An Outline of the Three-Layer Survivability Analysis Architecture for Strategic Information Warfare Research

Zhanshan (Sam) Ma   Axel W. Krings   Frederick T. Sheldon
ma@vandals.uidaho.edu   krings@uidaho.edu   sheldon@ornl.gov
University of Idaho, Moscow, ID. Oak Ridge National Laboratory, Oak Ridge, Tennessee.

ABSTRACT

We apply the *three-layer survivability analysis* architecture developed by Ma & Krings (Ma & Krings 2009, Ma 2008) in the context of distributed networks (such as wireless sensor networks) to the study of strategic information warfare. To simplify the research problem, we assume that the information warfare (IW) is conducted in an isolated paradigm, which we call an *electronic cosmos* (*e-cosmos*), i.e., independent of other national and/or war strategies, which is not realistic but allows us to develop a manageable mathematical architecture for modeling and simulation. In this architecture issues outside the cosmos, such as other national or war strategies, are abstracted and represented with the vectors of environmental covariates. This architecture integrates four closely related fields: reliability analysis, survivability analysis, dynamic hybrid fault models, and agent-based computing under a unified architecture. Analogically, it draws on biological inspiration from the studies on metapopulation dynamics, animal communication networks and conflict resolution, social learning and social foraging in behavioral and cognitive ecology. Mathematically, the architecture consists of three layers and is formulated around the core concept of dynamic hybrid fault models—the notion of "*Byzantine generals playing the evolutionary game*." The three-layer architecture includes a set of definitions, models and approaches: The *tactical level* deals with unpredictable, latent, unobserved or unobservable risks (*UUUR*) by utilizing survival analysis and its sister technologies. The *strategic level* integrates *dynamic hybrid fault models* (Ma & Krings 2008, Ma 2008) and tactical level models. From the strategic level, the evolutionary stable strategy (ESS) prescribes the *sustainable* or *survivable* strategies. In the third level—*operational level*—a duo of survivability metrics, action *threshold survivability* (TS) and the *expected survivability* (ES), are defined to help implement the survivable strategies. This new approach requires neither the knowledge of the probabilities of UUUR events nor the assignment of subjective probabilities. In addition, we subscribe to Deibel's (2007) concept of hierarchical strategies and consider IW strategy as simply a layer in a multi-layer structure of the *national strategy*. Due to the generalities of the mathematical approaches adopted in the architecture and of the architecture itself, the methodology we develop (temporality termed *enhanced evolutionary game theory*) may be applied to an expanded cosmos—when the strategic IW is put into a larger context such as warfare strategy.[1]

The Fifth CSIIRW2009, April 13-15, Oak Ridge National Laboratory, Tennessee, USA, Copyright © 2009 ACM 978-1-60558-518-5... $5.00

Keywords: Information Warfare, Information Security, Survivability, Three-layer Survivability Analysis, Dynamic Hybrid Fault Models, Byzantine Generals Playing Evolutionary Game, Enhanced Evolutionary Game Theory, Survival Analysis.

1. INTRODUCTION

Two fundamental elements manipulated in any warfare are the energy and information. Information is therefore essential for any warfare. What distinguishes *strategic information warfare* (IW) from the traditional use of information in warfare or other digital attacks in some specific domains (such as unauthorized hacking, computer crimes, and economic espionage) lies in that strategic IW is a means for state or non-state actors to achieve objectives by digital attacks on its adversary's centers of gravity (Rattray 2001). Furthermore, the center of gravity generally refers to the *national information infrastructure* (NII). According to Rattray (2001), *information infrastructure* is defined as: "a collection set of computer hardware and software, data storage and generating equipment, abstract information and its applications, trained personal and interconnections between all these components." The NII is vital to the following seven sectors of activities: national security, vital human services, other government services, public utilities, general commercial users, commercial information technology producers and providers, commercial network operators and service providers Rattray (2001). This list of sectors of activities mirror the critical national infrastructure established by the US President's Commission on Critical Infrastructure Protection (PCCIP). From this perspective, IW is closely related to the research on survivable network systems (SNS) and survivability.

There are three general categories of attacks against information infrastructure: mechanical, electromagnetic, and digital attacks, with the digital attacks attracting most attention. Digital attack is a type of micro-force and "weapon of ultimate precision" (Rattray 2001). These and other complex issues such as proper use of IW, boundaries of IW, and even what constitutes a digital attack are still actively researched. Overall, there is a huge amount of literature on IW [23], including the study of IW, in the broader context of Information Operations (IO) that also includes four other pillar capabilities: psychological operations (PSYOP), military deception (MILDEC), operations security (OPSEC) and electronic warfare (EW) (Paul 2008). However, the number of *quantitative* studies of IW seems disproportionally fewer. In this article, we are concerned with developing a mathematical framework to study the strategic IW. We set two objectives: (*i*) identify fundamental characteristics of strategic IW from the perspective of mathematical modeling (Section 2); (*ii*) outline a mathematical modeling framework (Section 3–5) with the focus on defensive IW by applying the three-layer survivability analysis architecture, which was developed in the context of survivability of distributed systems such as wireless sensor networks (WSN). Finally, we present a summary and a discussion on the future research topics.

2. CHALLENGES IN MODELING OF IW AND OUTLINE OF THE APPROACHES

2.1 Existing Research

Game theory is perhaps the most frequently applied mathematical technique for studying warfare and the study of IW is not an exception. Although there are many quantitative studies on warfare strategies and information securities, strictly speaking, few studies on strategic information warfare have been quantitative. Some of the quantitative studies labeled as IW or Cyber war actually fall in the scope of information security.

It appears that there are two major types of mathematical approaches being used in the study of IW. One is risk analysis and modeling, and another is the game-theoretic modeling approach. The examples of the former type include: Cohen (1998), Schneier (2000) and numerous studies performed in the context of information security. As observed by Jormakka & Mölsä (2005) in the context of risk analysis with the attack tree: "It seems, however, impossible to assign probabilities to various attack types. It is naturally possible to estimate the probabilities of particular attack types using some large set of analysed cases, but such probabilities do not predict the situation in special cases. The success probability of using an exploit is strongly time dependent: a vulnerability is first known only to a few, then public scripts exploiting this vulnerability will be available, and finally the associated security patch will be installed on most vulnerable computers and the exploit will no longer be useful. This time dependency associated with lack of knowledge makes building and updating a detailed attack tree practically impossible." We concur that the inability to estimate attack probabilities is a reality and also an inherent fundamental constraint in any study on information security and information warfare. Indeed, this is the very same issue in survivability analysis that Ma & Krings (Ma & Krings 2009, Ma 2008) addressed by introducing the notion of UUUR (*Unpredictable, latent, Unobserved or Unobservable Risks*) events and corresponding mathematical approaches to deal with them. In survivability analysis, fundamental difficulties emerge when one tries to quantitatively describe (*i*) the probabilities of malicious events and associated risks, which are usually *unpredictable*, (*ii*) the ignored risks (*latent*, *unobserved* or *unobservable*), and (*iii*) to a lesser extent, catastrophic natural disasters. These risks were collectively denoted as UUUR (Ma & Krings 2009, Ma 2008).

The second type of modeling, game-theoretic approach, has been used in warfare research extensively, but few applications to IW have been performed. Kumar and Marbukh (2003) proposed to model network survivability as a game model. Jormakka & Mölsä (2005) also approached IW with game theory models. They presented four example games to illustrate the different requirements for an effective playing strategy in IW. The four games they described are: terrorist game—bold strategy can result in domination; evildoer game—mixed defense strategies can reduce domination (e.g., for defense against new virus); vandal game—domination can only have a limited time span (e.g., denial of service attack); meta-strategies—modifying observations and orientation of the enemy in the well-known OODA-loop (Observation, Orient, Decision, and Action). The last game is probably the most useful for IW study, but Jormakka & Mölsä (2005) only outlined the general idea—deception (making the threat credible to enemies). Despite the *ad-hoc* (to specific scenarios) nature of the study, Jormakka & Mölsä (2005) indeed revealed a few limitations of the traditional game-theoretic approach. The first one is *rationality* assumption and "it is impossible to predict the outcome of a play if some players are irrational" (Jormakka & Mölsä 2005). Secondly, the mixed strategies still require the probability distribution of strategies to be taken by players. Thirdly, credibility is a central issue in dynamic games, which is actually central to any warfare, the issue of deception. Whether or not the enemy will be deceived is another uncertainty that affects the outcome of the games. In this study, we are particularly interested in addressing these three limitations.

Just as in the field of risk analysis, these three issues associated with traditional game theory are also mirrored in survivability research. It is these issues that prompted the proposal of dynamic hybrid fault (DHF) models and the three-layer survivability analysis by Ma and Krings (Ma & Krings 2008e, Ma 2008). DHF modeling is a new concept that extends traditional hybrid fault models from Agreement algorithms with time-dependent hazard functions from survival analysis and evolutionary game theory (Byzantine Generals playing Evolutionary Games). Unlike in traditional games, evolutionary games do not assume *rationality* and strategies are dynamically evolved. DHF models provide effective measures to deal with the *uncertainty* and *deception*—the second and third limitations associated with the traditional games. In the DHF models, the second issue with traditional games is addressed via UUUR and time-dependent hazard function for players, and the third issue is addressed via voting mechanisms from Agreement algorithms.

2.2 A Conceptual Model of Information Warfare

Deibel (2007) specified the strategies of a nation state as, from top down, national strategy, foreign affair strategy, national security strategy, grand strategy, and military strategy. The strategy of IW is very likely to be a sub-layer in the military strategy or parallel with military strategy, depending on the scope of IW. In this study, we assume that IW is conducted in an isolated cosmos and all the strategies above the strategic IW layer are treated as environmental constraints to the strategic goal of the IW. This assumption is not as restrictive as it appears to be on surface, given the generality of the architecture. We expect that the same modeling architecture and approaches may be adapted to the scope governed by a higher layer strategy such as grand strategy.

In the following, we envision the *battlefield* of an IW, the information infrastructure or the electronic cosmos (*e-cosmos*), with the analogy of an ecosystem. In this *e-cosmos*, the seven types of infrastructures, as summarized by Rattray (2001), can be envisioned as 7 *species* in the e-cosmos, and they form a complex community with a complex 'food web' (some are information producers like plants in ecosystems; some are consumers like animals who feed on plants). Each species consists of multiple metapopulations and each metapopulation consists of many (local) populations. Obviously, the entities of metapopulations and populations can be mapped to regional and local networks, respectively. With this analogy, several common properties between the *e-cosmos* (information infrastructure) and ecosystem (of biological species) emerge. For example, death of individuals or even extinctions of local populations usually will not endanger the survival of a species. The same mechanism applies to network survivability. Similarly, the behavior of individuals, the spatial-temporal dynamics of populations correspond to the behavior of network nodes, and the dynamics (reliability, survivability and performance) of networks, respectively. The behaviors can be cooperative, non-cooperative, deceptive, predatory, or parasitoid (similar to a virus). With this analogy, the bio-inspiration from population dynamics, behavioral ecology and corresponding mathematical modeling approaches can be borrowed, e.g., evolutionary game theory originated in the study of animal conflicts. In addition, both the *e-cosmos* and ecosystem are hierarchical and the notion of environment applies to both systems.

The above *e-cosmos* information infrastructure model inspired by the ecosystem is more suitable for capturing the *defensive* aspects of IW, where *stability* (ecosystem) or *survivability* (IW) is the ultimate goal. We think that the *offensive* networks are most likely more centralized and tightly controlled micro-force networks. However, physically some of them may be embedded into the information infrastructure, e.g., residing on border gateways between autonomous networks.

Others may be centralized and highly specialized networks trained for launching strategic digital attacks in wartime. While the information infrastructure (*e-cosmos*) should be inoculated to resist digital attacks (such as anti-virus, intrusion detection, firewalls), even launch counterattacks when called in, large-scale coordinated digital attacks should be conducted by a specialized digital army. To some extent, the offensive networks are very different information infrastructures. These offensive networks are in the heart of OODA loop and the intelligence of human commanders play dominant roles. These two types of networks are very different, and the modeling of offensive networks may be only appropriate when higher level strategies are considered. For example, the consequences of launching a digital attack must be assessed under the umbrella of warfare strategy or even national security strategy. For modeling of offensive networks, game theoretic approach such as those demonstrated by Jormakka & Mölsä (2005) may be sufficient because this kind of analysis may be more similar to the conventional warfare study. Nevertheless, even with modeling offensive networks only, there are unique factors that are specific to information infrastructures and must be put into the equation. For example, the "Rebel game—extreme domination resulting in rebellions" studied by Jormakka & Mölsä (2005), may be suitable for studying the consequence of launching an extremely dominant digital attack against enemies. In the case of the US, there is a huge dominance in digital technology from protocol development, information routing, GPS, and even basic hardware and software manufacturing. One consequence of the use of the dominance may push an adversary to develop its own hardware and software systems, which would hurt the US tech giants after the war.

From the discussion in previous sections, we summarize the following major challenges in modeling strategic IW and outline the approaches we have developed to deal with these challenges.

(*1*) The strategy of strategic IW is a layer under or parallel to warfare strategy in a nation's national strategy. From defense perspective, the mission of strategic IW is to protect the *center of gravity* of the national information infrastructure (NII) and the critical national infrastructures supported by the NII. The protection of NII is largely equivalent to the survivability of NII, which can be modeled with the three-layer survivability analysis architecture. The modeling approaches for traditional warfare research are not adequate for survivability analysis. From the offense perspective, the strategic IW should be considered in the context of higher layer strategies, such as warfare strategy or national security strategy. The modeling approaches developed in traditional warfare strategy research may still hold. But without considering the defense side, it is unlikely to achieve the strategic goal of IW. (*2*) The *uncertainty* exists in any warfare and it is particularly striking in IW due to the extremely "compressed" space-time dimensions, and the universally connected Internet further aggravates the uncertainty problem. The approaches we adopt are to capture the uncertainty with UUUR events and assess their consequences with survival analysis, competing risks analysis, and multivariate survival analysis. The whole three-layer survivability analysis incorporates the approaches to deal with UUUR events at each layer. (*3*) The *vulnerability* of information infrastructure is dynamic in space and time. Borrowing the terminology of reliability theory, the *hazard function* exposed to the vulnerabilities is time and space dependent, or covariates dependent. This dynamic vulnerability also carries into fault tolerance and Agreement algorithms, which are necessary to deal with *deception* problem. The solution we proposed for the dynamic vulnerability is *Dynamic Hybrid Fault* (DHF) models.   (*4*) As Sun Tzu stated, all warfare is based on deception [24]. Deception is particularly powerful in IW. However, unsuccessful deception could backfire and get punished. Deception could also make *rationality* assumption unreliable. Without rationality assumption, traditional game theory is not adequate. With *time-dependent deception*, evolutionary game theory alone is not sufficient either. We introduce "*Byzantine General Playing Evolutionary Game*," which turns Agreement-algorithm-based hybrid fault models into an *enhanced evolutionary game system* to deal with the *time-dependent deception*. Furthermore, the *handicap principle* (from the theory of animal communication networks) can be introduced to 'enforce' honesty. (*5*) *Evolutionary stable strategies* (ESS) are survivable, but to implement the *survivable strategies*, additional metrics (*Expected Survivability* and *Threshold Survivability*) are needed to conduct decision-making at the operational level. (*6*) The architecture can be *naturally* implemented with evolutionary computing algorithms, similar to agent-based computing. Figure 1 is a diagram showing the major issues in modeling strategic IW, as well as our proposed modeling architecture and the approaches to implement the architecture.

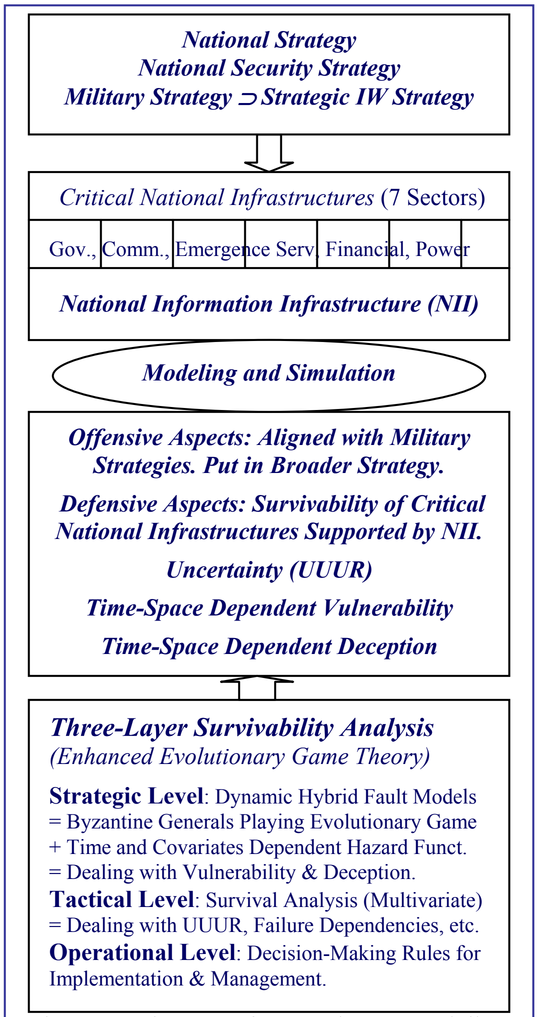
National Strategy
National Security Strategy
Military Strategy ⊃ Strategic IW Strategy
Critical National Infrastructures (7 Sectors)
Gov., Comm., Emergence Serv, Financial, Power
National Information Infrastructure (NII)
Modeling and Simulation
Offensive Aspects: Aligned with Military Strategies. Put in Broader Strategy.
Defensive Aspects: Survivability of Critical National Infrastructures Supported by NII.
Uncertainty (UUUR)
Time-Space Dependent Vulnerability
Time-Space Dependent Deception
Three-Layer Survivability Analysis
(Enhanced Evolutionary Game Theory)
Strategic Level: Dynamic Hybrid Fault Models
= Byzantine Generals Playing Evolutionary Game
+ Time and Covariates Dependent Hazard Funct.
= Dealing with Vulnerability & Deception.
Tactical Level: Survival Analysis (Multivariate)
= Dealing with UUUR, Failure Dependencies, etc.
Operational Level: Decision-Making Rules for Implementation & Management.

Figure 1. Diagram of Strategic IW Modeling

We assume that the basic unit of the e-cosmos, where the IW is conducted, is a *node*. The nodes form networks which can be hierarchical or form webs of networks. In ecological terms, they are *metapopulations*, *populations,* and *individuals*. Each node (individual) is a game player. In the following three sections, we briefly introduce each of the three levels in the three-layer survivability analysis, which offers the core modules in the above Diagram (Figure 1). In this article, we focus on the defensive IW.

3. TACTICAL LEVEL APPROACHES

At the tactical level, there are three critical aspects for modeling the survivability of an *e-cosmos*: lifetime, reliability and the assessment of UUUR events on network lifetime and reliability. Without considering UUUR, the tactical level default to regular lifetime and reliability modeling. The major mathematical approaches we propose to use are: survival analysis, competing risks analysis, and multivariate survival analysis. Comprehensive references for the three mathematical fields can be found in: Kalbfleisch and Prentice (2002), Lawless (2003) for survival analysis; Crowder (2001), Pintilie (2006) for competing risks analysis; Hougaard (2000), for multivariate survival analysis. In this paper, we use the term survival analysis to encompass the three fields. The applications of survival analysis to reliability and survivability are discussed in Ma & Krings (2008a, b& c).

3.1 Network Lifetime and Reliability

Given the failure time T of a network node, three functions (which are convertible from each other) can be used to describe the random variable T: the *survivor function*, the *probability density function* (pdf), and the *hazard function*.

The *survivor function* $S(t)$ is defined as the probability that T is at least as great as a value t; that is,

$$S(t) = P(T \geq t), \quad 0 < t < \infty \tag{1}$$

The *hazard function* specifies the instantaneous rate of failure at $T=t$, conditional upon survival to time t. It is defined as:

$$\lambda(t) = \lim_{\Delta t \to 0^+} \frac{P(t \leq T < t + \Delta t \mid T \geq t)}{\Delta t} = \frac{f(t)}{S(t)} \tag{2}$$

The *mean residual life* (MRL) is the expected remaining lifetime for a sensor node of "age" t and is defined as:

$$MRL(t) = E(T - t \mid T > t). \tag{3}$$

It can be proved that the following equation holds (Klein and Moeschberger 2003).

$$MRL(t) = \frac{\int_t^\infty (T-t) f(x) dx}{S(t)} = \frac{\int_t^\infty S(x) dx}{S(t)} \tag{4}$$

where $S(t)$ is the survivor function (1).

The *p-th quantile* of the survivor distribution of T is the smallest t_p such that,

$$S(t_p) \leq 1 - p, \quad \text{i.e.,} \quad t_p = \inf\{t : S(t) \leq 1 - p\}. \tag{5}$$

At the node level, survivor function, MRL, hazard function, as introduced here have straightforward meanings, similar to those in the reliability field. What is particularly attractive for network level research is the *p-th* quantile. We suggest defining *p-th quantile* as the *network lifetime*. With different applications, different levels of p-th quantiles can be adopted to make the metric for lifetime more appropriate for the specific applications. In general, a pair of (t_p, t_q) *quantiles* or a triplet (t_p, t_q, t_r) can be used to define the lifetime at network level.

A special challenge in studying network reliability is that reliability not only depends on lifetime, but also depends on other factors especially network connectivity, coverage, ambient environment, etc. These factors can be treated as covariates in standard survival analysis. Survival analysis offers both parametric and semi-parametric dynamic covariates regression models such as Cox *proportional hazard model* (PHM), accelerated failure Time model (AFT), and proportional mean residual life models. For example, Oakes and Dasu (1990) proposed the mean residual lifetime model as follows:

$$m(t \mid Z) = m_0(t) \exp[\beta^T Z] \tag{6}$$

where $m(t|Z)$ is the mean residual lifetime, conditional on the covariate vector Z, and $m_0(t)$ is baseline mean residual lifetime. Z can be any factors that may affect reliability. Similarly, the Cox PHM model depicts the covariates- and time- dependent hazard or survival functions; we list the survivor function here and the hazard function has a similar form:

$$S(t; z) = [S_0(t)]^{\exp(z\beta)} \tag{7}$$

3.2. Analyzing the Effects of UUUR Events.

The above definitions and models provide a sufficiently powerful model for modeling network lifetime and reliability at both node and network level. However, the most significant and unique feature survival analysis offers for survivability analysis is its unique feature in handling *censoring*. The following is an extremely brief introduction.

Censoring refers to the situations in which exact lifetimes are known for only a portion of the population sample. To some extent, survival analysis can be considered as the statistics for time-to-event random variables with censoring. Time-to-event is obtained by observing the occurrence of events from a well-defined time origin to a specific time. Failure time or lifetime is perhaps the most common time-to-event random variable. A particular difficulty in studying time-to-event data is the often unavoidable information or observation censoring, because observations through the full courses of failures are often impractical.

Formally, an observation is *right censored* at C if the lifetime (T) is only known to be greater than or equal to C. Similarly, an observation is left censored if the lifetime is only known to be less than or equal to C (Lawless 2003). More precise definitions can be achieved by further distinguishing censoring as *Type-I, Type-II* and *random censoring*, each of which can be referred to as either left or right censoring. *Random censoring,* whose censoring points are random, occurs naturally, for example, a network may be compromised by a malicious intrusion, which is often unpredictable.

There is a dilemma in processing censored observations in traditional reliability analysis since there are no mathematical procedures or models to properly handle the partial information embodied in the censored individuals. Survival analysis has developed a set of rigorous mathematical approaches and models to accommodate the *partial* information from the censored individuals, based on the counting stochastic process and Martingale central limit theorem.

Ma (2008) proposed to use the *random censoring* mechanism to describe the unpredictable events such as malicious intrusions in the modeling of network survivability. A comparative analysis of random censoring and malicious intrusions to computer networks (or any survivable systems) should support the argument. The most significant similarity is that both random censoring and malicious intrusions are unpredictable. In other words, we generally do not even know the probability that the event may happen. Specifically, the strike time of malicious act can be considered largely random but the event is only describable post-mortem. Therefore, the effects of malicious actions on survivor function (which represents lifetime or reliability as discussed previously) can be assessed by treating malicious events as censored events. Furthermore, by introducing different levels of censoring (e.g., percentage of censored individuals), one can simulate the effects of the strike *intensity* on the survivor function. If one defines survivability as a *threshold* of reliability breakdown (e.g., the survivor function crosses some *threshold* value), then this kind of simulation can produce very important insights. Besides survival analysis, competing risks analysis and multivariate survival analysis can also be used to assess the effects of UUUR events. We just discussed the way survival analysis is used to analyze the effects of unpredictable events.

Competing risks analysis can be used to analyze the so-called *latent risks* because competing risks analysis is advanced to study the phenomenon where multiple risks exists but only one of the risks cause the failure (the other are latent risks) (Ma & Krings 2008b). *Shared frailty* modeling can be used to model the *unobserved* or *unobservable* risks (Ma & Krings 2008c). The shared frailty, which is unobservable or unobserved, creates common risks that affect the failures of individuals in a population that is collectively exposed to the risks. Therefore, with the introduction of survival analysis, we possess a set of effective approaches and models that are able to assess the *consequence* of UUUR events. The most significant advantage of these approaches and models is that they do *not* require the knowledge of the occurrence probabilities of the UUUR events, which is often impossible to obtain in practice.

4. STRATEGIC LEVEL

4.1. Dynamic Hybrid Fault Models

Despite the close tie between reliability and the fault tolerance field, we realized that there is an unrealistic assumption with regard to the quantitative relationship between reliability analysis and hybrid fault models in the Agreement algorithm. One of the earliest Agreement algorithm problems was formulated as the Byzantine general problem by Lamport (1982), in which the components of a computer system are abstracted as generals of an army. Loyal generals (good nodes) need to find a way (algorithm) to reach a consensus (e.g., to attack or retreat) while traitors (or bad nodes) would try to confound others by sending conflicting messages. Because the focus of Agreement algorithms is to reach a consensus, in the hybrid fault models, the failure rate is often ignored or is implicitly assumed to be constant. In other words, the hybrid fault models only specify whether or not an agreement can be reached, given a certain number of traitors, but they do not keep track of *when* the generals committed treason. This assumption is appropriate in the study of Agreement algorithms because they are abstracted to study the possibility to reach a consensus, even if the voting is dynamic (multiple rounds of voting). However, when the fault models are applied to analyze a real-world system consisting of multiple components (generals), the *history* of the generals must be considered. Some generals may be loyal for their entire lifetimes; some may quickly become "corrupted;" still others may be loyal for a long time but ultimately become "corrupted." Each of the generals may have different (inhomogeneous) time-variant (not constant) hazard functions, $\lambda_i(t)$, $i = 1, 2, ..., g$, where g is the number of generals.

To overcome this limitation of lacking *real time* notion in tradition hybrid fault models, Ma and Krings (Ma & Krings 2008e, Ma 2008) extended the traditional hybrid fault models with the so-called *dynamic hybrid fault models*. Actually, there are two aspects for the applications of dynamic hybrid fault models in the strategic level analysis. The first is the lack of the notion of *real time* in traditional hybrid fault models, which we discuss in this subsection; the second aspect is the lack of *approaches* to incorporate hybrid fault models into reliability analysis *after* the issues associated with the first aspect are resolved, which we discuss in the next subsection.

The solution to the first aspect, the missing notion of real time, or the *Agreement-algorithm* side of the problem, is to introduce survival analysis (Ma & Krings 2008e). In particularly, time and covariate dependent survivor functions or hazard functions, introduced in Section 3 are suggested to address this issue. This extension with survival analysis is actually very straightforward. In the following, we use the *oral message* version of the Byzantine general problem (Lamport 1982) as an example to demonstrate the extension. The constraint of the Byzantine general problem under oral message assumption is, $N \geq 3m+1$, will be replaced with the following model in the dynamic version:

$$N(t) \geq 3m(t) + 1 \qquad (8)$$

Further assuming that the survivor function of *generals* is $S(t|z)$, a simplified conceptual model can be:

$$N(t) = N(t-1) * S(t \mid Z) \qquad (9)$$

$$m(t) = m(t-1) * S_m(t \mid Z) \qquad (10)$$

where $N(t)$ and $m(t)$ are the number of total *generals* and treacherous generals (*traitors*) at time t, respectively. $S(t|Z)$ and $S_m(t|Z)$ are the corresponding conditional survivor functions for the total number of generals and traitors, respectively. As in the previous section, Z is the vector of covariates, and the conditional survivor functions can adopt parametric or semi-parametric covariate models such as Cox models [Equation (7)]. One immediate benefit of the dynamic hybrid fault models is that it is now possible to predict the real-time *fault tolerance level* in a system.

4.2. Synthesizing Dynamic Hybrid Fault Models into Reliability and Survivability Analyses

The introduction of time and covariate dependent hazard (survival) functions transforms traditional hybrid fault models to time and covariate dependent ones, which we call *dynamic hybrid fault models*. This extension is necessary, but not sufficient for applying the dynamic hybrid fault models to reliability analysis, except for extremely simple cases. The difficulty arises when there are multiple types of behaviors. This is typical in real world dynamic hybrid fault models. For example, the failure modes (behaviors) could be *symmetric* vs. *asymmetric*, *transmissive* vs. *omissive*, *benign* vs. *malicious*, etc. Besides different failure modes, node behaviors can also include: cooperative vs. non-cooperative, mobile nodes vs. access points (which might be sessile), etc. To model the different behaviors, we will need multiple groups, or system of equations (9) and (10). The challenge is that we lack an approach to synthesize the models to study reliability and survivability. The solution to this challenge, or the reliability aspect of dynamic hybrid fault models, is the introduction of evolutionary game theory modeling. The approach was first outlined in Ma (2007, *unpublished dissertation research proposal, 2008*) as so-called "Byzantine Generals playing evolutionary games" by using the Byzantine Generals problem as an example.

In evolutionary game theory, replicator dynamics is described with differential equations. For example, if a population consists of n types $E_1, E_2, ..., E_n$ with frequencies $x_1, x_2, ..., x_n$. . The fitness $f_i(x)$ of E_i will be a function of the population structure, or the vector, $x = (x_1, x_2, ..., x_n)$. Following the basic tenet of Darwinism, one may define the success as the difference between the fitness $f_i(x)$ of E_i and the average fitness

$$f(x) = \sum x_i f_i(x) \qquad (11)$$

of the population. The simplest replicator model can be defined as:

$$dx_i / dt = x_i[f_i(x) - f(x)] \qquad (12)$$

for $i = 1,2,...,n$. The population $x(t) \in S_n$, where S_n is a simplex, which is the space for population composition, is similar to mixed strategies in traditional games (Vincent and Brown 2005).

Equations (11) and (12) are very general differential equation systems. They can be used to synthesizing the various groups of dynamic hybrid fault models represented with models such as equations (9)-(10). Notice that equations (9)-(10) are based on survivor functions introduced in the tactical level. Therefore, up to this point, tactical and strategic levels have already been integrated with the introduction of evolutionary game theory. The integration, besides providing a framework for analyzing lifetimes and reliability, producing the following new features: (*i*) the effects of UUUR events are considered; (*ii*) *real-time* notion is introduced to hybrid fault models—dynamic hybrid fault models; (*iii*) the various nodes behaviors (including failure modes) are modeled with different dynamic hybrid fault models, and these models are synthesized with evolutionary game modeling.

Previous sections outline approaches to predict the real-time lifetime, reliability and fault tolerance. An interesting and legitimate question is: can we predict the real-time survivability, similar to the prediction of lifetime or reliability? The answer we have, with regarding to our approaches, is no. We doubt this is ever possible as long as UUUR events are involved, because it is usually impossible to know the precise probability that UUUR events occur. However, the approaches we developed do offer an important contribution, i.e., the effects of UUUR events are incorporated in the modeling process. The whole three-layer survivability analysis architecture takes advantages from this contribution.

Given that the precise real-time prediction of survivability is not possible, the question we try to answer in the remainder of this article is: what can be done with regard to survivability with the three-layer approach? Two things can be done: one is the derivation of survivable strategies, and the other is the implementation of the survivable strategies. In the next subsection, we discuss the survivable strategies, and in Section 5 we introduce *operational level* modeling that implements the survivable strategies.

4.3. Evolutionary Stable Strategy (ESS) and Survivability

With network nodes as game players, reliability functions such as expressed in survivor function [equation (1)-(7)] as payoff (fitness) of the game, nodes behaviors such as represented with dynamic hybrid fault models, and replicator dynamics models as the game dynamics model, plus the optimization goal such as maximize network lifetime or reliability, we have all major components of an evolutionary game theory (EGT) model. One of the most important information from an EGT model is the evolutionary stable strategy (ESS), which is equivalent to the Nash equilibrium in traditional game model. ESS is *unbeatable* or *impregnable* in the sense that *mutants* or *dissidents* in a population cannot "invade" the population under natural selection, in terms of the reduction of fitness (Vincent and Brown 2005). With the above formulation, EGT modeling and the associated ESS provide sufficiently flexible and powerful approaches for analyzing network survivability at strategy level. In this formulation, *survivability* is a set of prescribed strategies (sustainable strategies), which is determined by various internal and external factors including hardly predictable ones such as UUUR or hardly quantifiable ones such as economic and anthropocentric values. UUUR is incorporated into the game model via *payoff* or *fitness* function (represented with reliability or survivor function). Therefore, strategy level modeling is set on the foundation of tactical level modeling.

5. OPERATIONAL LEVEL

5.1. Highlights of the Tactical and Strategic Levels

Let's first summarize what are obtainable at both tactical and strategic levels. The results at both tactical and strategic levels are *precisely* obtainable either via analytic or simulation optimization. With the term *precisely*, we mean that there is no need to assign subjective probabilities to UUUR events. This is possible because we try to assess the consequences of UUUR events (tactical level) or obtain the ESS strategies (strategic level), rather than to obtain real-time prediction of survivability. The following is a list of specific points:

(***1***) At the tactical level, we focus on dealing with three types of UUUR events. We believe that these UUUR events are sufficiently general to capture the major factors/events in reliability, security and survivability, whose occurrence probabilities are hard or impossible to obtain. Instead of trying to obtain the probabilities for these events, which are infeasible in most occasions, we focus on analyzing the consequences of the events. In addition, spatial frailty modeling can be utilized to capture the heterogeneity of risks in space (Ma 2008, Ma & Krings 2008d). This may be called the fourth type risks beyond the three UUUR events introduced previously.

To take advantage of the tactical level modeling approaches, it is obviously necessary to stick to the survivor functions (or hazard functions), rather than traditional reliability models. In other words, survival analysis can deal with UUUR events. Furthermore survivor function and reliability function have the exactly same mathematical definition. This is the critical junction that survival analysis plays critical role in survivability analysis at tactical level. However, we recognize that it is infeasible to get a simple metric for *survivability* similar to reliability with tactical level modeling alone. Actually, up to this point, we are still vague about the measurement of survivability or a metric for survivability. We have not answered the question: what is our metric for survivability? We think that a precise or rigorous definition of survivability at the tactical level is not feasible, due to the same reason we cited previously—the inability to determine the probabilities of UUUR events. However, we consider it is very helpful to define a *work* definition for survivability at the tactical level.

We therefore define the survivability at the tactical level as a metric, $S_u(t)$, which can be quantified as the survivor function or reliability function with UUUR events considered. In the framework of three-layer survivability analysis, this metric is what we mean with the term *survivability*. The "metric" *per se* is not the focus of the three-layer survivability analysis. It is not very informative without the supports from the next two levels—strategic and operational models. However, it is obvious that this metric sets a foundation to incorporate UUUR effects in the modeling at the next two levels.

(***2***) The strategic level modeling essentially has two objectives: (*a*) incorporate the *risks* and *covariates* that affect survivability which survival analysis alone is not adequate to deal with; (*b*) since the *work* definition of survivability at the tactical level is necessary but not sufficient for modeling survivability, we need to define what is meant with the term *survivability* at the strategic level. With regard to (*a*), the solution we proposed for the first issue was the dynamic hybrid fault models, which integrate survivor functions with traditional hybrid fault models. The solution we proposed for the second issue was the introduction of EGT modeling. One of the most important results from EGT modeling is the so-called evolutionary stable strategies (ESS) sustainable strategies. We map the ESS in EGT to *survivable strategies* in survivability analysis. Therefore, at the strategic level, our *work definition* for survivability refers to the *survivable strategies* or *sustainable strategies* in the native term of EGT, which can be quantified with ESS. Besides integrating dynamic hybrid fault models, another advantage for introducing EGT modeling at the strategic level is the flexibility for incorporating other nodes behaviors, such as counterattack behaviors.

Without UUUR events, both tactical and strategic level models default to regular reliability models. This implies that, in lack of UUUR events, reliable strategies are sustainable or survivable. Nevertheless, when UUUR events exist, reliable strategies and survivable strategies are different. This necessitates the next operational level modeling.

5.2. Operational Level Modeling

When UUUR events are involved, we cannot make real time predictions of survivability at tactical and strategic levels. This implies that the implementations of survivable strategies need additional measures that we develop in this section. We use possibly the simplest example to explain the dilemma. Assuming that the ESS solution for a network is expressed with the following simple algebraic conditions: survivability metric at tactical level, $S_U = 0.7$, Router-Nodes > 10%, Failed Nodes < 40%. They cannot be implemented because we do not know ***when*** the actions should be taken to warrant a sustainable system. These conditions lack a *correlation* with real time. This requires the next level of modeling, which we call *operational level modeling*.

The inability to implement ESS is rooted in our inability to assign definite probabilities to UUUR events, which implies that we cannot predict *when* something sufficiently bad will jeopardize the system survivability. What we need at the operational level is a scheme to ensure the ESS strategy is in place in advance. The fundamental idea we use to implement the ESS strategy is to *hedge* against the UUUR events. A similar idea has been used in integrated pest management and financial engineering. This can be implemented with the following scheme. Let us define a pair of survivability metrics: one is the *expected survivability* (ES) and the other is the *action threshold survivability* or simply *threshold survivability* (TS). ES is equivalent to the survivability metric at tactical level. ES corresponds to ESS at strategic level, but they are not equivalent since ESS is the strategy and ES is survivability. TS is the survivability metric value (at the tactical level) before the system reaches ES. Both ES and TS can be obtained from strategic level models. For example, if TS = $S_U(s)$ and ES=$S_U(t)$, then $s<t$ is a necessary condition for the implementation of ESS. In other words, the implementation of strategies that ensures TS at time s will guarantee the future ES level at time t. To make the implementation more reliable and convenient, multiple dynamic TSs can be computed at time $s_1, s_2, ..., s_k$, with $s_i < t$ for all i. These TS at times $s_1, s_2, ..., s_k$ should be *monitored* by some evaluation systems.

Unlike tactical and strategic levels, operational level modeling is *approximate*. The term *'approximate'* means that we cannot predict the real time survivability, or we do not know the exact time an action should be taken. Instead, the action is triggered when the *monitored* survivability metric S_U(r) drops below the threshold survivability (TS). In other words, by adopting the duo scheme of TS and ES, we ensure the ES by taking preventative actions (prescribed by ESS and triggered by the TS) in early stages, which *buffers* the potential consequences of UUUR events.

6. SUMMARY

In previous sections, we first outlined a conceptual model of the strategic IW (Section 2.2), and then applied the three-layer survival analysis to formulate a modeling and simulation architecture for studying the IW, with focusing on the defensive *e-cosmos* (Sections 3, 4, and 5). From the defense perspective, modeling the strategic information war is very similar to survivability analysis, and therefore, the application of the three-layer survivability analysis is relatively straightforward. If the defensive IW is largely equivalent to the survivability analysis problem, then why do we still formally propose this application or "simple exercise" of the three-layer survivability analysis? There are two motivations behind this exercise. The first motivation is to emphasize that the core of the three-layer survivability analysis possesses unique and powerful functionalities in dealing with three fundamental difficulties in studying IW, i.e., rationality (an assumption of tradition game theory), uncertainty (vulnerability), and deception. In particular, these three properties are dependent upon each other, and each of them can be time and space dependent. For example, what is perceived as an irrational strategy can be a deceptive scheme or a desperate move. This kind of strategy can be readily formulated into the *Dynamic Hybrid Fault* models, which integrate survival analysis and evolutionary game modeling and further introduce voting mechanisms from the Agreement algorithms. Furthermore, the *library* of Agreement algorithms can be extended with new algorithms—strategies proposed by IW commanders or strategists. These new algorithms or strategies can be offensive or counterattack strategies. Therefore, the architecture proposed in this paper should also be applicable for offensive IW. This is actually the second motivation for our exercise. Offense and defense should be considered with a unified goal, which may need to satisfy the requirements of a higher level strategy such as warfare strategy or national security strategy. In this article, we skipped offensive IW, but it should be a further topic for the future research on the proposed architecture. Another future research topic we suggest is that the proposed architecture should also be applicable, in principle, to traditional warfare or other national strategy research, such as defined by Deibel (2007), because rationality, uncertainty, and deception are common issues in any research on strategy. Finally, the implementation should be a software environment with modeling and simulation functionalities that implement the approaches and algorithms of the proposed architecture.

REFERENCES

[1] Cohen, F. et al. (1998). A Preliminary Classification Scheme for Information System Threats, Attacks, and Defenses: A Cause and Effect Model and Some Analysis based on That Model. Sandia National Lab.

[2] Crowder, M. J. 2001. *Classical Competing Risks*. Chapman & Hall

[3] Deibel, T. L. 2007. Foreign Affairs Strategy. Cambridge University P.

[4] Hougaard, P. 2000. Analysis of Multivariate Survival Data. Springer.

[5] Jormakka, J. and J. V. E. Mölsä. 2005. Modelling Information Warfare as a Game. Journal of Information Warfare (2005) 4 (2): 12 – 25

[6] Kalbfleisch, J. D., & R. L. Prentice, 2002. The Statistical Analysis of Failure Time Data. Wiley-InterScience, 2nd ed.

[7] Kumar, S., and V. Marbukh. 2003. A game theoretic approach to analysis and design of survivable and secure systems and protocols. Lecture Notes in Computer Science. vol. 2776: pp440-443. Springer.

[8] Lamport, L., R. Shostak and M. Pease. 1982. The Byzantine Generals Problem. *ACM Trans. on Prog. Lang. and Syst.,* 4(3):382-401,

[9] Lawless, J. F. 2003. Statistical models and methods for lifetime data. John Wiley & Sons. 2nd ed.

[10] Ma, Z. S. 2008. *New Approaches to Reliability and Survivability with Survival Analysis, Dynamic Hybrid Fault Models, and Evolutionary Game Theory.* PhD. dissertation, University of Idaho.

[11] Ma, Z. S. & A. W. Krings. 2008a. Survival Analysis Approach to Reliability Analysis and Prognostics and Health Management (PHM), *Proc. IEEE–AIAA AeroSpace Conf.*, March 1-8, 2008, MT. 20pp.

[12] Ma, Z. S. & A. W. Krings. 2008b. Competing Risks Analysis of Reliability, Survivability, and Prognostics and Health Management (PHM), *Proc. IEEE–AIAA AeroSpace Conf.*, March 1-8, 2008. Big Sky, MT. 20pp.

[13] Ma, Z. S. & A. W. Krings. 2008c. Multivariate Survival Analysis (I): Shared Frailty Approaches to Reliability and Dependence Modeling. *Proc. IEEE–AIAA AeroSpace Conf.*, March 1-8, 2008, Big Sky, MT. 21pp.

[14] Ma, Z. S. & A. W. Krings. *2008d*. Spatial Distribution Patterns, Power Law, and the Agent-based Directed Diffusion Sensor Networks. *Sixth IEEE PerCom*, March 17-21, 2008, Hong Kong, China. 6pp.

[15] Ma, Z. S. & A. W. Krings. 2008*e*. Dynamic Hybrid Fault Models and their Applications to Wireless Sensor Networks (WSNs). *The 11-th ACM International Symposium on Modeling, Analysis and Simulation of Wireless and Mobile Systems*. (ACM MSWiM 2008). 9pp.

[16] Ma, Z. S. & A. W. Krings. 2009. A New Three-Layer Survivability Analysis Architecture. *Submitted*.

[17] Oakes, D. & Dasu, T. 1990. A note on residual life. *Biometrika* 77, 409–10.

[18] Paul, C. 2008. *Information Operations Doctrine and Practice*. Praeger Security International. 175pp.

[19] Pintilie, M. 2006. *Competing Risks: A Practical Perspective*. Wiley.

[20] Rattray, G. 2001. Strategic Warfare in Cyberspace. MIT Press

[21] Schneier, B. (2000). Secrets & Lies, Wiley, New York.

[22] Vincent, T. L. and J. L. Brown. 2005. *Evolutionary Game Theory*. Cambridge University Press.

[23] http://www.au.af.mil/au/aul/bibs/informops.htm#boo

[24] Sun Tzu. *The Art of War*. http://classics.mit.edu/Tzu/artwar.html
http://www.ndu.edu/inss/siws/cont.html