [y_c - x_c]_+} \quad \text{and} \quad p_{C|N}^B = \frac{1}{1 + y_p}, \]

for \( B = S, M \). Then we have \( d_{CD}^B = \frac{c_{CD}}{g_D \ln \left( \frac{1 + y_p}{1 + [y_p - x_p]_+} \right)} \), for \( B = S, M \), which decreases in the total number of cyber attacks but increases in the number of attacks on non-reinforced cyber attacks. The net effect of the numbers of attacks and reinforcements on the survival probabilities of cyber and physical sub-infrastructures is also determined by correlation multiplier \( a_{CP} \) in addition to \( d_{PD} \) and \( d_{PD}^B \), for \( B = S, M \), as described in Section III-E.

V. Conclusions

We studied a class of infrastructures composed of a large number of discrete components that can be disrupted by either cyber or physical attacks, and are protected by cyber and physical reinforcements. Using a game-theoretic formulation, we capture the cyber-physical interactions in two ways: conditional survival probabilities of cyber and physical sub-infrastructures at the structure-level, and the survival probabilities of components determined by the number of cyber and physical component attacks and reinforcements. We derived Nash Equilibrium conditions in terms of cost terms and component survival probabilities, and estimated the sensitivity functions that indicate the dependence of infrastructure survival probability on cost parameters, component probabilities and the correlation multipliers of cyber and physical sub-infrastructures. We applied this approach to models of cloud computing infrastructures and energy grids at different levels of abstraction when both have a large number of components.

This formulation could be extended in several ways in future studies. It would be interesting to study sequential game formulations of this problem, and cases where different levels of knowledge are available to each party. Applications of our approach to more detailed models of cloud computing infrastructure, smart energy grid infrastructures and high-performance computing complexes would be of future interest.

Acknowledgments

This work is 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