REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
18-05-2004	FINAL	

4. TITLE AND SUBTITLE
Preparing the Virtual Battlefield for War: A Cyber Threat

"Survival Kit" for Commanders

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Carol J. Moore

Paper Advisor: CDR Alan Wall, USN

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Joint Military Operations Department
Naval War College
686 Cushing Road
Newport, RI 02841-1207

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution is unlimited.

13. SUPPLEMENTARY NOTES A paper submitted to the faculty of the NWC in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Department of the Navy.

14. ABSTRACT

While the "traditional" Intelligence Preparation of the Battlefield (IPB) process adequately supports the commander's overall planning and decision-making by providing a logical framework for battlefield analysis, it does not consider threats in the virtual battlefield. The process presented in this paper merges the structured approach of the IPB with the software/network security community's "Security Threat Modeling" approach into a new process called Intelligence Preparation of the Virtual Battlefield or IPVB. The purpose of the IPVB is to provide the Commander with a more holistic understanding of all the threats posed to the networks in the area of operations and allow improved overall decision-making regarding the "virtual battlefield."

15. SUBJECT TERMS
Information Warfare, Cyber Threat, Information Operations, Threat Modeling, IPB, JIPB

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Chairman, JMO Dept
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED		23	19b. TELEPHONE NUMBER *(include area code)* 401-841-3556

Standard Form 298 (Rev. 8-98)

NAVAL WAR COLLEGE
Newport, RI

PREPARING THE VIRTUAL BATTLEFIELD FOR WAR: A CYBER THREAT "SURVIVAL KIT" FOR COMMANDERS

By

Carol J. Moore, CISSP
National Security Agency

18 May 2004

A paper submitted to the faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations.

The contents of this paper reflect my own personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

Signature: _____

_____

CDR Alan D. Wall, USN

Abstract

While the "traditional" Intelligence Preparation of the Battlefield (IPB) process adequately supports the commander's overall planning and decision-making by providing a logical framework for battlefield analysis, it does not consider threats in the virtual battlefield. The process presented in this paper merges the structured approach of the IPB with the software/network security community's "Security Threat Modeling" approach into a new process called Intelligence Preparation of the Virtual Battlefield or IPVB. The purpose of the IPVB is to provide the Commander with a more holistic understanding of all the threats posed to the networks in the area of operations and allow improved overall decision-making regarding the "virtual battlefield."

Table of Contents

I. Introduction 1

II. Background 1

III. Overview of the IPB and Security Threat Modeling Processes 3

A. Intelligence Preparation of the Battlefield (IPB): 3
B. Security Threat Modeling: 4

IV. Proposed Process – Intelligence Preparation of the Virtual Battlefield (IPVB) 5

Objective, Means and Ends of the IPVB 5
1. Step 1: Define and Model the Virtual Battlespace Environment 6
2. Step 2: Identify Threats using *"Attack Tree"* Methodology 10
3. Step 3: Describe the *Effects* of Threats using "STRIDE" 12
4. Step 4: Consult Intelligence Community (IC) Threat Reporting Information 13
5. Step 5: Characterize the *Risk* using *"DREAD"* 15
6. Step 6: Determine Adversary Courses of Action (COA) 17

V. Counterarguments 18

VI. Recommendations 19

VII. Summary 22

Bibliography 23

Table of Figures

Figure 1 – Code Red Penetration Map 2

Figure 2 – Software Consortium's Security Threat Modeling Process 4

Figure 3 - Steps in the Intelligence Preparation of the Virtual Battlefield Process 6

Figure 4 - Sample of a Threat Tree 11

Figure 5 - Example of Threat STRIDE Classification 13

Figure 6 - Example of DREAD Criteria Evaluation 16

Figure 7 - Example of SANS Internet Storm Center 21

I. Introduction

While the "traditional" Intelligence Preparation of the Battlefield (IPB) process adequately supports the commander's overall planning and decision-making by providing a logical framework for battlefield analysis, it does not consider threats in the virtual battlefield. The IPB process must merge with the network security community's "Threat Modeling" methodology into a new process that provides a commander with a more holistic understanding of all the threats posed to the networks in the area of operations and allow improved overall decision-making regarding the "virtual battlefield."

II. Background

The importance of information in military operations cannot be overstated. "Net-Centric Warfare", "Information Dominance," "Information Superiority," "Full-Spectrum Dominance" are prominent themes in the U.S. National Security Strategy (NSS), the JCS Joint Vision-2020 (JV-2020) and the DoD Quadrennial Defense Review (QDR). Each document underscores the concept that obtaining the advantage in the "virtual battlespace environment" is vital for military forces to maintain the freedom of action to achieve military objectives. "Virtual battlespace awareness" includes the ability to have an interactive, timely, accurate and relevant "picture" of both adversary and friendly force operations within the virtual battlespace—a very tall order.

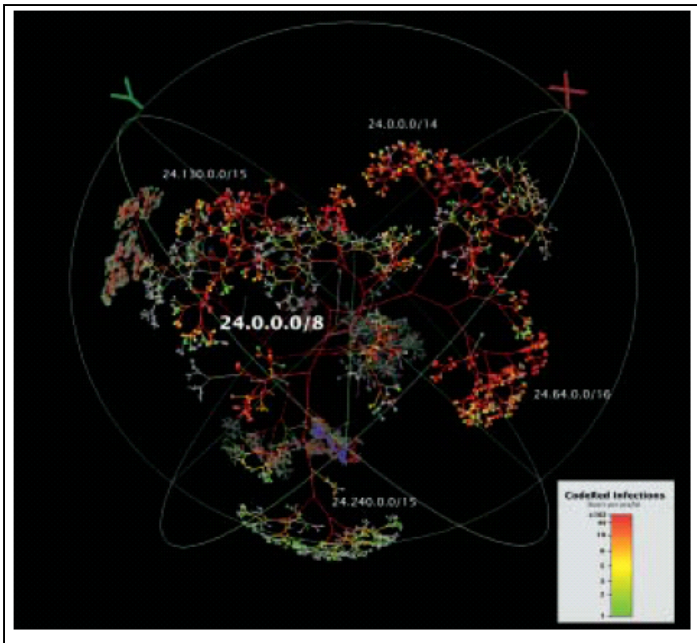
> ***"..In the future the DoD will treat information operations and intelligence not simply as enablers of current U.S. forces but rather as core capabilities of future forces."(DoD QDR)***

Rapid advances in technology have substantially increased both the availability and complexity of the information systems supporting military operations. These advances present many challenges to joint/combined military operations and require the operational

Commander to understand the interrelationships between the kinetic and virtual battlespace from both a defensive and offensive perspective. For example, one of the unique challenges in this environment is protecting friendly information while simultaneously adversely affecting the enemy's information. Further complicating this challenge is the ubiquitousness of the networks. Where public and private information systems were previously separate, today they connect to the same critical infrastructure backbone in which all the sectors of our economy operate—energy, transportation, finance and banking, information and telecommunications, public health, emergency services, water, chemical, food, agriculture and postal and shipping.[1] Estimates are that commercial information infrastructures support 95 percent of DoD communications.

> ***"…information, information processing, and communications networks are at the core of every military activity."(JV-2020)***

Commanders can no longer concern themselves solely with operational readiness and threats to military/DoD systems as if they were entities unto themselves. Therefore, IPBs prepared to support military operations must include the current readiness status of the virtual battlefield similar to the way public health "surveillance systems" collect and monitor data for disease trends and/or outbreaks so that health



A Mapping of Code Red Penetration on a Portion of the Internet.

Image courtesy UCSD/CAIDA (www.caida.org) © 2002 The Regents of the University of California.

Figure 1 – Code Red Penetration Map

[1] The National Strategy to Secure Cyberspace, http://www.whitehouse.gov/pcipb/, Internet, retrieved 27 April 2004.

professionals can take appropriate action to protect the public health. Using this analogy, a Commander "armed" with "network surveillance data" regarding current types of attacks occurring in the "virtual battlefield" can make better-informed decisions regarding military operations and the extent of protection required. In order to interpret and apply this information to a military campaign or operation, the Commander requires a more thorough understanding of friendly networks and the relative, threats, risks, and vulnerabilities facing them.

This paper outlines a proposed merge of the IPB and Threat Modeling processes using their key concepts into a new process called **Intelligence Preparation of the Virtual Battlefield (IPVB).**

III. Overview of the IPB and Security Threat Modeling Processes

A. Intelligence Preparation of the Battlefield (IPB):

IPB is a process used to analyze the threat and environment in a specific geographic area to support the Commander's military campaign or operations planning and decision making. It involves the following four basic steps:

1. **Define the battlespace environment**
2. **Describe the battlespace's effects**
3. **Evaluate the adversary**
4. **Determine adversary potential courses of action (COAs)**

IPB is a continuous process used throughout planned and executed military operations. Commanders and their staffs use the IPB "to visualize the full spectrum of adversary capabilities and potential courses of action across all dimensions of the battlespace." It assists analysts in identifying facts and assumptions about the battlespace environment and

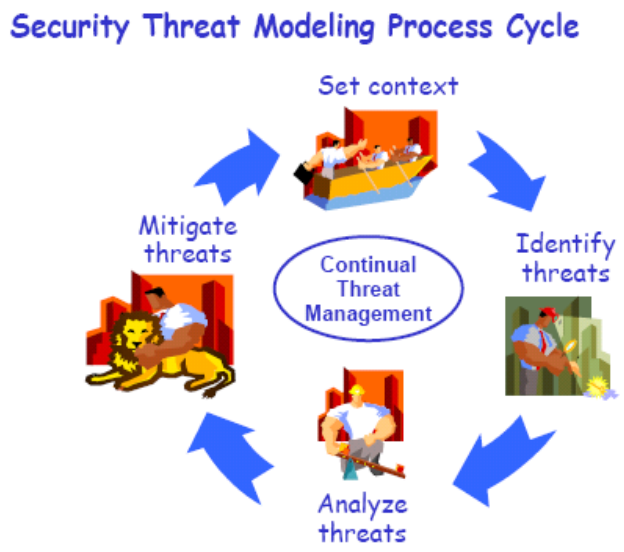
the adversary to facilitate campaign planning and development of friendly COAs. The output of the IPB also becomes the foundation for intelligence direction and synchronization to support the selected COA.[2]

B. Security Threat Modeling:

Security Threat Modeling is a risk assessment and mitigation process used in the private sector for securing network/system environments. The software development community also uses *Threat Models* to improve the security design of application and operating system software.[3]

Generally, a *Security Threat Model* is a security-based analysis that assists in determining the highest-level security risks posed to a product and how these attacks can manifest themselves.[4] A *Security Threat Modeling* process generally contains the four major steps shown in Figure 2. For example, Microsoft has begun to implement *Threat Modeling* during their software development cycles to assist designers

Figure 2 – Software Consortium's Security Threat Modeling Process



[2] Joint Publication 2-01.3, "Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace," dated 24 May 2000.

[3] The large numbers of publicly disclosed vulnerabilities in production software during the past few years has caused the software development community to implement Threat Modeling techniques into their design process. The premise is that by addressing vulnerabilities during the development stage when secure coding practices and mitigation techniques can be designed into a product is much cheaper than fixing vulnerabilities post-production when clients remain vulnerable until they download the latest vendor security patch and/or upgrade.

[4] Software Productivity Consortium, Quick Reference Card, www.software.org/security, retrieved from the Internet on 5/8/04.

in becoming aware of the various types of threats in the computing environment. Through the *Threat Modeling* process, a *Threat Profile* emerges which Microsoft software designers use to make decisions about how to eliminate or mitigate security risks. When changes occur in the product or environment, the effects are reassessed against the original *Threat Profile* and a new *Threat Profile* is produced.

IV. Proposed Process – Intelligence Preparation of the Virtual Battlefield (IPVB)

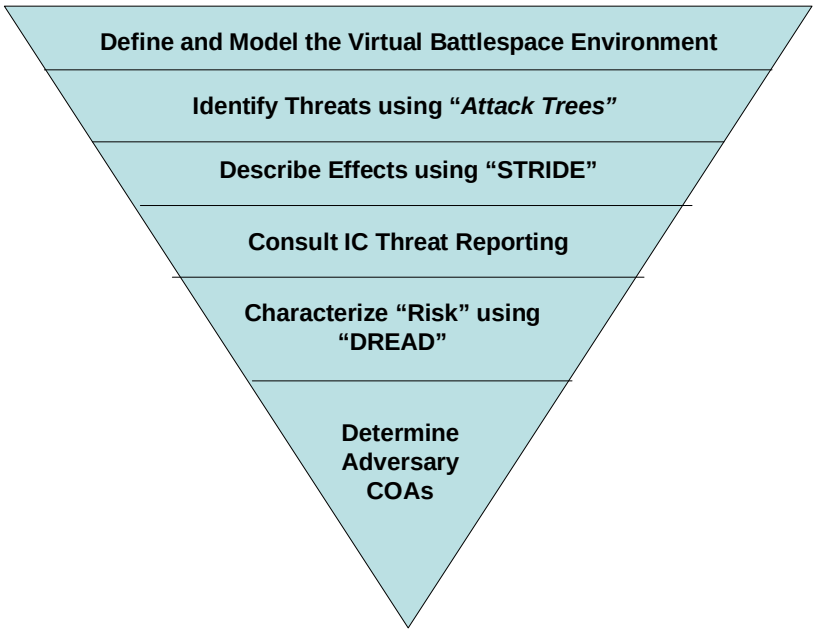
Objective, Means and Ends of the IPVB

The ***objective*** of the IPVB process is to provide a more holistic understanding of threats to the virtual battlefield to reduce uncertainties concerning the adversary, the environment, and the network "terrain" for any type of military operation[5]. The ***means*** used to accomplish this objective are *Threat Modeling* techniques adapted to the IPB process. The ***outcome or ends*** of the IPVB is an improved level of understanding regarding identified threats, risks and vulnerabilities, more focused Information Assurance (IA) intelligence collection and analysis, and better overall decision-making regarding the defensive and offensive perspectives of the "virtual battlefield" environment.

The IPVB process contains six steps shown in Figure 3. The following paragraphs discuss each step in the IPVB including various tools, methodologies, and resources. Included are suggested organizations that may have resources or key information for a particular step in the IPVB. These suggestions are a starting point and not necessarily a limitation of available resources. Section VI, Recommendations contains a discussion of additional areas that remain to be developed or must change to support the process.

[5] Security Focus, Infocus Article, Internet, http://www.securityfocus.com/printable/infocus/1234, retrieved on 5/6/2004.

Figure 3 - Steps in the Intelligence Preparation of the Virtual Battlefield Process



1. Step 1: Define and Model the Virtual Battlespace Environment

Step 1 of the IPVB is very similar to the first step in the IPB when an assessment of the physical battlespace terrain takes place. In this case, the analyst identifies the virtual "terrain" by gathering background information detailing significant characteristics of the network environment. As in the IPB, this step is the most critical because succeeding steps will specifically address characteristics of the virtual battlespace environment that may directly influence the campaign or operational objectives. The key to success in defining the virtual environment is to analyze it from an adversarial perspective. As is the case in the IPB analysis of physical terrain environments, the virtual battlespace environment includes limits in terms of areas of operation, areas of interest, and areas of influence. The following are suggested network environment categories identified in Step 1 during the planning stage and continuously refined throughout the military operation:

- **Network Classification**: The classification of the network(s) in which friendly forces will be operating (e.g., Internet, NIPRNET, SIPRNET, JWICS, Combined/Coalition Wide Area Network (COWAN), etc.) [Suggested Sources: J6 staff]

- **Architecture Types**: List the type of architectures (e.g., wireless local area network (LAN), Ethernet, Virtual Private Network (VPN), etc.) the adversary would traverse or encounter. [Suggested Sources: J6 Staff, Service CERTs, Service Red/Blue Team assessment results.]

- **Software Applications**: List the applications the adversary might encounter or target in the networks (e.g., OUTLOOK, PowerPoint, Excel, Internet Explorer, Netscape, JOPES, GCCS, etc.). [Suggested Sources: J6 Staff, Service CERTs, Service Red/Blue Team assessment results.]

- **Operating Systems**: List the main operating systems (e.g., Microsoft Windows, Linux, Unix, Apple, etc.) [Suggested Sources: J6 Staff, Service CERTs, Service Red/Blue Team assessment results.]

- **Existing Vulnerabilities**: List the publicly known vulnerabilities existing in the network environment. [Suggested Sources: DISA/IAVA, DoD/Service CERTs, Service Blue/Red Team Results.]

- **Type of Information:** List the types of information stored/processed in the identified networks (e.g., operational, command and control, classified, logistics, contracting, etc.) [Sources: J6 Staff, Service CERTs, Service Red/Blue Team assessment results]

- **Network Activity Baseline**[6]: If possible, determine the current baseline of activity in the identified network(s). Monitoring the level of activity on the network to develop a baseline is critically important in the planning/build-up stage as well as during military operations. Understanding and monitoring the current level of activity in the virtual battlefield environment is analogous to a doctor monitoring a patient's current heart or blood pressure because it provides a starting point from which to discover anomalous activity or behavior. In the virtual battlefield environment if activity suddenly occurs on the network(s) that is outside the normal profile, the Commander can consider the potential effects the activity may have on current/impending military operations.

Next, the analyst builds a network and/or data flow diagram to assist the Commander in understanding how the adversary views the virtual battlespace. The purpose of modeling the network(s) is to illustrate how data as well as "carbon-based units" interact in the operational network environment at the "10,000-foot level." This provides useful information for developing attack scenarios and mitigation techniques in later Steps. The following are items to include in building these model(s):

- **Identify major entry points into the network**: Defining these entry points helps to establish the boundaries of the virtual battlespace under analysis and to prioritize the Threat Modeling discussions in the next Step. For example, for each entry point into the network, the analyst considers what that entry point exposes about the underlying network(s) and the information/functionality it contains.

[6] Baselining: Wandel & Goltermann (June 1996, http://www.wg.com) define baselining as the actual measurement and recording of a network's state of operation over a period of time. It involves recording the current state of network operation to serve as a basis for comparison or control.

- **List all the places where the system *consumes data from*, *provides data to*, or *performs actions on behalf of* external entities:** Places where the networks intersect through guards, routers and firewalls, such as those between the Internet and NIPRNET, are obvious entry points to include. Additional places may include where data moves or is replicated from an external database onto a back-end database. Note that the level of detail involved in this step will be highly dependent upon the time available to complete the analysis. If the model and/or diagram show entry and exit points between networks of differing classifications, they must be classified accordingly. [Suggested Sources: Network/System Owner (e.g., DISA for SIPRNET, SECDEF for NIPRNET, DIA for JWICs, etc.), J6 Staff, Service Certs, Service Red/Blue Team assessment results.

- **Identify *assets* that could be the target of an attack by an adversary**: The importance of identifying assets during this step is that they may become the targets of threats to the network. In other words, the threat may be what the attacker may try to do to the asset or with the asset to affect military operations and/or decision-making processes. An asset example is information stored in a back-end database such as JOPES and/or a crucial firewall or router protecting a key network entry point.

- **Identify the *trust levels* required of entry points and assets:** A *trust level* describes the external entity that may interface with the entry point. In the case of *assets*, the *trust level* indicates what privilege level would normally be required in order to access the asset or entry point. For example, only a system/network administrator may be able to access a certain router serving as the entry point into another network. Trust levels assist in determining specific high-risk entry points and assets in the virtual battlespace

environment. This information is also very useful when discussing mitigation and risk strategies in later steps.

- *Trust levels* may also include *preconditions* required in order to access the asset or entry point. For example, all users accessing the SIPRNET must be U.S. citizens with SECRET-level clearances. The clearance in this example is the *precondition* to access the SIPRNET asset. *Preconditions* may also be role-based as in "only a user with system administrator-level privileges" can access firewall "A" which is the entry point into network "B."

- **Develop *Use Scenarios*:** *Use scenarios* describe how the network was intended or not intended to be used in the field. For example—

> ***The SIPRNET network is a US-only, war fighting, command and control network and not intended for combined/coalition command and control operations.***

For this level of analysis, the *Use Scenario* can be limited to a paragraph or two to document the original network design assumptions and as information to use in considering threat mitigation techniques. [Suggested Sources: J6 Staff, System Owners]

2. Step 2: Identify Threats using *"Attack Tree"*[7] Methodology

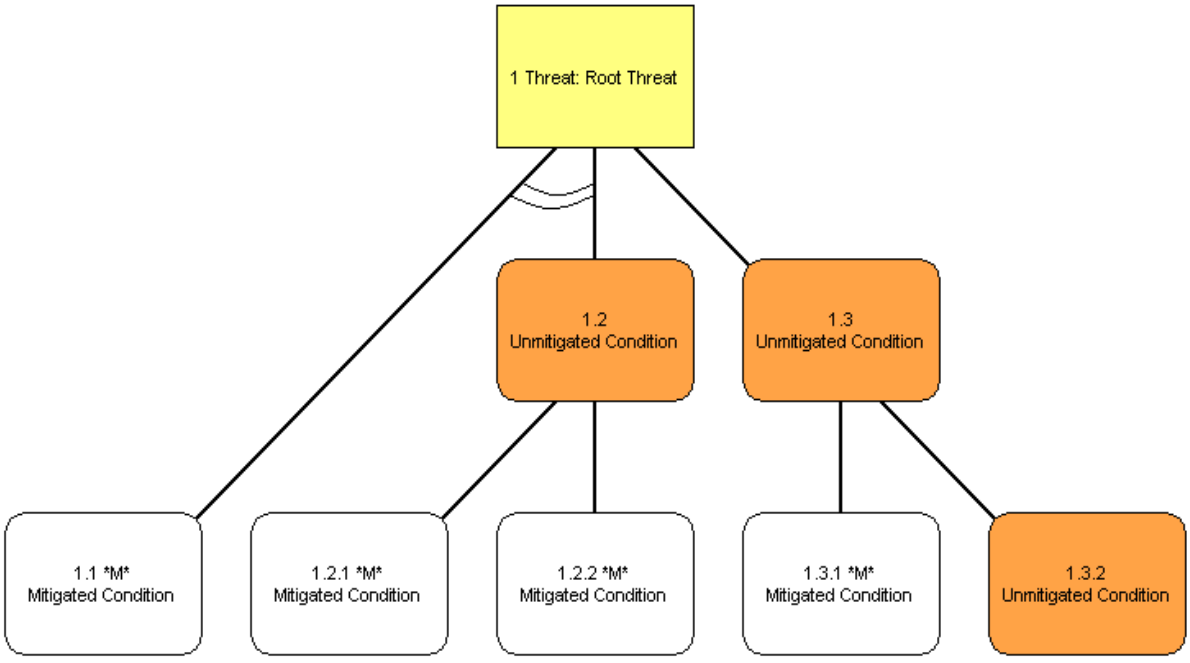
In Step 2, the analyst will use all the information produced in Step 1 to create attack hypotheses using "*Threat Trees*." Data flow diagrams and/or network models developed in the previous step are used here to develop specific threat hypotheses. They also assist the analyst and the Commander in better understanding the functionality exposed by

[7] One of the first individuals to suggest *"Attack Trees"* as a methodology for analyzing and mitigating attacks was the renowned security expert, Bruce Schneier. In his 1999 article on this topic, Mr. Schneier explains, "Attack trees provide a formal, methodical method for describing the security of systems, based on varying attacks." Refer to "Dr. Dobbs," http://www.ddj.com/documents/s=896/ddj9912a/9912a.htm.

the network/system and the attacker's potential goals. (Reference Bruce Schneier's 1999 article for more background information on "*Attack Trees*.")

Figure 4 is a Microsoft example of a *"Threat Tree."* This example visually represents valid attack paths for a root threat node labeled in Box 1 as "*Root* Threat." *Mitigated conditions* are represented in Boxes 1.1, 1.2.1, 1.2.2, and 1.3.1 (white boxes if you are viewing this document online) and *unmitigated conditions* are represented in Boxes 1.2 and 1.3 (orange boxes). In this example, there are four possible attack paths of which only one (Path 1.3.2 -> 1.3 -> 1) has no mitigating nodes and thus represents a valid attack path or vulnerability.[8]

Figure 4 - Sample of a Threat Tree



[8] Swiderski, Frank and Snyder, Window. Threat Modeling, Microsoft Professional Series, Microsoft Press, 16 June 2004 (advanced copy).

3. Step 3: Describe the *Effects* of Threats using "STRIDE"

The next step involves evaluating and documenting the potential *effects* of threats identified in Step 2. This step is very similar to describing the impact of attacks against military forces in the physical battlefield except that we are mainly concerned with effects on friendly capabilities and courses of action. For the virtual battlefield, *effects* describe what happens as a result of an adversary realizing a threat hypothesized in a *Threat Tree*. The *effects* to the virtual battlefield environment can be mission specific, depending upon the assets, resources, and current countermeasures in place. *Effects* may also depend upon the length of time that operations and/or critical functions are disrupted by the threat. The acronym "***STRIDE"*** is used by the software and network security designers to classify effects of threats to their specific environments. We use ***"STRIDE"*** as follows to describe and evaluate *effects* from threats modeled during Step 2[9]:

Spoofing: Spoofing allows an adversary to pose as another user, component, or other network that has an identity in the network being modeled.

Tampering: Tampering is the modification of data within the system to achieve a malicious goal.

Repudiation: Repudiation is the ability of an adversary to deny having performed some malicious activity against a network resource and/or asset because the system does not have sufficient evidence to prove otherwise.

Information Disclosure: Information Disclosure involves the exposure of protected data to the adversary.

Denial of Service: Denial of Service occurs when an adversary can prevent legitimate users from using the normal functionality of the system.

Elevation of Privilege: Elevation of Privilege occurs when an adversary assumes a Trust Level, with different privileges than he/she currently has, through illegitimate means.

Threats STRIDE Classification – Sample – Sample – Sample – Sample – Sample - Sample	
Threat	
ID	1
Name	Adversary gains access to the firewall remote administration interface resulting in access to the CENTCOM NIPRNET network.
Description	The main entry point into the CENTCOM network is a firewall with a remote administration interface that allows an authorized administrator to configure it via the Internet. The interface is disabled by default, but can be enabled using a default administrator username/password pair.
STRIDE Classification	**Tampering** **Information Disclosure** **Denial of Service** **Elevation of Privilege**
Mitigated?	No
Known Mitigation	If the remote administration interface is enabled, the administrator should change the default password.
Investigation Notes	(none)
Entry Points	(6) Remote Administration (3) Internet connection
Assets	(5) Firewall

Figure 5 - Example of Threat STRIDE Classification

[Suggested Sources: J6 Staff, System Owner, Service Red/Blue Team Members]

4. Step 4: Consult Intelligence Community (IC) Threat Reporting Information

In addition to evaluating the *effects* of threats, the purpose of Step 4 is to combine the results of the Step 2's *"Threat Tree"* analysis with intelligence information about specific adversaries. This step is similar to the IPB Step 3, "Evaluate the Adversary." The rationale for including this in the IPVB is that we know that adversaries are not "one size fits all." They have different levels of knowledge, skills, capabilities, resources, operating

[9] Adapted from Microsoft's interpretation of "STRIDE," taken from Writing Secure Code, 2nd Edition.

methods, tools, and motivation. Specific intelligence information about an adversary assists the analyst in refining parts of the "*Threat Tree"* that require immediate attention. For example, suppose we hypothesized in a "Threat Tree" during Step 2 that one of the threats we are concerned about is an adversary accessing the JOPES database and modifying the information it contains. The purpose of Step 4 in this case is to discover if there is a specific adversary planning to exploit JOPES. This information together with the *"Threat Tree"* analysis will help to develop and prioritize adversary courses of action that need to be mitigated.

During Step 4, be careful not to focus too much attention on the specific tools adversaries use (if known) as the single most important data set. Current cyber attack detection and response techniques focus on specific tools because they are analogous to *fingerprints* left behind at a crime scene. Although this may be useful to know for detection and response, it is **not** useful for conducting the kind of predictive analysis developed during IPVB.[10] What is useful is gaining an *understanding of the adversary's process of targeting friendly forces as well as their potential knowledge, skills, capabilities and motivation*. Step 4 is also an appropriate place to consult available "network surveillance" or "baseline" information to determine if there are indicators of impending attacks against the virtual battlespace area of operations (See Recommendations for more on this topic). [Suggested Sources: J2, Service CERTs, DoD-CERT, DISA/JTF-CNO, NSA's National Security Incident Response Center (NSIRC), DIA, CIA]

[10] Why is this so? Because cyber attack tools can be used in numerous, unpredictable ways. Attackers may combine one or more tools "chaining" them together to reach the ultimate objective. In addition, most clever attackers will modify their tool signatures to evade intrusion detection. The main point for this step is that simply collecting specific tool signatures will not be enough information to conduct the predictive analysis required for the virtual battlefield environment.

5. Step 5: Characterize the *Risk* using *"DREAD"*

In this step, the analyst characterizes the risk associated with specific vulnerabilities identified in Steps 3 and 4, for which we could not mitigate the risk, chose not to mitigate, or their mitigation status was unknown. In this context, a *vulnerability* is a *weakness in the network(s) that can be exploited by an adversary*.

"DREAD" is sometimes used as a method of characterizing risks associated with vulnerabilities in software. In IPVB, "DREAD" will be used to calculate the *risk* associated with vulnerabilities identified as a result of developing "Threat Trees" and analyzing the threat's *effects*. A sample risk analysis using "DREAD" criteria is shown in Figure 6. A value is calculated as an average of all the values assigned to each of the following criteria:

Damage Potential: Damage Potential ranks the extent of damage that occurs if a vulnerability is exploited.

Reproducibility: Reproducibility ranks how often an attempt at exploiting a vulnerability works.

Exploitability: Exploitability assigns a number to the effort required to exploit the vulnerability, and considers preconditions (such as whether the user must be an authenticated user).

Affected Users: Affected Users is a numeric value characterizing the ratio of installed instances of the network/system that are affected if an exploit becomes widely available.

Discoverability: Discoverability is the likelihood that the vulnerability, if left unpatched, would be discovered by external security researchers, hackers, etc. [Suggested Sources: J6 Staff, Service CERTs, Service Red/Blue Team members.]

Figure 6 - Example of DREAD Criteria Evaluation

Score	Affected Users	Damage Potential	Discoverability	Exploitability	Reproducibility
	How many of the users would be impacted by a successful attack?	What is the value of the damage that could be done by this threat?	How easily is this attack discovered?	How much effort and skill are required to perform this attack?	To what extent is the "success" of the attack deterministic?
10	All	The threat could jeopardize viability of the organization or the mission	Essentially not discoverable	Can be performed by a script kiddy or a novice	Works every time
8	Most	The threat could cause serious harm	Requires significant resources and expertise to discover	Requires some special operational or system knowledge	Requires several factors to be "cooperating"
5	Many	The threat could cause significant harm	Requires detailed, complex investigation	Requires overcoming moderately strong authentication and access control	Requires many factors to be "cooperating"
3	Some	The threat could cause an annoyance	Requires investigation but not too difficult to discover	Requires overcoming very strong authentication and access control	Requires very difficult to control sequence of events
1	None	The threat will cause no harm	Very easy to discover	Requires the resources of a nation-state, a lot of time, and money	Theoretically possible but very unlikely

* Howard, Michael, and David LeBlanc, *Writing Secure Code*, 2nd edition. Redmond, Washington: Microsoft Press, 2003.

6. Step 6: Determine Adversary Courses of Action (COA)

The next step in IPVB mirrors the process for determining enemy COAs in the IPB for a conventional conflict. In this step, the analyst develops a full set of adversary COAs based upon identified vulnerabilities that were evaluated as having the most damaging effects and best accomplish adversary objectives. The adversary COAs should also reflect current intelligence information regarding specific adversary objectives, desired end states, skills, knowledge, and capabilities. Note that each COA developed will be evaluated, prioritized, and refined over time as new information is learned.

During this step, the analyst should wargame each COA to determine how the adversary might execute operations in the virtual battlefield environment. If enough time is available, the COA should be wargamed in a lab setting where network environment conditions can be modeled. By modeling the targeted networks and their environments, the analyst will generate more qualitative information on each adversary COA's feasibility and effectiveness. This type of testing will highlight key events that must take place in order for the adversary to accomplish the main objective. Mitigation techniques can also be tested to ensure they effectively prevent the adversary from being successful.

Additionally, likely *branches* and *sequels* may be discovered through wargaming. For example, suppose the adversary breaks into a network with the intention of stealing sensitive information. While in the network, he discovers that he can also modify information in a key logistical database. A branch might involve developing the access to the database further to discover additional avenues of attack and exploitation. Another branch might involve additional network reconnaissance inside this network to discover other back end networks trusted by the network where the adversary initially gained access. Using

"trust relationships" between networks, the adversary may choose yet other branches and sequels. The *"Threat Models"* developed earlier will be very useful for conducting this type of analysis because the various *"Threat Paths"* documented in the model may represent potential branches/sequels.

An initial set of intelligence collection requirements should be developed based upon analysis and wargaming adversary COAs. These requirements should assist the Commander in addressing vulnerabilities that could **not** be mitigated. Using the JOPES example again, suppose we know that our specific adversary is planning to target JOPES, but we are uncertain how. Intelligence collection requirements could be developed that seeks to answer that uncertainty. Additional "network surveillance" requirements might also be requested to monitor the JOPES system for indicators of an impending attack. [Suggested Sources: J2, J6, Service CERTs, Service Red/Blue Team Members.]

V. Counterarguments

Some might argue that having a separate process for preparing the virtual battlefield is unnecessary and in most cases nearly impossible to accomplish. The Global Information Grid (GIG) concept supports all Department of Defense, National Security and related Intelligence community missions and functions in war and peacetime. It also will provide interfaces to coalition, allied and non-DoD users and systems. Modeling threats in this large and complex network environment will admittedly be difficult. The key, however, is to begin documenting the entry points, assets and resources in each of these networks, and analyzing the effects of threats and vulnerabilities to those environments. Once a baseline understanding of each network is documented in IPVB for the first time, subsequent assessments will add more depth and analysis to understanding the GIG's overall "security

health." Perhaps the most significant benefit of using threat modeling is that once these models are completed, virtually anyone can understand the threats and vulnerabilities in the environment without having to have knowledge of all the technical details of the networks and vulnerabilities involved.

VI. Recommendations

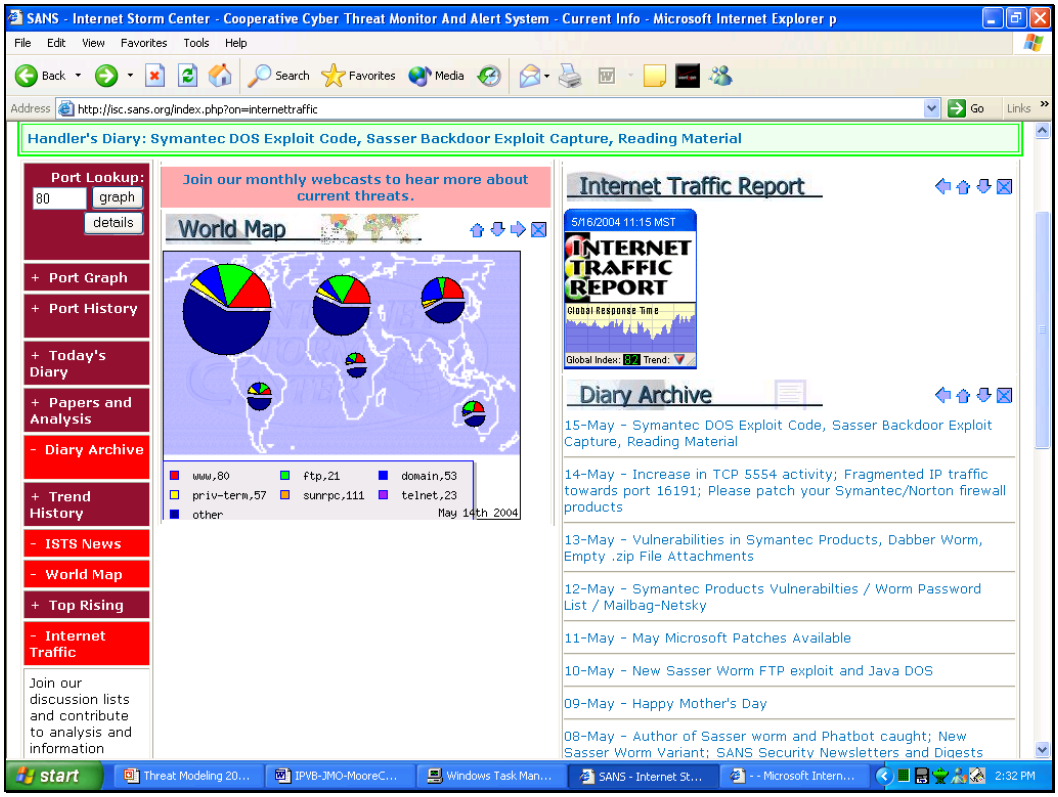
The IPVB process proposed in this paper addresses information a Commander and his /her staff needs to prepare for and operate in the virtual battlefield. The purpose of the IPVB is to support the Commander's campaign planning and decision making by identifying, assessing and estimating threats, vulnerabilities and risks to the virtual battlefield environment and determining the most likely and dangerous COAs to friendly forces and mission. In order to refine and validate it, the IPVB process should be tested in a war game and/or exercise scenario to refine the steps and tools involved and improve the overall concept. In addition, the IPVB process should become either part of the Joint IPB (JIPB) document (Joint Publication 2-01.3) or a separate publication. It should also become part of the standard JMO curricula information at the service War Colleges.

There are some significant holes in the IPVB where contributing information is either incomplete or nonexistent. For example, as discussed earlier, there is a need to provide Commanders with proactive vice reactive "network surveillance" data. The "network surveillance" information on DoD networks is an emerging capability supported by NSA and DISA. The Joint Task Force-Computer Network Operations (JTF-CNO), which is collocated with DISA, is the organization officially tasked with monitoring the status of DoD information networks; however, its capability in the past has been more reactive vice proactive.

In the Director of Central Intelligence' 2002 Annual Report, CJCS Chairman General Myers noted, "NSA has developed and deployed a computer network defense intrusion detection system that significantly enhances protection of the Defense Information Infrastructure (DII). The system consists of a network of sensors that are strategically placed within the DoD infrastructure, providing analysts the capability to identify anomalous cyber activities traversing the network. The system complements local DoD intrusion detection systems by providing a layered cyber-defense system."[11] Although this capability is emerging, the analysis of anomalies in the DII and GII must become a key part of the IPVB process because it will provide the proactive "network surveillance" information required for successfully planning and executing current and future military operations on the virtual battlefield. The challenge is how to get similar "surveillance data" for other networks in the virtual area of operations such as the Internet, JWICS, etc. A good example of the type of "network surveillance" information may be the SANS (System Administration, Audit, Network Security) organization's "Internet Storm Watch" web site which provides "early warning data" for Internet users (see Figure 7).[12]

[11] Director of Central Intelligence 2002 Annual Report of the United States Intelligence Community, January 2003, http://www.cia.gov/cia/reports/Ann_Rpt_2002/index.html.
[12] See http://www.incidents.org, SANS "Internet Storm" Web site.

Figure 7 - Example of SANS Internet Storm Center



In addition to "network surveillance" information, Red Team results are suggested as potential key sources of information to use in the IPVB. No organization and/or group of people, other than actual adversaries or certain foreign intelligence organizations, can better characterize the U.S. virtual battlespace environment than Red Teams. Obtaining access to Red Team assessment information may prove difficult, however, since this information is normally treated as *proprietary* between the specific Red Team and customer organization. For this reason, it is recommended that all DoD/Service/Agency Red Teams provide "trend data" (e.g., most commonly found applications, operating systems, firewalls, vulnerabilities, etc.) yearly to JTF-CNO. The goal must be to provide this type of reporting more frequently, perhaps even weekly, at some point in the near future.

VII. Summary

The current IPB process adequately supports the commander's overall planning and decision-making by providing a logical framework for battlefield analysis; however, it does not holistically consider threats to the virtual battlefield. The process presented in this paper merges the structured approach of the IPB with the software/network security community's "Security Threat Modeling" approach into a new process called Intelligence Preparation of the Virtual Battlefield or IPVB. Further refining the steps in the IPVB through exercises and war games, incorporating network surveillance data, and Red Team trend information will result in an IPVB process that proactively provides the Commander with a holistic and predictive analysis capability of all the threats posed to the virtual battlefield area of operations.

Bibliography

Snyder, Window and Swiderski, Frank. Threat Modeling. Microsoft Press, Microsoft Professional Series, 16 June 2004.

Howard, Michael and LeBlanc, David C. Writing Secure Code, Second Edition, Microsoft Press, 4 December 2002.

Joint Publication 2-01.3, Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace, dated 24 May 2000.

The National Strategy to Secure Cyberspace, http://www.whitehouse.gov/pcipb/, Internet, retrieved 27April 2004.

JTF-CNO Fact Sheet, http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm, Internet, retrieved 1 May 2004.

Software Productivity Consortium, Quick Reference Card, www.software.org/security Internet, retrieved 8 May 2004.

Schneier, Bruce. Attack Trees: Modeling Security Threats, Dr. Dobb's Journal, http://www.ddj.com/documents/s=896/ddj9912a/9912a.htm, December 1999, Internet, retrieved 8 May 2004.

Internet Traffic Report, http://www.internettrafficreport.com/details.htm, Internet, retrieved 1 May 2004.

Military and Cyber-Defense: Reactions to the Threat, http://www.cdi.org/terrorism/cyberdefense-pr.cfm, Internet, retrieved 3 May 2004.

Defensive Information Warfare Organizational Action Plan, http://www.fas.org/irp/threat/cyber/docs/diw/ch16.html, Internet, retrieved 30 April 2004.

Winterfield, Steve. Cyber IPB, dated December 2001, http://64.233.161.104/search?q=cache:T6ygOVGrCVEJ:www.giac.org/practical/Steve_Winterfeld_GSEC.doc+combatant+commander+intelligence+requirements+AND+CND&hl=en, Internet, retrieved 2 May 2004.

Cyber IPB, http://www4.ncsu.edu/~jjyuill/Professional/Research/Projects/c-ipb-paper.html, Internet, retrieved 1 May 2004.

Director of Central Intelligence, 2002 Annual Report of the Intelligence Community, Support to Military Operations Chapter, January 2003,

http://www.cia.gov/cia/reports/Ann_Rpt_2002/smo.html, Internet, retrieved 2 May 2004.