Proceedings of the 12th Colloquium for Information Systems Security Education
University of Texas, Dallas
Dallas, TX June 2 - 4, 2008

Developing Standards for IO Using CNSS as a Model

Abstract – The Information Assurance community has long benefitted from the development of standards as part of the CNSS process. This paper summarizes efforts conducted over the last year to start a similar standards based methodology for Information Operations (IO) and to develop a framework for IO training and education.

Index terms – Standards, Information Operations

I. Introduction

Information Operations (IO) is defined as the integrated employment of the core capabilities of electronic warfare, computer network operations, psychological operations, military deception and operations security, in concert with specified supporting and related capabilities, to influence, disrupt, corrupt or usurp adversarial human and automated decision making while protecting our own. As a relative newly defined activity, this publication proposed to revolutionise the manner in which warfare, diplomacy, business and a number of other areas are conducted. Information is and always has been a somewhat a nebulous term, but in this new era it possesses a capability that is now considered crucial to the success of American national security. However there are still many questions about the best method in which to most successfully utilise this element of power to the best extent by the United States government. Because IO crosses so many boundaries within the interagency processes, it is often very difficult to quantify exactly what constitutes an information campaign. Training and education in IO topics and areas are considered crucial to this warfare areas success, yet discussions at a recent International Conference on IO and Information Warfare held in the Naval Post-Graduate School in Monterey California in March 2007 identified the following gaps in that need to be addressed:

- Information Operations is a field that has no current standards.
- As a result of recent technological developments, the stakeholders of the Information Operations are not just nation states and military groups any more, but also commercial and governmental organizations that are members of the Critical National Infrastructure of a nation and of that nation's allies.
- Information Operations is a cross disciplinary set of practices that bring together specialists in computer science, sociology, psychology, communications international relations and military science.
- There is a need for the stakeholders and their international partners to be able to cooperate and collaborate for producing standards and defining the practice and science of IO.

This discussion was based on the widely perceived need for a coherent set of IO Standards that are recognized across the interagency and coalition organisations. One of the reasons for this concern, and the basis of why the need for standards are so important, is that one must understand that there are many different IO or IO related courses in existence today, most of which are unrelated and uncoordinated. Most of these courses are stovepipe or standalone entities, which do not entitle the student to any commonly recognized qualification. This problem has evolved because there are no recognized IO standards today, which is a crucial step to the recognition of any education or academic curricula. This is because standards provide credence or relevance to a course or area of study. Examples of existing successful similar standards include the National Security Agency (NSA) Committee for National Security Standards (CNSS) 4011-4016 series in Information Assurance (IA), which are recognized across not only the Department of Defense (DoD) but United States government as well. These CNSS standards were developed as part of a methodology utilised through the National Information Assurance Training and Education Center (NIATEC) in conjunction with NSA and CNSS, to conduct a series of workshops entitled electronic Develop a Curriculum (eDACUM), to bring together IA experts from across the DoD, federal government, academia and private industry, to build these aforementioned IA standards. The same process is proposed to build a set of recognized IO standards.

II. The Development of IO Standards

Therefore, as a result of these discussions, it was decided to establish a working group with academic, military and

commercial industry members from a number of participating countries (United States, United Kingdom, Finland and Australia) to coordinate the stakeholders in this new organization and to help develop a set of requirements for the proposed group as shown below. Specifically it is desired that the IO Standards Working Group (IOSWG) will conduct the following activities:

- Creation of a statement of Goals, Motivation, Mission and Vision for the IO Standards Working Group
- Creation of relationships with the Police, the Military, professional bodies, other defense agencies, and the corporate world, in the participating countries
- Coordination of a series of International Information Operations Standards workshops
- Development and publication of a set of international standards for Information Operations

The IOSWG's goal is the creation of a virtual community bringing together the members of the working group for identifying and producing a course of action. This will involve the use of a web site, creation of mailing lists, and the use of existing scientific conferences for disseminating results. The steering committee of the Information Operations Working Group will be expected to promote the principles of Information Operations in their respective countries and to identify and establish relationships with stakeholders: the 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. At this stage, we expect that one annual workshop will be adequate.

This first milestone in the creation of a virtual community will as hoped, serve to bring together the members of the working group for identifying and producing a course of action. This will involve the use of a web site, creation of mailing lists, and the use of existing scientific conferences for disseminating results. There are three international scientific conferences that examine specifically IO and Information Warfare, and these venues will be important time periods where the IOSWG will update the community on its progress:

- International Conference in Information Warfare
- European Conference in Information Warfare
- Australian Conference in Information Warfare

Members of the IOSWG would be expected to attend these conferences, and furthermore, the steering committee of this effort will be expected to promote the principles of IO in their respective countries and to identify and establish relationships with stakeholders: the academia, professional bodies, the corporate world, the military forces, other defense agencies, and the police. This involves organizing a series of meetings, organizing workshops and disseminating results following traditional publication approaches. At this stage, it is considered that one annual workshop will be adequate.

The second step is the development of the group's public statement of its goals, intentions, and vision of International IO standards. Once the steering committee of the Information Operations Standards Working Group is established, it will produce a statement of its Goals, Mission and Vision, which will guide the future actions of the Group. The Group goal is to develop a collaborative set of Information Operations standards that will be disseminated to the public via journal papers, conferences, workshops and press releases.

The third step is the creation of relationships with the European Network & Information Security Agency, the United States Department of Defense, the United Kingdom and Finnish Ministry of Defence and the Research Network for a Secure Australia.

Ultimately, the main outcome is the creation and release of International Information Operations standards, possibly as two sets, one for military operations and one for the public. The establishment of an IO Standards Working Group is expected to greatly improve the capabilities to produce a coherent set of IO standards, especially across the United States and its federal bureaucracy.

III. Modeling International IO Practices

The lack of standardization in the IO training environment has hampered efforts to develop interagency and coalition support. The liaison proposed as part of this effort will provide assistance and insight into the accomplishments to the disparate organizations involved in this effort. The key will be to utilize a well-recognized standards development approach such as led by the National Security Agency (NSA) through its National IA Training and Education Center (NIATEC). The latter is well recognized throughout the United States government as a leader in standardization efforts in the information assurance. The desire is to translate this expertise in standardization methodology over to the IO community, through a series of workshops involving key joint IO organizations such as the Joint Forces Staff College, Joint IO Warfare Center, National Defense University, The Joint Staff and academia. The IOSWG personnel will work alongside NIATEC in the administration of these workshops by coordinating with federal personnel with

experience in IA standardization efforts. Specifically the IOSWG will gather all existing IO standards from disparate databases, to build a base level of information for the working groups. The process for the development of standards has already been set by NSA, and this methodology could be followed here as well. The outcome after a number of working groups would be to build a broad IO Standard, with an apprentice, journeyman and master subsets and specific smaller standards for the unique capabilities such as Deception, Psyop, etc. Figure 1 shows an example of IO Standards and Training Levels.

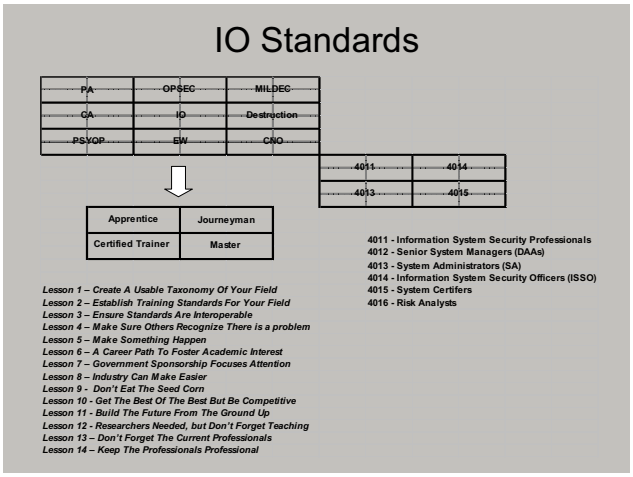

Figure 1. IO Standards and Levels of IO Training

A key step will be to create a Model of IO as practiced by trusted international partners against their enemies. Achieving a good model of IO requires seeing IO both as extension of the IA model and a supportive subset of Irregular Warfare operating concepts. The USG and its allies are increasingly engaged in Irregular Warfare.

An IO model is in some ways analogous to the model of IA used in recently completed IA standards. The IA Model used is extended from earlier definitions of Information Security (INFOSEC). It therefore has a mainly defensive focus on data/information. The model of IA has four dimensions:

- Information Characteristics to be maintained: Availability, Integrity and Confidentially
- Information State: Storage, Transmission and Processing
- Security countermeasures applied: Technology, Policy -Practice, and training-education.
- Time, which allows technology to evolve, processing to produce new information, training to take hold, policies to change, etc.

The dimensions of an IO Model are less orthogonal than the IA dimensions. Relationships of Situation, IO components to use and expectations are more important and not a linear list necessarily.

- Information and Knowledge Characteristics to be maintained: Availability, Integrity and Confidentially, privacy, non-repudiation, plus situational relevancy
- Information and Knowledge State: Storage, Transmission and Processing, plus *Situational* Accuracy, reliability, timeliness, relevancy, consistency.
- Security-Defensive Countermeasures: Technology, Policy -Practice, and training-education, *Situational* IO component set for Defense.
- Offensive Measures: : Technology, Policy - Practice, and training-education, past & current expected relevancy, reliability and effectiveness, expected relevancy, reliability and effectiveness, *Situational* IO set for Offense
- Management and Integration: "Jointness", USG components Support sources,
- Information Operation application Set: IA, OPSEC, Military Deception, Electronic Warfare, PSYOPS, Civil Affairs, Public Affairs, CNA/CNO, Military Destruction of IO related cites,
- Situation where Applicable- *Situational* IO set to use,
- Time, which allows Situation and technology to evolve, processing to produce new information-knowledge, training to take hold, policies to change, etc.

An IO model must account for the scope of IO as an offensive and defensive set of information operations, of which IA is only one basic component. Most importantly, the model must include actions and views of both (all) sides of a conflict, the military and the adversary, partners etc. The fully symmetry model of IO is captured by the "new adage" with apologies to Sun Tzu: "Know your enemy and yourself well" AND "influence your enemy to NOT know you or himself well". "Knowing" includes knowing current facts and also expected outcomes based on past and current information and knowledge.

The intent of IO is therefore to produce joint plans and actions focused on two sets of knowledge or perceptions. Each set has both offensive and defensive activities. One set informs the combatant commander and his IO Planners about their own and the adversary's situation - with the goal of acting to plan and execute a successful mission. The other set projects information and actions onto the adversary, with the goal of producing a perception that leads the adversary to behavior in the interests of the military's mission and contrary to the

adversary's own goals. The adversary will take the reverse point of view in his own IO.

IO also extends the defensive focus of IA. The definition of IO, as stated in the IO Roadmap is as follows: *'The integrated employment of the core capabilities of electronic warfare [EW], computer network operations [CNO], psychological operations [PSYOP], military deception, and operations security [OPSEC], with specified supporting and related capabilities to influence, disrupt, corrupt, or usurp adversarial human and automated decision-making while protecting our own.'* (*DoD IO Roadmap*, 30 October 2003)

As seen in this definition, the practice of IO therefore supports both defensive and offensive actions. IO practices must model the enemy (and the enemies partners') offense and defense capabilities and status as well as its own capabilities and status and those of its own allies. However, IO is itself a critical component in conducting Irregular Warfare. In support of Irregular Warfare, the scope of IO and hence the international standards for IO practice are considerably widened. IO and its standards must address the task of modeling all actors, allies as well as enemies, aligned partners and nonaligned organizations, stakeholders as well as non-governmental organizations too.

Irregular Warfare is another important concept in the modeling of IO and it is defined as "*... a violent struggle among state and nonstate actors for legitimacy and influence over the relevant populations. IW favors indirect and asymmetric approaches, through it may employ the full range of military and other capabilities, in order t erode and adversary's power, influence and will. It is inherently a protracted struggle that will test the resolve of our Nation and our strategic partners. "(Irregular Warfare (IW) Joint Operating Concept (JOC) Version 1.0, 11 September 2007)*

This document goes on to say that "Influencing foreign governments and populations is a complex and inherently political activity", that "Irregular Warfare is about people, not platforms." and that "Waging protracted irregular warfare depends on building global capability and capacity." These aspects of Irregular Warfare make for a significantly more complex support task for IO and hence even more the need for the development of common methodologies and processes in the conduct of IO across the federal and military communities.

IV. Developing IO Standards

As in any development project, there are many phases including Analysis – Design – Development – Implementation and Maintenance that must be met as part of an evaluation and approval gates associated with the ultimate approval and forward movement, as shown below:

- The authority requiring the standards and who approves the standard produced.
- The stakeholders and partners who participate and collaborate to produce the standards
- The Process of Standardization
- Theory, methods, and tools/facilities used to promote collaborative building of the standards
- The content of the Standards produced
- Form and format of the standards
- The maintenance of the standards once produced
- The policies necessary to manage and track application of the standards by users and agencies.

As part of this proposal, we suggest two phases to develop a model for IO, to address the need for International IO collaboration and produce a set of coherent and enterprise-wide IO Standards.

Utilize current International conferences to present IO Standard Tracks which gather and review needed information on necessary IO Standards and training. Utilize the existing facilities and methods of NIATAC and eDACUM to refine, produce and maintain the final IO standards and Training requirements.

For the first phase, the IOWSG proposes using the three main IO and information warfare academic conferences as the best way to gain widespread insights into current practices of IO internationally. Specifically, at these venues, tracks should be set up to develop an ontology and knowledge base of IO, which would entail the gathering of data surrounding current usage of IO in operations and mission around the globe. The following items are basic ingredients for producing a taxonomy, ontology and knowledge base of IO:

- A clear definition of what IO is and how it works. The intent here is to obtain the clearest current ideas around what IO and its practice are currently and what the shortcomings are in the view of an international set of practitioners.
- A glossary of IO, Information Assurance, Information Warfare, Irregular Warfare and other terms. These should be further sorted by user and source of the terms.
- A mind map of important things of all sorts related to IO and how they are related in multiple ways. The graphical view of the mind map, showing the relevant items connected to items they relate to lends itself to a discussion of the items, relationships and connections in the mind map. This will further indicate a variety of

additional relationships among the components and practices of IO. i.e. methods, processes, who uses them, what they entail, how they relate to action states- offense, defense, collaboration, C&A, trust, what function they support, what function they depend on etc.
- A components breakdown of IO things (i.e. something is a part of or something is contained by another function, operation, organization),
- A mental model of how IO is used, who uses it, where appropriate, include all stakeholders and players, whom it is used against, who or what is protected, information, data and knowledge common among these players.
- Assumptions about all of the above material are very important to explicitly state. Mistaken assumptions are always a major source of error in modeling as well as analysis.

The combination of ontology and a parts hierarchy will be very helpful in capturing the elements of IO, which will be included into an IO knowledge base. .An ontology differs from taxonomy, in that a taxonomy is a tree or hierarchy of kinds of things. It shows a breakdown of general to more particular class. Taxonomy is also a hierarchy of classifications. If one must pick only one classification hierarchy, there will be differences in opinion of the best one. Ontology on the other hand, is a hierarchy of what you know and understand about a subject. An ontology of IO will explicitly contain all kinds of relevant IO things, relationships of all kinds, sets of all kinds, sets of particular instances of IO kinds of things. The ontology can therefore be very important, because it will contain the elements of many points of view about IO.

A knowledge base is a web of relationships among the items in the ontology. The web of relevant IO items and how they are specifically related defines the IO knowledge about those items. The structure of IO knowledge or knowledge about anything really, is more complex than that of a relational database for example. Knowledge has sometimes been erroneously called "unstructured" by database practitioners. This is not true but the structure of IO knowledge will be complex in comparison to relational databases. As part of this effort, a portal should be developed to allow the use of a web service that academics could use to access the web of knowledge and get answers based on it.

The second step further analyzes and refines the IO information collected earlier using the NIATAC facilities and eDACUM methodologies. One important goal of this phase is to reduce the knowledge about IO practice to a well-defined and understandable form that can be translated into actionable standards statements. The simplified steps are:

- Start with refining the information previously identified in the first phase. Address the essential IO capabilities and related core competencies desired for IO Planners, Knowledge Skills and Attributes (KSA) needed for competency are developed for IO tasks.
- Knowledge – the broad comprehension of IO needed,
- Skills – comprehension of IO that is /can be specifically applied to an IO task and
- Attributes (Abilities) – the personal characteristics that can be developed or enhanced. E.G. IO job performance will be based on these.
- KSAs for IO will correspond to the hierarchy of IO jobs and tasks.
- Performance required for each IO task is identified and the conditions, desired actions and criterion for standard behavior are determined.

The resulting Job/task Analysis is further refined using a taxonomy of specially selected verbs (Blooms taxonomy) related to Knowledge, Performance and attitudes/feelings. This is used as a foundation to writing the IO standards document. Interdependencies of the component IO capabilities will also be factored in.

It is proposed that the NIATEC facilities at Idaho State University be utilized for collaboration to facilitate the process of developing IO standards in:

- Capturing and refining all ideas, mind maps
- Gaining agreement
- Capturing, documenting and producing the document

The resulting documented standard describes a framework for a standard course of IO. Validation and Approval is carried out in successive eDACUM sessions. eDACUM is an electronic method of involvement and consensus building to determine training needs as identified by skilled workers and professionals. It is a joint NSA and Idaho State University (ISU) venture for producing Training Standards.

V. CONCLUSION

To summarize, there is a significant requirement for both national and international IO standards. The prevalence of technology supporting asymmetric warfare, the lack of existing IO standards , the need to work efficiently with international partners and the transition to waging Irregular Warfare all point to this requirement.

We propose that an IO Standards Working Group (IOSWG) be formed to guide the development of International IO Standards. There will be a three-pronged attack on producing the missing IO Standards and addressing the need for International IO collaboration.
Form an International IO Standards Working Group (IOSWG) and manage International IO Standards development via the working group.
Utilize current International conferences to present IO Standard Tracks which gather and review needed information on necessary IO Standards and training.
Utilize the existing facilities and methods of NIATAC and eDACUM to refine, produce and maintain the final IO standards and Training requirements.

We propose that the steering committee of the IOSWG meet on a quarterly basis to decide on guiding actions for the Group, collaborating, exchanging research findings and evaluating feedback from disseminated results. Twelve two-day meetings are proposed throughout the 3-year duration of the project. An annual workshop is proposed for disseminating the research findings. The first workshop will disseminate the Goals, Vision and Mission Statement of the IOSWG. The other two annual meetings will disseminate the drafts and the final versions of the Information Operations standards. Other activities involve:

- The use of a Web portal that will help the participants to form a virtual community.
- The publication of a series of journal papers
- A series of press releases

In conclusion, the CNSS has been very successful over the last 15 years in developing standards for IA training and education efforts. The goal of the IOSWG, will be to continue that tradition and apply the processes and methodology to the IO arena. It is hoped that the establishment of a standard set of ontologies and taxonomies to this warfare area, will allow it to normalize in much the same manner as IA has done.

VI. References

[1] *DoD IO Roadmap*, 30 October 2003.

[2] *Irregular Warfare (IW) Joint Operating Concept (JOC) Version 1.0,* 11 September 2007.

[3] *Joint Publication 3-13 Information Operations (13 February 2006*