1. Background. Working in the DARPA Cyber Panel project and with Air Force Research Lab (AFRL/IFGB), Zel Technologies (ZelTech) developed a process called Intelligence Preparation of the Information Battlespace (IPIB). Based on the traditional Intelligence Preparation of the Battlespace (IPB) found in Army Field Manual 34-140 and Joint Publication 2-03.1, the IPIB process gives analysts the tools to conduct a structured, thorough intelligence preparation of cyberspace for planning and organizing computer network defense (CND). (Figure 1) IPIB assists with the production of intelligence estimates, assessments, and other products to support a Commander’s decision-making. It is a five-step cycle that helps a Commander know where to look, when to look, what to expect, and what to defend in cyberspace. ZelTech subsequently developed a software prototype to assist analysts in organizing and analyzing the massive amounts of information required to conduct CND. Our IPIB technology was recently selected by the Air Force for integration in their Information Warfare Planning Capability (IWPC) integrated tool set as a CND planning tool. We would be pleased to demo the software at DISCEX 3.

2. Discussion. The purpose of the IPIB software is to provide a solution to assist in the development of an overall strategic computer network defense plan for the organizations that utilize it. The IPIB process that the tool implements is a derivative of a key Army process called IPB, or Intelligence Preparation of the Battlespace, which provides the analyst with a structured methodology and set of tools to perform predictive intelligence for land warfare by analyzing the mission, enemy, terrain, available time, weather and other significant factors influencing the battlefield. It was ZelTech’s hypothesis that this process could be extended to the cyber world and used in the field of computer network defense (CND). We developed a 5 step continuous process, based on traditional IPB, which included the following steps:

1. Define the battlespace environment
2. Describe the battlespace effects
3. Evaluate the threat
4. Determine the threat’s potential courses of action (COAs)
5. Apply IPIB through a Cyber Defense Plan

These steps were then set to software to assist the analyst with determination of where to deploy traditional CND tools to properly protect, detect, and prevent attacks against the system, while still performing the mission. The IPIB team designed the tool in 2 phases. Phase 1, known as IPIB1, yielded a prototype to use in conjunction with the manual planning process of IPIB. The prototype attempted to implement all 5 steps in the IPIB process, which on paper still included traditional IPB tasks, via a software mechanism; however, in the development and testing of the prototype it was found that although certain tasks, ideas, and concepts from traditional IPB transitioned well to cyber defense, not all did. For instance, weather is not a factor in cyber IPB for computer network defense. We also tested the tool from a usability perspective to determine the best methods of entering and visualizing the IPB data. Phase 2, also known as IPIB2, was scoped to implement lessons learned in the initial prototyping. IPIB2 also added increased functionality. IPIB1 was built to test concepts but did not follow good, contemporary design philosophies and at the time we did not know the best way for visualizing data. For instance, our first try at Attack Trees was with a standard Java tree viewer. This proved to be slow and unwieldy when the trees got large and it was not easy for a user to view. IPIB2 has been built with use in mind and has a much better user interface for data entry and visualization, as well as a more robust underlying architecture. The system is dependent upon the Java 2 runtime, the Xerces XML processor, Openmap, JDAF, Oracle, and Amenaza's SecurITree™. IPIB2 implements a basic toolkit for defining the critical functions of a mission, the network and software elements that are required by the critical functions, and analysis of the raw data to gain information about what critical functions will be impacted if specific elements are attacked by an adversary, and predicting Enemy COAs in the form of Attack Trees. Future releases will assist in preparing a complete Cyber Defense Plan.

3. Point of Contact (POC): Dr. J. Ken Williams, (757) 722-5565, kwilliams@zeltech.com.