

**Intelligence Preparation of the Information Battlespace – A Cyber Playbook for
Information Survivability**

**James K. Williams
Roderick A. Moore
Charles McCain**

**Zel Technologies, LLC.
Hampton Virginia**

Interest Areas: Information Assurance of Mission Critical Systems; Survivability Foundational Concepts and Philosophy; Using Formal Methods to Analyze Survivability; Managing Business Risk for Survivable Systems; Critical Infrastructure Protection

ABSTRACT

Conventional Information Assurance and Survivability technologies are largely concerned with firewalls; intrusion detection systems (IDS) and countermeasures that are either preventative or that can be applied in real-time during an active information attack. Zel Technologies, under the DARPA/AFRL Information Assurance and Survivability program has developed an automated Intelligence Preparation of the Information of the Battlespace (IPIB) decision support tool.¹

The intent of the IPIB tool is to provide predictive intelligence, using a structured process to assess survivability, with the aim of extending Information Assurance and Survivability activities into a proactive effort and reaction within human timelines. We do this with a systematic, continuous process that identifies where to look, when to look and what to expect to see (IDS definition, sensor placement, and tasking.) This should inform a cyber defense planner of the full range of activities (checklists) prior to attack and enable dynamic cyber decision support and control in the pre-attack, attack and recovery stages. This process also identifies critical functions and capabilities that must be protected/monitored to assure continuous operations and to insure survivability and recovery of those mission/application critical capabilities.

Put simply, the IPIB process is intended to help a decision maker visualize and understand the cyber environment of his/her critical infrastructure, define what is important to complete key functions/ their interdependencies and relationships to other infrastructure components, understand a potential adversary's courses of actions to effect those critical components, when to look for these activities/indicators and what to expect to see. When we consider the nanosecond timelines for cyber attacks, this is particularly beneficial, because it permits the decision-maker to anticipate an attack and establish

¹ This work is sponsored by DARPA under the contract management of the Air Force Research Laboratory (AFRL) Contract F30602-99-C-0168

survivability requirements/countermeasures before an attack takes places. *More importantly, it provides the decision maker the capability to dynamically model and simulate critical systems survivability based on potential adversary courses of actions prior to an experiencing cyber attack.*

INTRODUCTION

The traditional information survivability paradigm has focused on prevent, detect, respond and recover mechanisms inside a protected enclave. This concept presupposes an attacker must be inside your defended (mission critical) area when and if detected and has already begun an attack course of action. Using this paradigm requires a “duck and cover” mode of operations in an effort to “ride out” the attack...survivability is defined as a means of recovering operations and applications that have hopefully not been infected or affected by the cyber attack. In this schema, detection, assessment and critical asset recovery would have to be autonomic to be effective.

The IPIB process shifts the paradigm by creating a cyber defense strategy plan or “cyber defense playbook”. Similar to its kinetic counterpart in sports, the cyber defense strategy plan incorporates a structured process to assess survivability and develop defensive and potential “offensive” checklists with scripted plays to support a broad defense strategy. The first plays of the cyber defense playbook are scripted for static defense. As the IPIB process is repeatable and measurable, dynamic defense countermeasures can be modeled and simulated to provide a counter strategy and options. This IPIB cyber defense strategy uses a five-step process to²:

- develop a ranked list of mission critical operations and functions as well as associated infrastructure components,
- develop adversary courses of action with high value targets of interest,
- produce named areas of interests and observables (metrics) that would allow users to establish defenses outside the boundary controllers,
- identify survivability strategies and define minimum essential capabilities for redundancy, prioritized restoration and recovery planning,
- model and simulate survivability strategies against potential adversary high probability courses of actions and probable axis of attack based on identified defended network topology and configuration,
- identify and recommend electronic/cyberspace information sensor placement and a coverage matrix to provide indications and warning of

² The IPIB process description is available at the Zel Technologies IA web site (<http://projects.zeltech.com/ia>). Detailed description is omitted for brevity.

- possible adversary activities/cycles³ prior to delivery of the “packet of death”,
- provide information (indications and warning) that attacks are pending. This has the potential of moving adversary activities outside the enclave and into neutral areas where human interdiction and analysis can occur within human response times.

INTELLIGENCE PREPARATION OF THE INFORMATION BATTLESPACE

The IPIB process is modeled after the Automated Assistance with Intelligence Preparation of the Battlespace (A2IPB) Evolutionary Prototype systems. A2IPB is a joint kinetic warfare IPB automation system tailored for Theater Missile Defense. Zel Technologies is developing the A2IPB under Air Force sponsorship. We used the A2IPB effort as a guide for conceptual efforts in the domain transition to Cyberspace, as well as for reuse of compatible design and in some instance, code⁴. The Intelligence Preparation of the Battlefield (IPB) is derived from Army Field Manual 34-130⁵ and is described as systematic, continuous process of analyzing the threat and environment in a specific geographic area. It is designed to support military staff estimate and decisions making. Applying the IPB formal methods process helps a military commander selectively apply and maximize his combat power at critical points in time and space on the battlefield.

A key step in confirming the efficacy of the IPIB process and system is to conduct experiments that affirm or refute the central hypothesis, that the IPIB process improves the cyber defense process. Using the DARPA CC2 program’s Experiment Working Group process, we proposed and refined a series of experiments with respect to IPIB. The first, which is currently underway as this writing, is a “whiteboard” experiment whose main hypothesis is that the IPIB process helps improve network defense beyond security best practices. Sub hypotheses are that:

1. Detection mechanisms configured using the IPIB process improve detection capability beyond security best practices.
2. Prevention mechanism configured using the IPIBN process improves prevention capability beyond security best practices.
3. The IPIB process identified attack targets better than security best practices.
4. The IPIB process predicts enemy/adversary courses of actions better than best security practices.

³ Wood, Bradley and Schudel, Gregg “Modeling Behavior of the Cyber Terrorist”, pre-publication draft presented at various 1999 DARPA Workshops. This paper identifies an adversary cycle that leads to such a “packet of death”. This cycle consist of an Adversary Orient, Observe, Decide and Act (OODA) loop consisting of intelligence gathering, preparation, and development, live network discovery, test-practice-replan, attack and damage assessment processes.

⁴ Automated Assistance with IPB (A2IPB) Requirements and Design Documentation.

⁵ US Army Field Manual 34-130, “ Intelligence Preparation of the Battlefield”.

Three different friendly (Blue) teams will be used to develop network defense plans that include a static countermeasure configuration and defensive deployment plan (prevent mechanisms and IDS).

One Blue team consists of members familiar with the IPIB process with no experienced information security experts. This team will employ the IPIB process and a semiautomated IPIB prototype decision support tool to produce a likely Enemy Courses of Action (EnCOA), a list of network links and applications that are likely attack targets, a listing of critical/high value targets and its network defense plan. A second Blue team will consist solely of information security experts. This team will use computer and network security best practices to develop its network defense. Then, the two teams will merge to combine conventional best practices and the IPIB process and prepare an enhanced (we hope) defense plan. In parallel, an adversary (Red Team simulating a hostile nation state) will design and specify a series of Information Operations attacks intended to deny or disrupt activities.

An Assessment team will rank the probable success of each defense configuration on an attack-by-attack basis. The ranking scheme will compare the Blue Teams IA effectiveness using a numerical schema at the sub hypotheses level. The Assessment team will seek differences in each of the respective lists. If no difference exists, than the main hypotheses is refuted. If the Assessment team identifies differences in the respective network defenses then either a clear indication will exist or more experiments must be conducted to gather sufficient data to prove or refute the main hypothesis. Using three Blue teams will allow us to measure whether the structured IPIB analytical process can improve network defenses and survivability for poorly trained defenders, and whether it is useful for assisting security experts to develop better defenses than they would have normally done.

At the time of writing, the first phases of the experiment have been completed with significant differences identified between the Novice/IPIB Blue team and the Expert Blue Team. The Assessment teams scoring defensive measures against the Red Team attack results are to be completed shortly. Final experiment observations and conclusions will be available at the conference

This initial experiment did not permit implementation of a dynamic cyber plan extending the cyber defense playbock beyond a series of scripted plays against a static defense. We have proposed a series of experiments that will validate or refute our hypothesis of IPIB as tool in creating a cyber defense strategy and providing further evidence that the IPIB process is critical to defining and supporting systems survivability.