# Developing a Framework to Improve Critical Infrastructure Cybersecurity

Peregrine Technical Solutions LLC (Peregrine), is a small disadvantaged business, 8(a) and HBZ (#47857) certified, ANC, operating under a NAICS code of 541513, with its principal office located in Yorktown, VA. Founded by Dr. Leigh Armistead, CISSP, a former Information Operations (IO) master faculty at the Joint Forces Staff College, who wrote his dissertation on the use of cyber-attacks and defense strategies, we specialize in providing supporting for cyber offense/defense activities, including full-spectrum Information Assurance (IA), Cyber Warfare, and Security Engineering for Critical Infrastructure Protection (CIP).

## 1.0 Why is there no rhyme or reason to the IO Training and Education curricula?

When evaluating the sheer multitude of IO, IA and CIP courses by the United States government, one must realize that the major problem is that none of these courses has any standards or common learning objectives upon which to base their curriculum. These classes are normally based on different theories (service and agency), different skill levels of users (beginners to advanced), different ranks or grades of the audience (enlisted to flag/general officer), as well as different foci (strategic, operational, and tactical). Given these variables, it should not be surprising that there are over 70 such courses in existence today, taught by a variety of United States government organizations and commands, but which aren't integrated or standardized. For example, one cannot obtain IO training in one service and then serve in a joint organization without needing additional specialized training. Additionally, there are no common denominators or goals that translate well across the American armed forces with regard to IA training and educational requirements. These and other standardization issues have thwarted the United States government and academia in moving toward the development of curricula emphasizing the power of information in general and CIP in particular.

## 2.0 Can Lessons be learned from the Information Assurance Community?

| IO Education and Training Goals | Means |
|---|---|
| Delivery of training must be cheap and fast | Internet |
| Access must be worldwide and standard | Portal |
| Clear, concise, authoritative and readable | Textbook |
| Information Battlespace | COP |
| Planning Tool/Checklist | Excell App |
| Study Real World Operations | Case Studies |
| Common IO Definition/Language | Taxonomy |
| Change Perceptions and generate interest | Exercises |
| Parallel Play/Multiple Courses | Interfaces |
| Worldwide IO Game | Everquest? |
| Standard IO Training Material | CD-ROMs |
| Training must be standardized | Qualifications |
| Red Teaming must be incorporated | VA Teams |

During a daylong session in which British, American, and Australian academics and military officers met, at the 2nd Annual IO Conference hosted in Londona tremendous amount of energy

**Dr. Leigh Armistead, CISSP, President**
**Peregrine Technical Solutions LLC, www.gbpts.com**
**Cell (757) 581-9550, larmistead@gbpts.com**

and analysis was devoted to finding a solution to help develop better access to CIP training and education capabilities across the three nations. The figure above, is a synopsis of those efforts and reiterates what the participants of this project have been advocating for a long time, mainly that any curriculum developed must be based on open and accessible standards and that a web or internet based set of courseware was the best answer to deliver content globally. While this matrix is not the sole answer to the problem, it may help to act as a checklist or guide to focus the attention on possible solutions to these IO, IA and CIP education and training goals. However, there is still a gap between the large number of military-oriented courses and the study of this academic concentration by civilian universities.

## 3.0 Issues that still exist with developing commonality with respect to the IO, IA, and CIP Training and Education Situation

The dichotomy between increased emphasis by the American military on the conduct of IO, IA, and CIP *and* the lack of corresponding academic programs within academia is not unprecedented. Early work at National Information Assurance Training and Education Centre (NIATEC) to develop a set of standards eventually led to the National Institute of Standards publication 800-16 and the Committee for National Security Systems' (CNSS) series of publications. These standards, developed by the National Security Agency (NSA), are now widely recognized throughout the Department of Defense (DoD) and interagency as the de facto baseline of tasks for IA across the federal bureaucracy. In addition, the CNSS series has become widely used in academia, through NSA sponsored IA programs and curriculum. Together these groups are a hub of IA activity in which a tremendous amount of activity has occurred in the last decade, with an entire cadre of IA professionals having been trained and who now occupy key and influential positions within the federal government as a result of the education that they received from these programs. The key component of this success has proven to be the development of the CNSS standards, which are grouped into six categories (4011 to 4016). Updated on a regular basis, these standards serve as a basis for all the certifications and academic programs sponsored by the NSA and NIATEC Program as well as the IA academic community in general.

If the problem of developing standards and an academic interest in improving critical infrastructure cybersecurity and CIP are to be solved, several steps are required. They can be modeled on the process originally recommended for the IA discipline. The first step is to build personnel capacity, for if critical infrastructure is to become a civilian academic field, one must have sufficient faculty. The main problem is that very few college professors are trained in the United States; plus, currently, the computer science, IA, or information systems programs would be unable to adequately to the increased demand for critical infrastructure cybersecurity courses. For the long-term, it will be necessary to increase faculty in all areas of information technology: IA, IO, and current CIP practitioners should be encouraged to enter the professoriate by creating academic positions for professionally qualified individuals. In the United States, there are currently no comprehensive critical infrastructure curricula or graduate programs in academia. Nascent master's curriculums are underway, but more institutes and programs are needed to help close this gap, if significant progress is to be made. Likewise, the role of industry also cannot be overlooked in making faculty retention and development easier for this initiative, and it is imperative to attract quality students to programs producing CIP specialists. As demonstrated in

various IA initiatives, an undergraduate scholarship program has the largest potential influence to solve the short-term problem. In the absence of some form of graduate stipend program, there will probably still continue to be a dearth of individuals to become the next generation professoriate and to fill governmental and industrial needs. Production of master's and doctoral students is also essential, because traditional undergraduate and graduate programs alone cannot meet the need for IO professionals, and any comprehensive solution must include ongoing professional education for the existing workforce.

## 4.0 Develop a Comprehensive Standards Effort with respect to CIP Training and Education

Based on multiple discussions at a series of IO conferences (International Conference on Information Warfare), numerous delegates have suggested the establishment of a CIP Standards Working Group to conduct the following activities:

- Create a CIP Standards Working Group manifesto;
- Foster relationships between Industry, the Federal government, professional engineering organizations, and other defense agencies;
- Coordinate a series of CIP Standards workshops;
- Develop and publish CIP standards to improve critical infrastructure cybersecurity.

Specifically after a recent International Conference on Information Warfare that was held in the Naval Post-Graduate School in Monterey, California, the following deficiencies in CIP were identified:

- Critical Infrastructure is a field that has no current standards;
- The stakeholders of CIP are not just nation states and military groups anymore, but commercial organizations as well., as was pointed out as over 15 years ago in PDD-63;
- Critical Infrastructure is a cross-disciplinary field that brings together specialists in engineering, information technology, and cyber security;
- the aforementioned parties need to be able to cooperate and collaborate in order to produce standards and define the proper roles to protect CIP.

The first step to address these issues is the creation of a virtual community, which could bring together the members of the working group to identify and to produce a course of action. It is suggested that this steering group would utilize a web site, creating a series of mailing lists and using existing scientific conferences for disseminating results. The steering committee of the proposed CIP Working Group would be expected to promote the principles of critical infrastructure to identify and establish relationships with stakeholders: academia, professional bodies, the corporate world, the military forces, other defense agencies, and law enforcement. This involves organizing a series of meetings, organizing workshops, and disseminating results following traditional publication approaches. The second milestone would be the development of the group's manifesto. The future actions of the Group would be dictated by the manifesto. The group will develop a collaborative set of critical infrastructure standards that would be disseminated via journal papers, conferences, workshops and press-releases. It is hoped that the establishment of this CIP Standards Working Group would greatly improve the capabilities of a set of critical infrastructure standards, especially across the United States and its federal bureaucracy.

Developing standards alone will not meet all of the needs for CIP training, and there is no fast and simple solution. By encouraging and increasing the capacity of current programs, there would be an immediate, small increase in flow created by accelerating the progress of students currently in the programs. At present, the production has been increased to a few hundred a year. Experience with the IA scholarship program indicates that de novo programs take as long as 4 - 5 years to produce the first individuals with baccalaureate degrees focusing on information operations. To produce individuals at the master's level takes an additional year and a half, and an additional 2 - 3 years are required to produce a PhD. The foregoing discussion provides investment solutions that initiate and rapidly build an educational critical infrastructure capacity for the long-term national interest. It involves

- Investing in undergraduate/graduate students to encourage them to enter the profession;
- Providing incentives for current faculty to keep them in academia;
- Converting faculty to support IO initiatives;
- Encouraging research to maintain the state of the art and advance the profession;
- Aiding in the development of CIP as a recognized discipline in conjunction with IA; and
- Assisting faculty in professional development and publication of research results.

The following nine-point program would establish an integrated academic methodology to provide the education and training required to support the use of CIP to protect the elements of the critical national information infrastructure. Specific actions proposed include:

- Create a scholarship program to encourage both undergraduate and graduate students to enter the profession;
- Add distinguished professorships and associated stipends to encourage faculty both to join and to remain in the academic ranks;
- Create joint research opportunities with government;
- Find ways to maintain currency of teaching and research facilities;
- Encourage government, industry, and academic personnel interchanges;
- Foster joint academic-industry research consortia to address current needs;
- Create a CIP training program to increase the number of faculty teaching and researching in the area;
- Create joint education and training programs to keep current practitioners current; and
- Encourage the creation of innovative research outlets for faculty

The point of this push to upgrade the critical infrastructure training and education curricula is to help attract qualified personnel and students to the profession, with the development of a sufficiently large and well-informed faculty to guide education, training, and research programs for these personnel and students. In addition, improved infrastructure is needed to support such programs, as well as strengthening ties between industry, government, and academia through joint education, training, and research initiatives and opportunities. Finally as has been emphasized in Estonia and Georgia recently, the use of Cyber Warfare tactics are becoming more prevalent. Training and education in IA and IO capabilities, with the development of appropriate standards, could also help to alleviate some of these risks and vulnerabilities.