

Chapter 2

Alternatives to Cyber Warfare: Deterrence and Assurance

Robert J. Elder, Alexander H. Levis and Bahram Yousefi

Abstract Deterrence as practiced during the Cold War was largely defined in terms of capabilities to impose punishment in response to an attack; however, with growing concern over the proliferation of cyber technologies, deterrence has evolved to be understood more generally in terms of cost/benefit calculi, viewed from not only a national perspective, but also recognizing the importance of both friendly and adversary perspectives. With this approach, the primary instruments used for deterrence are those which encourage restraint on the part of all affected parties. The use of a multiple lever approach to deterrence offers a path to an integrated strategy that not only addresses the cost/benefit calculus of the primary attacker, but also provides opportunities to influence the calculus of mercenary cyber armies for hire, patriotic hackers, or other groups. For this multiple lever approach to be effective a capability to assess the effects of cyber attacks on operations is needed. Such a capability based on multi-formalism modeling to model, analyze, and evaluate the effect of cyber exploits on the coordination in decision making organizations is presented. The focus is on the effect that cyber exploits, such as availability and integrity attacks, have on information sharing and task synchronization. Colored Petri Nets are used to model the decision makers in the organization and computer network models to represent their interactions. Two new measures of performance are then introduced: information consistency and synchronization. The approach and the computation of the measures of performance are illustrated through a simple example based on a variation of the Pacifica scenario.

R. J. Elder (✉) · A. H. Levis · B. Yousefi
System Architectures Laboratory, George Mason University, Fairfax, VA, USA
e-mail: relder@gmu.edu

A. H. Levis
e-mail: alevis@gmu.edu

B. Yousefi
e-mail: byousefi@masonlive.gmu.edu

© Springer International Publishing Switzerland 2015
S. Jajodia et al. (eds.), *Cyber Warfare*, Advances in Information Security 56,
DOI 10.1007/978-3-319-14039-1_2

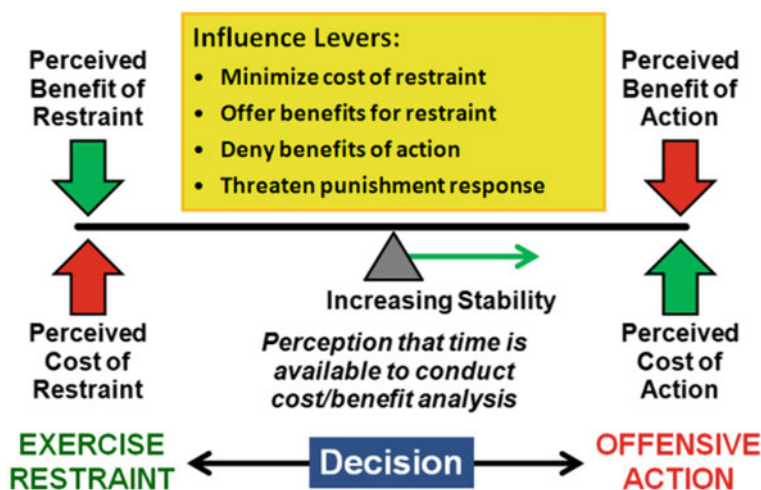


Fig. 2.1 Deter/Assure decision influences. (figure based on DO-JOC (2006))

2.1 Introduction

The evolving primary deterrence objective is to encourage restraint on the part of all affected parties, and the primary means is to establish mutual understanding among actors designed to prevent one actor from conducting actions or exhibiting behaviors that are so unacceptable to another that the responses become escalatory. In this context, the instruments of deterrence are not only the capabilities to impose punishment (threaten punishment response) or deny the effects of adversary actions (deny benefits of action), but also the means to identify friendly and competitor vital interests, to communicate with friends and adversaries, to validate mutual understanding of red lines, and to control escalation (minimize cost of restraint and offer benefits of restraint.). These Deter/Assure influences along with the influence levers are shown in Fig. 2.1.

Deterrence often fails because mutual understanding between actors is lost, or one actor's cost/benefit calculus drives an unacceptable behavior despite the threat of punishment. Therefore, a holistic approach to deterrence requires the US to identify both US and competitor vital interests, to establish a robust, open dialogue with competitors and friends, and to develop and maintain a range of actions to preserve the stability of the relationship. This naturally leads to the development of strategies designed to (1) assure friends and allies, (2) dissuade adversaries from developing capabilities that threaten national well being, (3) deter potential adversaries by encouraging restraint, denying benefits, and threatening to impose unacceptable cost, and (4) maintain capabilities to terminate conflict at the lowest level of destruction consistent with strategic objectives. Regardless of the decision maker, deterrence involves four primary considerations: (1) The perceived cost of restraint (calculus: costs of not taking an action); (2) The perceived benefits of restraint (calculus: benefits

of not taking an action); (3) The perceived benefits of taking action (calculus: will action achieve the desired effect?); and (4) The perceived costs of taking action (calculus: how will the competitor respond?). Understanding how these factors are interrelated is critically important to determining how best to influence adversary decision-making.

The Deterrence Operation Joint Operating Concept (DO-JOC 2006) outlines a basic approach to deterrence and was a first attempt to apply Cold War lessons to post-Cold War challenges. The US Strategic Command has evolved this concept dramatically over the last three years and is in the process of updating the 2006 document. The DO-JOC postulates a series of critical assumptions for effective deterrence of adversarial actions and behaviors that can be applied to cyber deterrence: First, the United States is aware that an adversary (state or non-state) possesses a cyber attack capability that threatens its vital interests. Second, the adversary actions to be deterred result from deliberate and intentional calculations regarding alternative courses of action and their perceptions of the values and probabilities of alternative outcomes associated with those different courses of action. Finally, cyber deterrence must assume that at least some adversary values and perceptions relevant to their decision-making can be identified, assessed, and influenced by others. The DO-JOC goes on to note that some actors (both state and non-state) will be extremely difficult to deter; however, truly irrational actors are extremely rare. Their calculus may be very different from that of the United States but what constitutes rational behavior must be understood in their terms. The following examination of cyber deterrence accepts these fundamental assumptions and focuses on deterring rational actors from attacking US vital interests in or through cyberspace.

When most people think of deterrence, the first thought that comes to mind is the ability to impose significant punishment in retaliation for an attack. However, the Deterrence Operations JOC suggests that adversaries can also be deterred if they feel their actions will not achieve the desired benefits (denial; for example, through resilience) or that restraint from the action will achieve a better outcome than taking the action the US seeks to deter.

It is instructive to assess how the DO-JOC applies to cyber deterrence. General Larry Welch (2008) has stated that cyber deterrence is difficult unless an actor first understands its own critical vulnerabilities and takes action to protect them. Another important concept can be found in a report by the Air Force Scientific Advisory Board (AFSAB 2008) which argued that it is important to protect the United States from the *effects* of attacks rather than just protect the *targets* of the attacks, or attempt to blunt the attacks themselves. One might think of this protection against effects as “mission assurance” or “cyber resiliency” as contrasted with traditional “information assurance” which focuses on the protection of networks and systems, or cybersecurity which focuses on actions taken to deny the success of known attack vectors. From a deterrence perspective, the idea is to introduce uncertainty in the adversary’s mind that the attacks will achieve the desired effects; if they don’t, and there is a possibility that the source of the attack might be determined through forensic analysis or intelligence means, this potential denial of benefit of the attack, or loss of benefits that would result from exercising restraint should affect the adversary’s

decision calculus. The potential for attribution can be improved by “reducing the noise level” through improved security and defense of critical information, systems, networks, and infrastructure, making it easier to detect behaviors that might pose a threat to the United States. This could include establishment of protocols and standards that govern both the public and private sectors in areas that could affect United States vital interests. Daniel Geer (2010) addressed the need for policy choices that support risk management versus risk avoidance, clearly recognizing that our current risk avoidance approach to cyberspace is attractive, but impractical. He postulated that Americans want freedom, security, and convenience, but they can only have two of the three. The Nation must make choices to implement a cyber deterrence strategy; anything that sacrifices vitally important aspects of national and economic security in cyberspace for purposes of convenience simplifies the attack problem for a cyber adversary.

2.2 Applying Multi-Modeling to Cyber Deterrence

An approach based on multiformalism modeling (or multi-modeling) is proposed as an aid to applying the deterrence operations concept to cyberspace. In general, the models can provide insights into the calculus of potential adversaries and provide a means to evaluate courses of action which reduce the adversary’s perceived cost of restraint (not taking an action which affects US vital interests), increase the adversary’s perceived benefits from restraint, reduce the perceived benefits of taking actions unacceptable to the US, and/or increasing the perceived costs of taking actions which will lead to a US response.

It is clear that imposing punishment based on the effects of cyberspace actions is difficult because of our limited ability for attribution and the length of time it takes to conduct the forensic analysis. However, from a deterrence perspective, what the adversary perceives as the capability of the United States to attribute these actions is more important than the capability itself. Therefore, US strategy in this regard should raise doubts in the adversaries’ calculus that such perpetrators can conduct their actions anonymously. From a denying benefits perspective, one approach is to increase the Nation’s defensive or protection capabilities already embodied in US cyber security and information assurance programs. However, another way to deny benefits is to ensure that the United States can continue operations effectively in the areas that came under attack. This approach calls for resiliency across all sectors (Pflanz and Levis 2014); the military typically refers to this capability as *mission assurance*.

Turning to the concept of escalation control it is useful to recognize that cyber escalation control will likely involve activities that are not conducted directly in cyberspace. For example, cost of restraint to potential adversaries is affected by their perception of risk to their vital interests from the United States in any domain. Conversely, the United States might be able to influence an adversary’s perceived benefit from restraint by taking full advantage of its superpower status to provide incentives

which potential adversaries clearly recognize would be lost should they engage in major conflict with the United States. With proper messaging, the United States can place particular emphasis on the loss of benefits an adversary might expect should it attack US vital interests through cyberspace. This messaging issue is highlighted in a recent mass media article with the title “The Decline of Deterrence: America is no longer as alarming to its foes or reassuring to its friends” (The Economist 2014).

As in other forms of deterrence, the means for cyber deterrence are capability posturing, visible activities, and messaging. There are many possible ways to posture US cyber capabilities for potential adversaries to see. For example, simulations can demonstrate the ability to continue governmental operations while under cyber attack. There are also a variety of visible activities that can be used to support the basic deterrence elements. For example, by conducting cyber warfare exercises the US demonstrates its readiness to act in cyberspace; and by demonstrating its forensics capabilities, even if not performed in real time, the United States can demonstrate its ability to attribute the sources of attack. The Department of Homeland Security, with its exercises conducted to prepare for both natural disasters and attacks, demonstrates US commitment to resiliency and incentivizes the entire Nation to establish measures which contribute to mission assurance across all sectors. And, finally, public messaging and private diplomacy allow the United States to explain to its friends and potential foes what the Nation considers to be unacceptable actions or behaviors in cyberspace, and the reasons for its own posturing and activities. All of these means can be modeled individually; the challenge is to understand and model their interactions.

Multi-modeling offers a structured approach to develop, analyze, and assess the multiple elements of a deterrence and assurance strategy as it applies to cyberspace. A key component of such an approach is to be able to assess the effects of cyber exploits on operations and compute measures that will enable the comparison of alternative strategies that are focused on mitigating the effects (i.e., denying benefits to the adversary). The use of multiple federated models brings together the expertise of subject matter experts across multiple domains; it can enable analysts to identify their own knowledge gaps; and allow improved information and knowledge sharing across different areas of expertise.

In the following sections a more detailed examination of the modeling approach and the definitions of several relevant measures of performance are described. The approach is illustrated using a vignette in which the effect of cyber exploits on a decision making organization (e.g., an Operations Center) is evaluated. The approach is showing great promise as a means to understand the complex interactions among the many actors that are affected by cyber exploits and thus support analysts and planners as they develop cyber deterrence strategies.

2.3 Multi-Formalism Modeling

Assessing the effect of cyber exploits on an organization's performance is a challenging problem. A cyber exploit is an action that affects the performance of an information system by taking advantage of its cyber vulnerabilities. The evaluation of the effectiveness of a decision making organization consisting of human decision makers supported by systems and interacting through networks is a complex issue: many interrelated factors affect the effectiveness of the overall system, e.g., the limited information processing capacities of the decision makers and the hardware and software characteristics of the systems. Consequently, models are needed of organizations performing well defined tasks and of their information systems, as well as performance evaluation measures and procedures for computing them. An integrated methodology that exploits multi-formalism modeling and is based on some earlier work has been developed and is described in this paper.

One of the key effects of cyber exploits is the degradation of the cohesiveness of organizations carrying out well-defined tasks in a coordinated manner. A mathematical description of coordination was developed for decision-making processes by Grevet and Levis (1988). When confronted with a particular task, organization members need to access information from the supporting systems and to interact with each other following well defined processes. Such is the case in operations centers such as Air Operations Centers, Air Traffic Control Centers, etc. When decision makers interact, they must have some protocol to recognize that they are working on the same task and sharing information that pertains to that task, i.e., that they are coordinated. Two measures for evaluating coordination were introduced: information consistency and synchronization. The latter measure relates to the value of information when the decision makers actually process it.

The approach taken is that of modular, horizontal multi-formalism (Gribaudo and Iacono 2014). A generic Petri Net model of an interacting decision maker is used (Levis 1992). That model has been extended to include systems that support the decision makers and communication networks that enable their interaction. The decision making organization is modeled as a Colored Petri Net (Jensen and Kristensen 2009) and is implemented in CPNTools (CPNTools 2014). The computer networks are modeled as queuing nets and implemented in OMNeT++ (OMNeT++ 2014). These two models, though expressed in a different modeling language (formalism), interoperate through an infrastructure, the Command and Control Wind Tunnel. This is shown in Fig. 2.2 (Hemingway et al. 2011). The validity of the interoperation of these two formalisms was established in Abu Jbara and Levis (2013) based on the approach described in Levis et al. (2012).

2.4 The Decision Making Organization Model

The decision making organizations under consideration consist of groups of interacting decision makers processing information received through systems that enable information sharing (e.g., a cloud) and who interact to produce a unique organizational

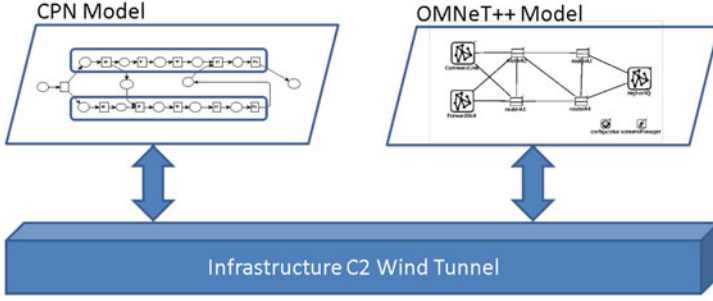


Fig. 2.2 Multi-formalism modeling and simulation architecture

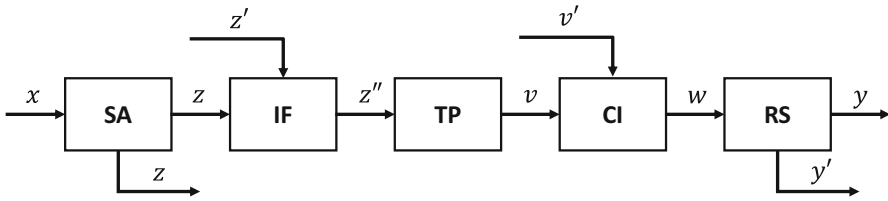


Fig. 2.3 The five stage decision maker model

response for each task that is processed. Each interacting organization member is modeled as consisting of a five-stage process as shown in Fig. 2.3.

The decision maker receives a signal x from the external environment or from another decision maker. The Situation Assessment stage (SA) represents the processing of the incoming signal x to obtain the assessed situation, z , which may be shared with other decision makers. The decision maker can also receive situation assessment signals z' from other decision makers within the organization; z' and z are then fused together in the Information Fusion (IF) stage to produce z'' . The fused information is then processed at the Task Processing (TP) stage to produce v , a signal that contains the task information necessary to select a response. Command information from other decision makers is received as v' . The Command Interpretation (CI) stage then combines v and v' to produce the variable w , which is input to the Response Selection (RS) stage. The RS stage then produces the output y to the environment, or the output y' to other decision makers.

A Petri Net model is used to depict interactions between decision makers; the admissible interactions are limited to the four types shown in Fig. 2.4 in which only the interactions from the i th (DM_i) to the j th decision maker (DM_j) are shown. Similar interactions exist from the j th to the i th one. Furthermore, not all these interactions can coexist, if deadlocks are to be avoided (Remy et al. 1988).

A decision maker may have access to or select different systems and different algorithms that process the input depending on the type of signals received. The DM chooses an algorithm according to his area of expertise and the prevailing circumstances (timeliness, access to systems, etc.). Each algorithm is characterized by the

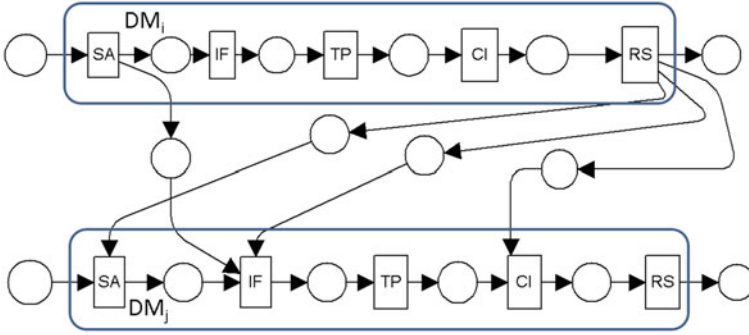


Fig. 2.4 Interacting decision making entities

accuracy of its output and the associated delay in producing it. The algorithms may all reside in one system (e.g., at the command unit) or be located in different system nodes; they may be accessible directly through an intranet or they may be accessible through the communication networks. There may be inconsistent or conflicting assessments at the IF stages of the two units for a variety of reasons: using different data sets (e.g., new vs. old data) or different assessment algorithms. A mechanism would be needed to resolve such inconsistencies or conflicts. A similar argument is made about the Response Selection stage where DMs have different algorithms for generating a response.

2.5 On Measures

In order to assess the effect of cyber exploits, measures are needed. A set of new measures is defined here that is computable from the Colored Petri net model of the decision making organization. These measures were originally defined in Grevet and Levis (1988).

To characterize the coordination for an interaction such as at the IF or CI stage in the model of Fig. 2.5 order relations are defined on the set of tokens fired by the corresponding transition:

Ψ_1 is a binary relation defined by:

$$((x, y, z)\Psi_1(x', y', z')) \leftrightarrow ((x = x') \text{ and } (z = z'))$$

Ψ_2 is a binary relation defined by:

$$((x, y, z)\Psi_2(x', y', z')) \leftrightarrow ((x = x') \text{ and } (z = z'))$$

Each token in the Colored Petri Net model is characterized by the triplet (T_n, T_d, C) where T_n is the time at which this input token was generated by the source, T_d is the time at which a token entered the current processing stage, and the attribute C characterizes the mission or task.

The firing of IF (or CI) is synchronized if and only if:

$$\forall i \in \{1, 2, \dots, r\} (T_n^i, T_d^i, C^i) \Psi_1 (T_n^k, T_d^k, C^k)$$

where i and k are two decision makers. This definition allows to discriminate between firings that are synchronized and firings in which one or several tokens arrive in their respective corresponding places with some delay.

The firing of IF (or CI) is *consistent* if and only if:

$$\forall (i, j) \in 1, 2, \dots, r \times 1, 2, \dots, r, (T_n^i, T_d^i, C^i) \Psi_2 (T_n^j, T_d^j, C^j)$$

i.e., the data fused by a decision maker are consistent if they correspond to the same task or mission C. On this basis, the following definition for the coordination of an interaction is obtained: *The firing of a transition (such as IF) is coordinated if, and only if, it is synchronized and consistent.*

The definition of coordination applies to a single interaction. The definitions of the coordination of a single task, i.e., for a sequence of interactions concerning the same input, as well as for all tasks executed in a mission are as follows: The execution of a task is coordinated if, and only if, it is coordinated for all interactions that occur during the task. The execution of a mission is coordinated if, and only if, it is coordinated for all its tasks.

Consider a transition such as IF (or CI) with multiple input places. The $V(x_i, IF)$ denotes the vector that describes the colors of the tokens in the preset that have been generated as a result of the signal x_i (task or mission) produced by the external source. Then the *Degree of Information Consistency* (DIC) for stage IF and input task x_i is defined as:

$$d(x_i, IF) = \sum_{V(x_i, IF)} \text{prob}(V(x_i, IF)) \frac{n(V(x_i, IF))}{z(V(x_i, IF))}$$

where $\text{prob}(V(x_i, IF))$ is the probability of having tokens with attributes generated by x_i in the input places of IF. Then let z be the number of subsets of two elements of $V(x_i, IF)$:

$$z(V(x_i, IF)) = \binom{r}{2} = \frac{r!}{2!(r-2)!}$$

and let n be the number of subsets of $V(x_i, IF)$ such that the two elements are equal.

By adding the degrees of information consistency for IF and CI and each task x_i and weighing by the probability of having that input task, the organizational degree of information consistency, DIC, for the tasks at hand can be evaluated:

$$DIC = \sum_{x_i} \text{prob}(x_i) \sum_{B=IF, CI} d(x_i, B)$$

This measure varies between 0 and 1, with 1 being the ideal information consistency of all interactions across all tasks.

The total processing time for a task by a decision maker consists of two parts: (a) the total time during which the decision maker actually carries out the task; and (b) the total time spent by the information prior to being processed. The latter time is due to two factors: (i) Information can remain unprocessed until the decision maker decides to process it with a relevant algorithm. Since an algorithm cannot process two inputs at the same time, some inputs will have to remain in queue for a certain amount of time until the relevant algorithm is available. (ii) Information can also remain unprocessed because the decision maker has to wait to receive data from another organization member. Consequently, an organization is not well synchronized when decision makers have to wait before receiving the information that they need in order to continue their task processing. Conversely, the organization is well synchronized when these lags are small.

The *Degree of Synchronization* for the organization, DOS, is given by:

$$DOS = \sum_{x_i} prob(x_i) \sum_{B=IF,CI} S(x_i; B)$$

where $S(x_i, B)$ is the total delay in transition B because of differences in the arrival time of the enabling tokens in its preset.

Two more measures were defined for evaluating the effect of cyber exploits on organizational performance.

Accuracy of the Organization $J(\delta)$ is the degree to which the organization produces desirable results (with lowest penalty) when using strategy δ . This is a global measure which ideally would be one but in realistic situations it is always less than one.

$$J(\delta) = \sum_i prob(x_i) \sum_h cost(y_h, y_{di}) prob(y_h | x_i)$$

where $\{x_i\}$ is the set of tasks and $\{y_h\}$ is the set of admissible responses from which the response y_h is selected for task x_i and y_{di} is the ideal response for input x_i . $Cost(y_h, y_{di})$ represents the cost associated with the organization's response.

Timeliness of the Organization $T(\delta)$ is the total response time of the organization from the time a task arrives to the time a response is produced, i.e., the task has been executed using strategy δ .

$$T(\delta) = E(elapsed\ time)$$

Up to this point, the model of an organization executing a set of tasks that arrive according to some probability distribution has been described. Also, measures of performance of the organization have been defined.

When fusion of data is performed by a decision maker it is possible that the available markings may allow multiple enablement of the IF (or CI) transition. Consequently, enablement rules need to be introduced at this point. Two alternative rules have been considered:

Rule 1 Transition IF (or CI) is enabled, if all its input places contain a token with the same value of the time attribute T_n . Rule 1 means that the transition IF (or CI)

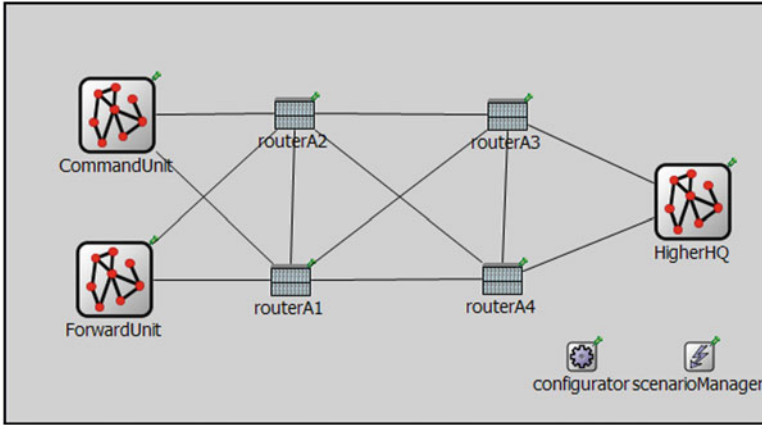


Fig. 2.5 OMNET++ Representation of the Communication Network

is enabled if and only if all its preset places contain at least a representation of the same input x_i .

Rule 2 The transition IF (or CI) is enabled if Rule 1 applies or if delays in receiving inputs from other organization members exceed a pre-specified limit.

2.6 The Network Model

A network model was implemented using OMNeT++ (2014) which is an extensible, modular, component-based C++ simulation library and framework, primarily for building network simulators. This is a discrete event simulation environment consisting of simple/compound modules with each module having a defined functionality (according to the relevant C++ class). Each module could be triggered with an appropriate event defined in its class. For the model of Fig. 2.5 the INET 2014 (2014) framework was used which supports different networking protocols including the four layers of the TCP/IP protocol. The framework provides simple/compound modules for all the four layers of the TCP/IP. The nodes in Fig. 2.5 contain in them the internal network structure for the corresponding entity (command unit, forward unit, and Higher HQ).

2.7 Modeling Cyber Exploits

Two types of cyber exploits were implemented for the computational experiments with the example described in Sect. 2.8: (1) Denial of Service attacks and (2) Integrity attacks. The Denial of Service is an attempt to make a network resource unavailable or render it too slow to be useful. This attack affects a localized region of the network

topology, e.g., some routers. The Integrity attack, as was defined in this case, involves tampering with the contents of the data packets in order to compromise the performance of the organization through deception. It is usually the case that the attacker intercepts the data being passed between two terminals for a considerable amount of time; this sometimes leads to the detection of an anomaly.

The two types of attack were implemented in OMNeT++ for a predefined scenario that can generate coordinated attacks of both types. The Denial of Service exploits were modeled as a delay in a communication path or as a total failure of a network resource (e.g., a router) for a finite amount of time as defined in the scenario. The integrity attacks were implemented as an alteration in the message contents, i.e., by changing the attribute values of the tokens, at specified times as defined in the scenario. The results of the attack were evaluated using the measures of performance defined in the measures section.

2.8 A Pacifica Vignette

The island of Pacifica contains three sovereign countries: The Confederation of Washorgon States; The Republic of Nevidah; and The Peoples Republic of Califon. Califon is a Regional Hegemon in long-standing conflict with Nevidah over minerals and other economic issues. Nevidah is in mutual defense arrangement with Pacific nations including the USA. Washorgon traditionally maintains neutrality with Califon and Nevidah due to trade relationships and access to port facilities in Califon and Nevidah. The year is 2022; the Pacifica mineral fields are a major source of rare minerals. Califon has been conducting a campaign against Nevidah to obtain exclusive control of the mineral fields. Califon, seeks to limit US influence on Nevidah and the ability of US to provide assurance to Nevidah by exploiting the dependence of US forces on spectrum & cyber. The objective is to assess the effect of cyber attacks by Califon on a US Operations Center.

2.8.1 *The Organization Model*

The relevant components of internal organization structure of the Operations Center have been assumed to consist of the Situation Understanding Community of Interest (SU-COI), the Design and Plan COI (DP-COI) and the Command COI. (CC). It is assumed that all decision makers in each COIs share the same set of Situation Assessment (SA) and Response Selection (RS) algorithms (Fig. 2.6) and that they form a team. All the team members share the same goal. However, each team member may have a different area of expertise. For example, in the SU-COI different intelligence organization may be represented. The different areas of expertise have been modeled by assigning different probabilities for selecting the SA and the RS algorithms that a particular DM will use when an event occurs. Tables 2.1 and 2.2 reflect the assignment of probabilities for each DM in a COI.

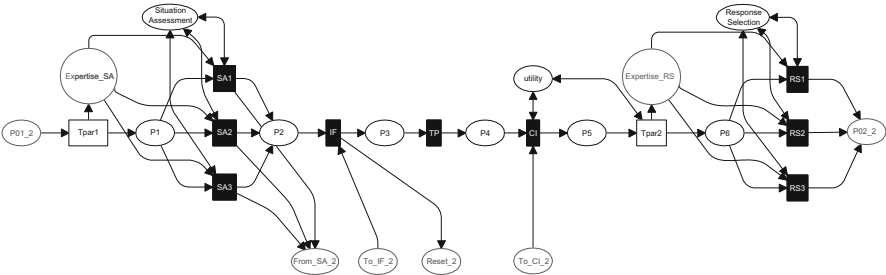


Fig. 2.6 Colored Petri net model of five-stage decision maker with three SA and three RS algorithms. (or processes)

Table 2.1 Probability of each individual DM selecting each SA algorithm for each incoming cyber event. (Expertise SA)

	SA algorithm 1	SA algorithm 2	SA algorithm 3
Event 1	p_{11}	p_{12}	p_{13}
Event 2	p_{21}	p_{22}	p_{23}
Event 3	p_{31}	p_{32}	p_{33}

Table 2.2 Probability of each individual DM selecting each RS algorithm for each identified cyber situation. (Expertise RS)

	RS algorithm 1	RS algorithm 2	RS algorithm 3
Situation 1	p_{11}	p_{12}	p_{13}
Situation 2	p_{21}	p_{22}	p_{23}
Situation 3	p_{31}	p_{32}	p_{33}

The COI teams may have different structures based on interactions between members. Two main structures were modeled: Collaborative (Fig. 2.7) and De-Conflicted (Fig. 2.8) as defined in Alberts and Hayes (2005).

The team designs in Figs. 2.7 and 2.8 were expressed in the form of Colored Petri Nets. In Fig. 2.9 the Petri net of the Design & Plan COI is shown. The hierarchical capabilities of Petri nets were used: each DM in Fig. 2.9 is represented by a substitution transition which contains the five-stage model of Fig. 2.6.

Since the team members receive some common inputs but each one can receive unique inputs, inconsistencies can occur that result in different situation assessments. Three mechanisms for resolving inconsistencies within a team have been postulated and modeled: (a) Repeat assessment for inconsistencies at the Information Fusion (IF) stage; (b) Utility maximizing decision at the Command Interpretation (CI) stage; and (c) Plurality voting at the Response Selection (RS) stage. If a decision maker encounters an inconsistency at the IF stage, the entire team will repeat the situation assessment. This may continue until a predefined time interval is exceeded tat which time the DM will continue with his own assessment even if it is not consistent with the assessment of other team members. If the DM faces conflicting data at the CI stage then he will select the option with the lowest associated cost. An example of the utility table that each decision maker uses is shown in Table 2.3.

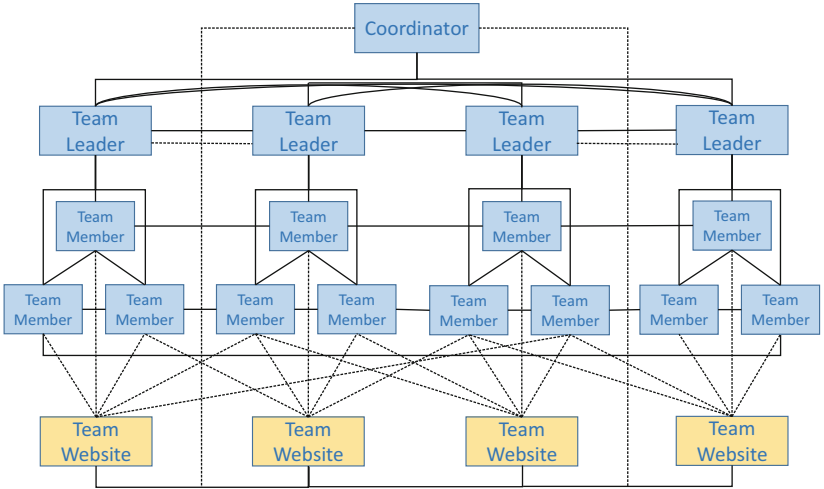


Fig. 2.7 Collaborative team structure. (Alberts and Hayes 2005)

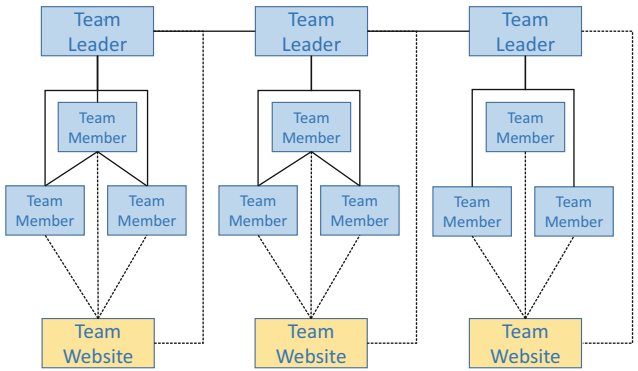


Fig. 2.8 De-conflicted team structure. (Alberts and Hayes 2005)

The team’s final response in the case of any inconsistencies would be decided based on a plurality vote, i.e., the response that received the highest number of votes from the team members.

2.8.2 The Network Model and Cyber Exploits

The communication network that enables interactions among the organization members and also between the organization and the external environment has been modeled using the OMNeT++ simulation framework (OMNeT++ 2014). Each DM is assigned a dedicated terminal to work with. The implicit assumption is that

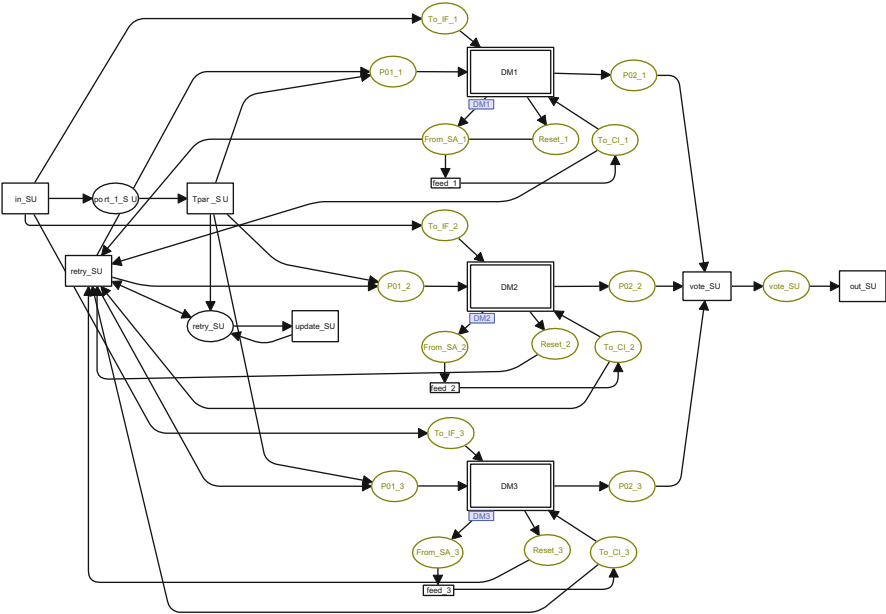


Fig. 2.9 Model of a three DM SU-COI team using the de-conflicted team design

Table 2.3 Cost of selecting a response for each situation

	Response 1	Response 2	Response 3
Situation 1	1	100	100
Situation 2	100	1	100
Situation 3	100	100	1

all the communications pass through network. The structure of the network model is shown in Figs. 2.10, 2.11 and 2.12.

The effects of two kinds of cyber exploits have been modeled: the effects on the organization’s interactions of availability attacks such as denial of service and of integrity attacks in which data are modified by the attacker. The availability attacks were implemented by changing the communication channel’s data rate during the execution of the scenario. The starting time of the attack (in the scenario timeline) and the reduction of channel throughput rate expressed as a percentage are two parameters characterizing the availability attack. The locality of the attack is another attribute.

The integrity exploits were implemented by the attacker modifying the data received by a DM. This could happen at the IF stage or the CI stage. Attributes of the integrity attack are the he probability of exploit being present during the scenario execution and the place in the organization model at which it occurs.

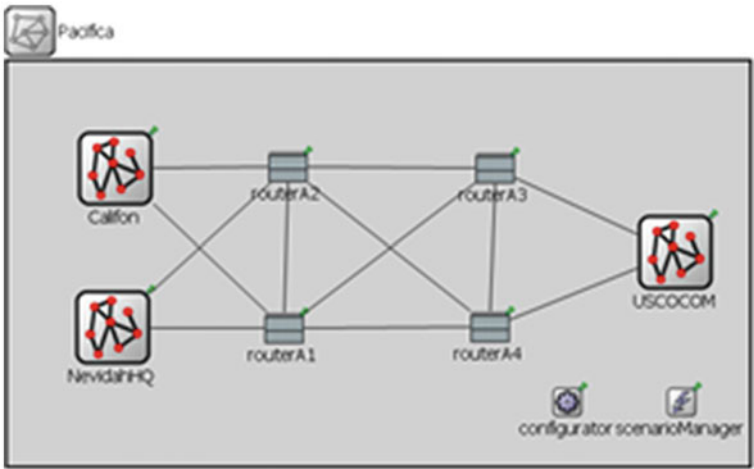


Fig. 2.10 The communication network. (top page)

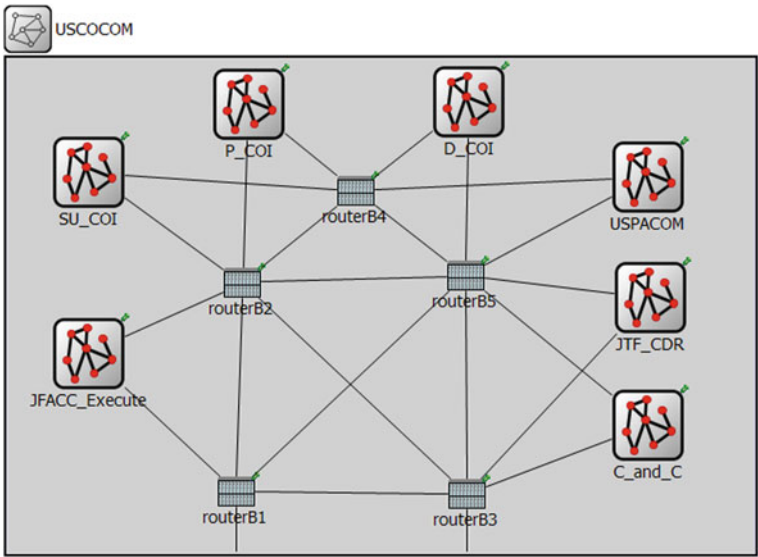
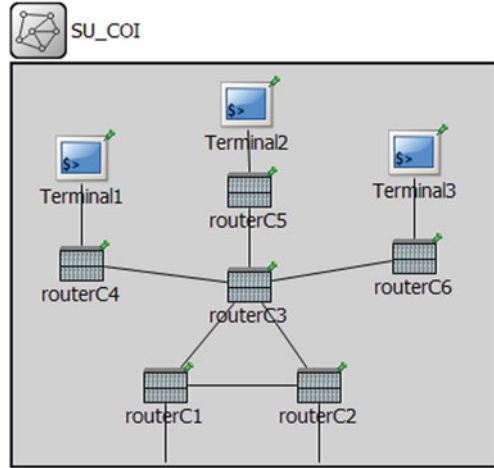


Fig. 2.11 The operations center network structure. (top page)

2.9 Computational Experiment and Results

For the Pacifica scenario in addition to the Situation Understanding COI and the Design and Plan COIs, additional entities were needed: the US Pacific Command (USPACOM), the Joint Task Force Commander (JTF_CDR), the Nevada Commander (NCDR), the Capabilities and Constraints COI, and the Task Forces (Execute

Fig. 2.12 Network topology for the situation understanding community of interest



COI). These were represented by single nodes; only the SU and DP COIs were modeled by organizational structures. The SU COI was modeled with the de-conflicted team design while the Design COI and the Plan COI have collaborative organizational structures. The underlying architecture is an experimental architecture to effect Integrated Global Command and Control. The Petri net model of the complete organization (the top level) is shown in Fig. 2.13. All communications between the entities and within the entities occur through the network.

An activity model was developed to indicate the flow of data and of control and the resulting communications. A segment of the activity model is shown in Fig. 2.14.

The expertise probability tables for the decision makers, defined in Tables 2.1 and 2.2, were assigned the values shown in Tables 2.4 and 2.5.

Given this model, the Colored Petri net model of the organization and the OMNeT++ model of the network were executed on the C2 Wind Tunnel and data were collected so that the four Measures of Performance could be computed. The four measures were:

1. Accuracy of Organizational Response (*Accuracy*)
2. Timeliness of Organizational Response (*Timeliness*)
3. Degree of Information Consistency (*DIC*)
4. Degree of Synchronization (*DoS*)

These four measures provide us with a holistic view of organizational performance. The MOPs under normal condition (no exploit) are presented in Table 2.6 as a reference.

The availability attack is localized in the USPACOM network area and starts at scenario time t_{start} equal to 20. The throughput will be decrease from $10Mbps$ to $4Mbps$ for all the links directly connected to the main routers during the attack. The MOPs under availability exploit are summarized in Table 2.7.

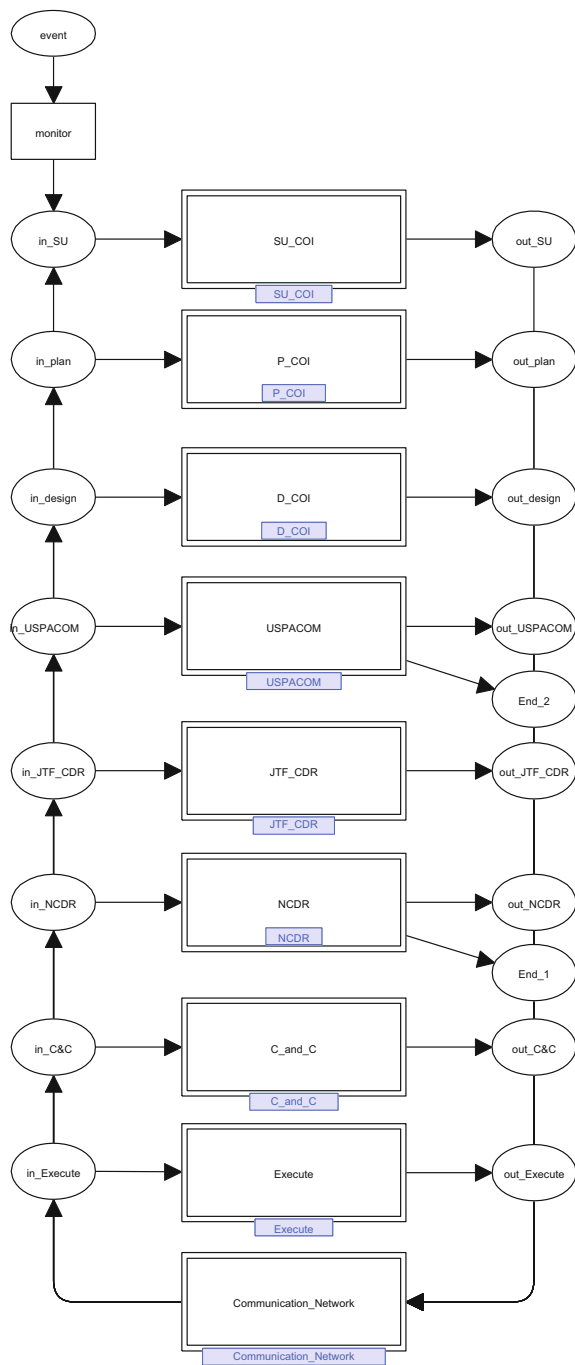


Fig. 2.13 The Petri net model of the Pacifica vignette. (top page)

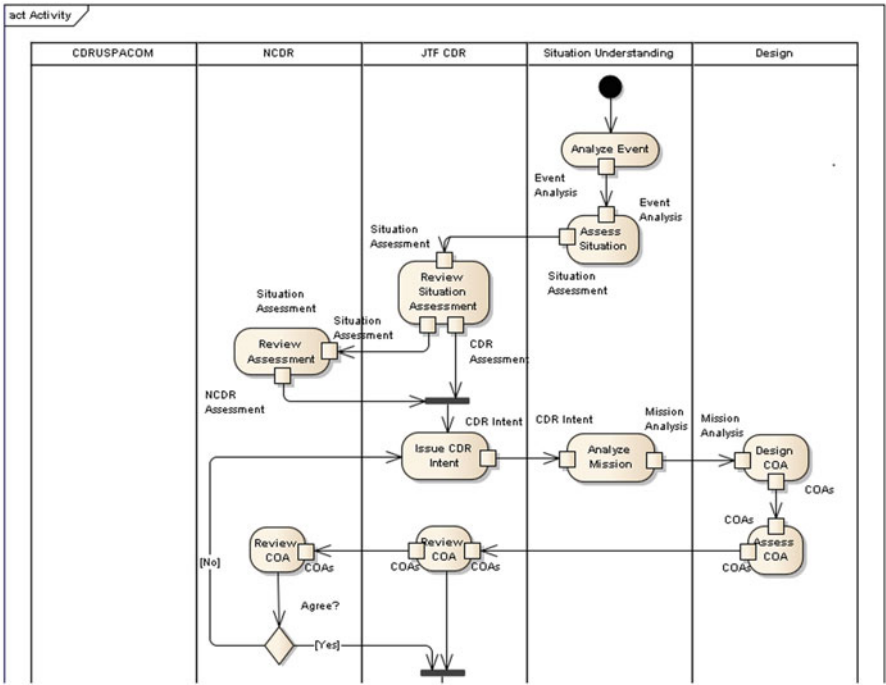


Fig. 2.14 Segment of the activity diagram describing the Pacifica scenario vignette

Table 2.4 Expertise of each DM at the SA stage

	SA algorithm 1	SA algorithm 2	SA algorithm 3
Event 1	0.9	0.05	0.05
Event 2	0.1	0.8	0.1
Event 3	0.2	0.1	0.7

Table 2.5 Expertise of each DM at the RS stage

	RS algorithm 1	RS algorithm 2	RS algorithm 3
Situation 1	0.9	0.05	0.05
Situation 2	0.1	0.8	0.1
Situation 3	0.2	0.1	0.7

The integrity attack is targeted on the Information Fusion (IF) stage of the fifth decision maker (DM-5) in the Planning COI team. The probability of the exploit being present is high ($p = 99\%$). The outcomes of the experiment are provided in Table 2.8.

Comparison of the results under normal conditions (Table 2.6) with no cyber exploits and the availability exploit (Table 2.7) displays an increase in operation time and degradation of organizational accuracy. A similar comparison between

Table 2.6 Performance measures in the absence of cyber exploits

Accuracy	Timeliness	DIC	DoS
0.71	294	0.94	7.35

Table 2.7 Performance measures in the case of availability attacks

Accuracy	Timeliness	DIC	DoS
0.53	301	1.00	7.35

Table 2.8 Performance measures in the case of integrity attack

Accuracy	Timeliness	DIC	DoS
0.65	308	0.93	7.88

Tables 2.6 and 2.8 shows that all the measures of performance were degraded when a focused integrity attack was made on a single decision maker in this large multi-person decision making organization. These results suggest that an integrity attack will cause performance degradation across the various measures while availability attacks prolong the mission and decrease the accuracy of the response but they will not affect the information consistency and synchronization of an organization, i.e., its coordination.

These results can now form the basis for assessing the effect of various vulnerabilities and provide needed information in developing a strategy for denying benefits of action and for determining the red lines for punishment responses.

2.10 Conclusions

A new approach based on multi-formalism modeling to model, analyze, and evaluate the effect of cyber exploits on the coordination in organizations has been presented. The focus is on the effect that cyber exploits have on the performance of a decision making organization when its ability to share uncorrupted information in a timely manner is degraded due to cyber exploits on the networks that support the interactions between organization members. Two new measures of performance, information consistency and synchronization, were used to demonstrate the effect of cyber exploits, as well as the traditional ones of accuracy and timeliness. The approach provides useful data for developing effective cyber deterrence and assurance strategies and for prioritizing elements of the four influence levers.

References

- Abu Jbara A, Levis AH (2013) Semantically correct representation of multi-model interoperations. Proc. 26th International FLAIRS Conference, St Pete Beach, FL, May
- AFSAB (2008) Defending and operating in a contested cyber domain, Air Force Scientific Advisory Board, Sztipanovits J Levis AH (eds) SAB-TR-08-01
- Alberts DS, Hayes RE (2005) Campaigns of experimentation: Pathways to innovation and transformation. CCRP Publication Series, Washington, DC
- CPN Tools (2014) <http://www.cpntools.org>
- DO-JOC (2006) Deterrence Operation Joint Operating Concept, Version 2.0, Department of Defense, 2006 (Available at <http://www.dtic.mil/futurejointwarfare>)
- Geer Jr., Daniel E., (2010) Cybersecurity and national policy, Harvard National Security Journal, vol. 1
- Grevet JL, Levis AH (1988) Coordination in organizations with decision support systems. Proc. 1988 Symposium on C2 Research, Monterey, CA, June 1988, pp. 387–399
- Gribaudo M, Iacono M (2014) An introduction to multiformalism modeling. In: Theory and Application of Multi-Formalism Modeling, Gribaudo M Iacono M (eds), IGI Global, Hershey, PA, pp. 1–16
- Hemingway G, Neema H, Sztipanovits J, Karsai G (2011) Rapid synthesis of high-level architecture-based heterogeneous simulation: A model-based integration approach. Simulation, March
- INET (2014) <http://inet.omnetpp.org>
- Jensen K, Kristensen LM (2009) Coloured Petri Nets. Springer, Berlin
- Levis AH (1992) A Colored Petri Net model of intelligent nodes. In: Robotics and Flexible Manufacturing Systems, Gentina JC Tzafestas SG (eds) Elsevier Science Publishers B. V., The Netherlands
- Levis AH, Zaidi AK, Rafi MR (2012) Multi-modeling and meta-modeling of human organizations. Proc. 4th Int'l Conf. on Applied Human Factors and Ergonomics—AHFE2012 San Francisco, CA, July
- OMNeT++ (2014) <http://www.omnetpp.org>
- Pflanz M, Levis AH (2014) On measuring resilience in Command and Control architectures. In: Suri N and Cabri G (eds) Engineering Adaptive and Resilient Computing Systems. Taylor & Francis, London
- Remy PA, Levis AH, Jin VY (1988) On the design of distributed organizational structures. *Automatica*, 24(1) 81–86
- The Economist (2014) 411(8885):23–26
- Welch, Gen. Larry (2008) presentation to Cyber Warfare 2008, London, U.K., 31 March 2008

Cyber Warfare

Building the Scientific Foundation

Jajodia, S.; Shakarian, P.; Subrahmanian, V.S.; Coyan, V.; Wang, C. (Eds.)

2015, XIII, 321 p. 83 illus., 49 illus. in color., Hardcover

ISBN: 978-3-319-14038-4