Creating a Common Body of Knowledge (CBK) for Information Assurance and Security Academic Programs and Certificates

ICETI 2012

Alfredo CRUZ, PhD
Graduate School, Polytechnic University of Puerto Rico
Hato Rey, Puerto Rico
and
Sandra BONILLA, MS CS
Graduate Student, Polytechnic University of Puerto Rico
Hato Rey, Puerto Rico

ABSTRACT

Information Assurance (IA) is a field that is rapidly evolving in the information technology (IT) scenario. The urgent need for information security professionals has brought together industry, government, and academic sectors, to define the requirements for information assurance and security education. Developing core courses for graduate and undergraduate IA programs with a Common Body of Knowledge (CBK) in Information Assurance and Security is critical for new and practicing IT security professionals, including technical and managerial personnel. The CBK maps courses to information security elements required in industry, government, and academia. Standards are currently regulated by the CISSP domains, National Security Telecommunications Information Systems Security Institution (NSTISSI) standards, and the NIST. The authors from Polytechnic University of Puerto Rico use their experience in obtaining the CNSS IA course certification and the CAE/IAE designation, to obtain the criteria needed to develop a graduate program in information assurance. A research instrument (questionnaire) was applied to a randomly selected group of industry IT professionals to reveal their needs, opinions, and preferences on the specialization areas suggested for the program. A group of randomly selected graduate and undergraduate students from related areas was also surveyed. There is a need to match the resources needed in the area of information assurance and security at local and federal government and industries, with the knowledge and skills that are delivered to students in related areas of study.

Key Words: Common Body of Knowledge (CBK), Information Assurance (IA), CAE/IAE designation, NSTISSI standards, CISSP domains, NIST, Model IA curriculum.

I. Introduction

Since the 90’s the need for security professionals has become critical, bringing together industry, government, and academic sectors, to define current and upcoming requirements for information assurance and security education at the undergraduate and graduate level, and certificates. Information Assurance is a new field that is rapidly evolving in the information systems and technology fields.

The development of core courses with a Common Body of Knowledge (CBK) in Information Assurance and Security (IAS) is needed to create a model curriculum for a Master Degree (MS IAS) that is: crucial for practicing IT professionals in information assurance; provides students with professional skills and knowledge to excel in their professions; and provides stakeholders with a clear and concise accounting of the knowledge and skills to be learned. The CBK is based on the mapping of the courses to the information security elements that are required to fulfill the needs of: the industry, government, academia, CISSP domains, National Security Telecommunications Information Systems Security Institution (NSTISSI) standards, and the NIST. Since IA is a constantly changing field, reviewing these standards in the industry and government and applying the required changes to a CBK is imperative. The role that each course has in each of the IA knowledge areas needs to be mapped to industry and government needs (elements). Specialization areas need to be created in the programs that focus students knowledge and skills in specific areas of IA that are in great demand.

The courses should combine what the industry is looking for in an employee and the learning interests of students in this area. Surveys will be done to students and IA professionals to create a CBK that will reflect the needs of the public and private sectors in this area.

Finding a CBK will lead to more effective academic programs and certifications in IA. This will contribute to increase significantly the number of competent IA faculty in academia, and IA professionals in the government and industries. It will also contribute to increase significantly the number of institutions with CAE/IAE and COE designations for the benefit of our Nation’s security infrastructure, and national security organizations such as the NSA and the DHS.

II. Information Assurance Educational Background

In the early days, experts in the security area had military backgrounds, because the military had the technology, needs, and also the funding for the development of new technologies in the security area [1]. Military standards define numerous security disciplines, including computer security, information security, communications security, physical security, personnel security, operations security, and others, that are interrelated, but differently focused [2]. Activities like: employee awareness, operating procedures, social engineering, and system recovery, enable organizations to function in a secure manner, and need a comprehensive term to identify them. As an all-encompassing concept that covers all (safeguarding) aspects of securing information and technology, Information Assurance includes classified and non-classified systems, software, hardware,
human resources, and the procedures to keep the information systems available and accurate [3].

III. Justification

Information security and information assurance fields are related and share the common goal of protecting the confidentiality, integrity and availability of information and intellectual assets. Information Security means protecting information and information systems from unauthorized access, use, modifications, damage and disruption [4]. Information Assurance (IA) is a term that covers the activities needed to assure the confidentiality, integrity, availability, and authentication; protecting and defending information and information systems. These measures include the restoration of affected information systems by incorporating protection, detection and reaction capabilities [5]. Information needs to be reliable, accurate, available at the appropriate time and verifiable as having come from a legitimate source, in order to serve the needs of the organization. Information assurance is an encompassing term, which includes hardware, software, classified and non-classified systems, human resources, and the procedures needed to keep the information in computer systems available, reliable and accurate [3].

The protection of information assets and the continuous advances in information security, pose significant challenges for academia, industry and the government sectors [6]. To address this need the President of the United States issued Presidential Decision Directive (PDD63), a Policy on Critical Infrastructure Protection, which prompted the NSA to established outreach programs like the designation as a Center of Academic Excellence in Information Assurance Education (CAE/IAE). The growing awareness for the need to protect information assets has led to a demand for Information Assurance training and education.

Actually there is no standardized curriculum to teach Information Assurance in institutions of higher education in programs such as Computer Science or Computer Information Systems. Although Information Assurance educators have been looking closely at the best way to deliver the needed expertise, the only recommendation that currently exits is a draft that resulted from a workshop sponsored by the National Science Foundation (NSF) and the American Association of Community Colleges [7].

There are two dominant technology curriculum guidelines currently in use:


2) IS 2002 Model Curriculum Guidelines for Undergraduate Degree Programs in Information Systems, co-sponsored by: Association for Computing Machinery (ACM), Association for Information Systems (AIS) and Association for Information Technology Professionals (AITP) [8].

One major problem is that established curriculum bodies like the ACM, ABET and IEEE do not have a formal or effective standardized information security curricula model developed [9]. Furthermore, different questions arise about which and what subjects should be covered in an Information Assurance program for a graduate track level. Information Assurance is a field that has not matured sufficiently to develop processes associated with performing specific information security job tasks [10].

The main goal of universities that educate students in IT and information security are to prepare them to recognize and combat information system threats and vulnerabilities that could weaken the infrastructure of the nation [11]. The designation as Center of Academic Excellence in Information Assurance Education (CAE/IAE) is an asset for any university and is preceded by the CNSS course certification, where courses are evaluated through a mapping of specific required elements that apply to each course that has IA related topics.

The goals of this paper are to disseminate the experiences encountered while developing the following activities:

1) Acquiring the Information Assurance courseware certification from the CNSS for standards 4011 and 4013E for the Polytechnic University of Puerto Rico by doing the course mapping to understand the elements evaluated in Information Assurance education and which courses contain them.

2) Obtaining the DHS, NSA designation as a Center of Academic Excellence in Information Assurance Education for Polytechnic University of Puerto Rico by complying with the required criteria for designation.

3) Using these experiences to develop specialization areas and core courses for the design of IA programs and certifications.

4) Identifying the Common Body of Knowledge areas considered important for practicing information assurance professionals to provide students with the professional skills and know-how they require to excel in their professions.

5) Providing stakeholders with a clear and concise accounting of the knowledge and skills that need to be learned.

6) Preparing professionals in computer and information security areas, which are of great demand worldwide, by understanding the overall interests and needs of the industry in the information security specialization areas.

IV. Relevance and Significance

In the past ten years due to world events and federal initiatives, Information Assurance has been a field that has grown rapidly. The need for knowledge and skills in Information Assurance has increased parallel to the needs in industry, government and academia [12]. When important assets of the organization (databases, networking, web applications and classified information of the computers) are attacked, damaged or threatened business operations can be damaged or interrupted; confidentiality and data integrity can be compromised. Bishop [13] identified the need for a standard curriculum in Information Security in two of his articles presented in the National Colloquium of Information System Security; and how these could be applied in the academia in an undergraduate, graduate, and doctoral level. In another presentation, Bishop [14] stated that at the undergraduate level, the curriculum should be focused on the application of the principles of computer security. If students want a deeper understanding and knowledge of the principles they would need to continue graduate studies or study on their own. However, graduate students will be more focused on the design and specifications
to secure the systems, than on the implementation of these designs.

Kim and Choi [15] stated that in the development of an Information Security curriculum, experts in the field should determine the educational requirements for Information Security professionals. Since a formal definition of the basic principles of information security did not exist, this lack contributed to an unstructured approach to information security [16].

Standards for Information Assurance education, curriculum materials, and the process of completing the requirements for the National Center of Academic Excellence in Information Assurance and Education (CAE/IAE) have been developed by NIETP (National IA Education and Training Program). In 1999 there were seven Centers designated, the number increased to 50 in 2003, 66 in 2005, and currently there are more than 94 Centers, including the Polytechnic University of Puerto Rico (PUPR); which is one of the very few HSI’s with the designation, and the only in Puerto Rico.

During the efforts of accrediting Information Technology as an academic discipline (a model curriculum), representatives of the ACM, IEEE, ABET and SIGITE stated that one of the major challenges was acquiring knowledge in the area of security. However the IT2005 Model Curriculum [17] presents Information Assurance and security as a core for any student in an Information Technology program, considering that knowledge in the area has risen sharply in importance in recent years [18].

Today, Information Assurance educators in areas like academia, government and industry are looking closely at the best way to deliver the needed expertise, success and improvements in the information assurance field.

V. Research on Information Assurance Education

The development of a model curriculum in Information Assurance would directly benefit academia, industry, and government agencies. By supporting formal educational efforts, the academia emphasizes on the principles that underlie computer security and information assurance. The industry focuses upon applying information assurance and security to their infrastructure and proprietary information, and the government uses computer security to protect the national interest [19].

Several universities have developed programs focused on Information Assurance curricula for undergraduate levels. Programs in universities like Purdue University have resulted from collaboration and sharing among early Information Assurance educators in forums such as the Colloquium for Information Systems Security Education and governments grants, that are crucial to Information Assurance program development [20].

Mattord and Whitman [21] explain five approaches that should be analyzed and considered before developing an Information Assurance curriculum. Available resources, time, technology, faculty, money, and student demand, are elements that need to be considered before developing any of the following approaches:

1) Security elements added to existing courses
2) Security elements added to a capstone course or courses
3) Independent information security

4) Information security certificates/minors –
5) Information security degree programs: There are three types of information security programs:
   o Managerial Information Security – This program is not mainly focused on technical aspects and skills. It is based more on the administration and management of information security.
   o Technical Information Security – This program covers the technical aspects and is one of the most popular and common IS programs.
   o Balanced Information Security Program - A balanced program combines technical and managerial aspects into one program.

VI. Current Advancements in Information Assurance Education at PUPR

In the last three years more than 150 graduate and undergraduate students have enrolled in Computer Forensics and Ethical Hacking courses. Actually, PUPR is the only academic institution in Puerto Rico to offer some these courses. Recently, certifications have also become very important for IT professionals as the need to up-date their knowledge and skills is constantly required.

PUPR currently has a Master in Science in Computer Science (MS CS-thesis option) and a Master in Computer Science (MCS-non-thesis option). These Master Degrees are the first in Puerto Rico, and have a specialization in Information Technology Management and Information Assurance (ITMIA).

In 2010 the Graduate School introduced a Graduate Certificate in Information Assurance and Security (GCIAS) [22] to highlight the ITMIA specialization as well as to prepare other Information Technology, Computer Engineers, and Information System professionals who are working in the development or maintenance of information and computer security systems or products, such as graduate engineers, scientists, or managers in related fields. This certificate helps these professionals develop a secure cyberspace and information structure nationwide. It prepares the student and professional with IAS skills that are already of great demand in today’s fast paced, high-tech, competitive work areas.

In the feasibility study to develop the GCIAS a sample of students from related fields of study at PUPR were asked if they consider information assurance and security an important IT issue. A total of 95 percent of the sample answered yes. A total of 97.25 percent of students also considered that obtaining additional skills in IAS would help them excel in their professional careers, and 78.75 percent answered that they are willing to enroll in the GCIAS to acquire additional skills in IAS. This gave us a very positive feedback from students currently studying in related areas at PUPR.

Students can obtain the GCIAS while studying the ITMIA specialization without the need for additional courses.

The GCIAS provides students with theoretical components and hands-on-practice in a curriculum that is specially designed to cover the managerial and technical aspects of IAS. The certification is composed of 6 key courses (18 credits) in information assurance and security topics: Two current graduate courses of 3 credits each that are highly recommended electives for the ITMIA specialization in the MS CS and MCS programs. These courses are: 1) EE 6130: Data Communication Networks;
2) CECS 7570: Computer Security. Four new graduate courses of 3 credits were created for the GCIAS, which also serve as electives for the ITMIA specialization: 1) CECS 6005: Principles of Information Security; 2) CECS 6035: Contingency Planning; 3) CECS 6015: IT Auditing and Secure Operations; 4) CECS 6045: Law, Investigation and Ethics. These six courses cover key topics that are essential for IT security professionals.

The GCIAS focuses on threats and vulnerabilities, cryptography, IT auditing, contingency planning, authentication and access control, security models, data communications, computer and network security, Internet security, trusted computer systems, distributed system security, applications security and security management policies, ethical and legal aspects, among others.

The great demand for IA education in other critical areas and the proven need for these skills in the industry also motivated the Graduate School to propose the development of a Graduate Certificate in Computer Forensics (GCCF). The goal of computer forensics is to examine digital media in a forensically sound manner with the aim of identifying, preserving, recovering, analyzing and presenting facts and opinions about the information.

In a recent feasibility study done to propose the GCCF [23] a sample of students in related areas were asked if they were interested in enhancing their IT professional skills with IA certificate programs that are in great demand. As can be observed in Figure 1, a total of 92.59% of the students surveyed were interested in enhancing professional skills with certifications in IT.

![Figure 1. Percentage of Students Interviewed Interested in Enhancing Their Professional Skills with Certifications](image)

Students enrolled in this certificate will use the recently inaugurated and unique Computer Digital Forensics Investigation Laboratory (CDFIL). This lab was inaugurated on March 10, 2010 by Mr. Richard George, Technical Director of the Information Assurance Directorate of the National Security Agency (NSA) and past advisor of the NSA Director. Officials from the FBI, US Secret Service, Immigration, Homeland Security, and PR Police Department were present.

The Certificate is primarily for students who are pursuing a Master Degree in Computer Science or who are working in the area of Information Technology (IT) and wish to broaden their skills and knowledge base in computer forensics. The GCCF will be the first in Puerto Rico; and a great opportunity for local and federal employees, as well as the private sector. The development of the certificate was supported with an award from the DoD HBCU granted in 2010 to Dr. Alfredo Cruz, from PUPR. At this moment, the GCCF is being revised by the PUPR Academic Council and will be sent to the local agency Council of Higher Education of Puerto Rico for accreditation.

The GCCF prepares IT professionals to combat imminent IT threats through the mastery of critical capabilities such as network infrastructure design, advanced digital investigative techniques, and state-of-the-art forensics strategies. The GCCF is anticipated to attract people from local and national law enforcement agencies who need the background in this area to enhance their job skills and overall performance.

To complete the certificate program the student must take a total of 5 graduate courses of three (3) credits each: 1) Computer Security; 2) Network Security; 3) Computer Forensics; 4) Advanced Computer Forensics; 5) Law, Investigation, and Ethics.

Through this certificate, participants will gain vital insight into obtaining and documenting digital information, determining the source of information compromises and delivering expert testimony concerning digital crime related to data in computers, networks and hand-held devices. In addition, the certificate addresses recovery of corrupted, encrypted and hidden information, providing a comprehensive preparation for assisting in the prevention and prosecution of malicious information theft and other criminal activity.

VII. Developing a Graduate Program Curricula in Information Assurance

Before the development of a graduate IA program, it is important to understand the needs of local and federal governments, and the industries; map these needs to the course curriculum, and develop the specialization areas that will provide the knowledge and skills that are most in demand. A complete graduate program in Information Assurance should be a combination of both technical and managerial skills in IA that can significantly mitigate all types of logical and physical threats that an information system can be susceptible to.

In recent thesis work by done by Sandra Bonilla [24] at PUPR, she goes through the processes that lead to the development of core courses for a Master Degree curriculum in information assurance with a Common Body of Knowledge (CBK). This is important for practicing professionals in information assurance and also provides students with professional skills and knowledge to excel in their professions, and stakeholders with a clear and concise accounting of the knowledge and skills to be learned. However the CBK is based in the mapping and needs of the industry, professional graduate students, CISSP domains, NSTISSI standards and NIST. The results of her investigation showed the approach, focus, position and roles to the knowledge areas, and the specific courses in IA fields that were more in demand.

In the quest to develop a model curriculum for a Master in Information Assurance and Security program a questionnaire was used as a research instrument to measure student and industry knowledge, opinions, preferences, interests, and importance in relation to developing a graduate IA program. There is an imperative need to match the knowledge and skills required in the area of information assurance and security in the local and federal government and industries, with the knowledge and skills that are to be delivered to students in an Information Assurance program in certificates, and academic degrees, in this case at the graduate level. Another important issue is how this program can provide students with these skills and know-how and at the same time create the necessary awareness so that these skills can become of interest and
importance to students in their IT careers. In such a way these programs can significantly increase the number of IT professionals with IA skills to serve the needs of local/national government and industries in protecting their intellectual assets, and in effective organizational contingency planning, and threat response protocols for national security, and organizations in general.

Interviews were done to students, executives, managers, and technical personnel from local and national companies.

The industry survey was distributed randomly to companies in Puerto Rico and in the United States to employees in technical and managerial positions. It revealed that the need for IA education was highly recognized by the IT professionals surveyed, whom constitute possible candidates for enrollment in the program. It acknowledged the awareness in the industry of the importance of IA education. The student survey questionnaire was administered to students of different institutions in the metropolitan area of Puerto Rico. It concluded that the majority of the students enrolled in related Bachelors or Masters Programs at different institutions were interested in enrolling in a Master in Information Assurance program to complement undergraduate and graduate studies. They were conscious of the need for information assurance and security skills in their professional careers.

When presented with the different security areas of interest, students revealed that they consider Network Security (technical field) as the most in-demand IA specialization area. System Auditing (managerial field) was their second choice, and Computer Forensics (technical) was third. Contingency Planning (managerial) was fourth in importance to the students interviewed, and Cryptography was fifth. As seen in Figure 2

![Figure 2. Students Interviewed: Most Important IA Specialization Areas](image)

The industry survey also revealed that Network Security is the most in demand specialization area in IA; according to their experience, 75.41% consider that Network Security has the greatest demand in the field of information security. Second choice was System Auditing with 49.18 percent and third choice was Contingency Planning with 47.54 percent. Following fourth was Computer Forensics with 45.90 percent and Cryptography with 32.79 percent as the fifth preference. Please see Figure 3:

![Figure 3. Industries Interviewed: Most Important Specialization Areas](image)

As could be observed in the survey, the need for a combination of technical and managerial skills is perceived in the industry and also by the students. Understanding this need will facilitate the selection of the topics and course curriculum for the development of a Master in Information Assurance program. A balanced security program with both technical and managerial aspects is suggested.

The thesis work done [24] helped to consider a set of core courses that include both managerial and technical skills for graduate IA students. These core courses were designated to meet existing national security standards, certifications, and security documents, and provided a foundation for the curriculum model. Two programs were created composed of the six core courses in information assurance and security topics:

1) Introduction to Information Assurance - provides fundamental concepts to understand technical and managerial key issues. Exposing these information assurance concepts help assure that every student has a decent knowledge of security at the beginning of the program if in their undergraduate program do not teach any security concept.

2) Management of Information Assurance and Security - covers methods used to raise general security awareness, reviews current industry practices, and develops expertise needed to adapt policies, procedures and regulations to safeguard proprietary information.

3) IT Auditing, Secure Control and Operation - outlines the concepts of information technology to understand the audit concerns, controls for application systems, techniques for auditing automated systems in the IT environments.

4) Computer Security - covers the principles, mechanisms and implementation of computer security and data protection. Learning how attacks work, how to defend against them, and how to design systems to withstand such attacks.

5) Network Security - provides an introduction to the fundamental insecurities in today’s networks and the commonly used tools and techniques used to secure them.

6) Computer Forensics - provides the skills and knowledge to acquire and preserve evidence from a computer and knowledge to analyze data and to report their findings.

The first program is focused in electives courses in technical areas. The second program focuses the elective courses on managerial skills. Please see Figure 4:
This section will explain the process of applying for the CNSS Certification and the CAE/IAE Designation.

Figure 4. Curriculum for a Master Information Assurance Program

VIII. Applying for the CNSS Certification and the CAE/IAE Designation

The National Information Assurance Education and Training Program (NIETP) office within the Information Assurance Directorate at NSA, manages the IACE program. The NIETP operates under national authorities, serves as a National Manager for Information Assurance education, and develops training standards within the Committee of National Security Systems (CNSS) [26].

The CNSS provides a forum for the discussion of policy issues and sets the national policy, operational procedures, and guidance for the security of national security systems. The security of the national systems is imperative. These systems contain classified information or involve: intelligence activities, cryptographic activities related to national security, and the command and control of military forces and equipment that is an integral part of a weapon or weapons system and/or critical to the direct fulfillment of military or intelligence missions.

The training/educational standards for information assurance and system security issued to date are [18]:

- NSTISSI-4011, National Training Standard for Information Systems Security (INFOSEC) Professionals
- CNSSI-4012, National Information Assurance Training Standard for Senior Systems Managers (SSM)
- NSTISSI-4013, National Information Assurance Training Standard For System Administrators (SA)
- NSTISSI-4014, Information Assurance Training Standard for Information Systems Security Officers (ISSO)
- NSTISSI-4015, National Training Standard for Systems Certifiers (SC)
- CNSSI-4016, National Information Assurance Training Standard For Risk Analysts (RA)

The standards were developed by the government as unclassified information to develop an information assurance community and to expand the education and training throughout the nation. The IACE program is located on a secure interactive website (https://app.cnss.gov/nietpcw352.nsf/), which certifies the institutions courseware, not its programs or certifications. The standards justify IA education, training, resource education, and help to increase the national security infrastructure.

Information system security professional standards (NSTISSI/CNSS 4011) need to be mapped for the CNSS certification and it is based on: Communication Basics; Automated Information System Basics; Security Basics; NSTISS Basics; System Operating Environment; NSTISS Planning and Management; NSTISS Policies and Procedures. NSTISSI 4011 responds to the need for a theoretical foundation for modeling the information systems security sciences, and addressing the needs for information systems security.

Mapping NSTISSI 4011 with CNSSI-4012, NSTISSI-4013, NSTISSI-4014, NSTISSI-4015 and/or CNSSI-4016 is the first requirement for the designation of the institution as a CAE/IAE [5]. PUPR chose the NSTISSI-4013, which requires a minimum training for the development and implementation of Information Assurance (IA) training for System Administrators (SA) and is related to the courseware of the Institution.

For NSTISSI-4013, NSTISSI-4014 and CNSSI-4016 a hierarchical level or bloom taxonomy is one of the best ways to categorize levels of questions commonly used in the educational area and to evaluate that the curriculum meets the needs of the students [27]. The levels are: 1) Entry - define, demonstrate, identify, outline, use; 2) Intermediate - design, manage, prepare, recommend, implement; and 3) Advanced - compare, evaluate, integrate, resolve, revise, verify

Entry level requires less skill and does not require any implementation or problem resolving. In entry level NSTISSI-4013 the System Administrator will be able to describe and apply the appropriate actions to manage and administer an Information System in a secure manner.

IACE reviewers validate if the institution courseware covers and maps 100% of the elements; the institution should provide their course syllabus (objectives, topics, and references) as evidence. After the validation, the institution will receive a formal certification of its courseware, certifying that all of the specific standards are met. IACE certification is awarded at the annual Colloquium for Information System Security Education Conference [28].

Polytechnic University of Puerto Rico, was the first university in Puerto Rico that mapped their courseware in a 100%, by the Committee on National Security Systems (CNSS), completing the National Standards 4011 and 4013 (entry level). The CNSS courseware certification is valid for 5 years, after that the institution needs to recertify.
IX. Summary
The protection and security of an organization’s intellectual assets has become an important challenge that should be considered in current academic curriculums. The continuously rapid change in the security field makes it extremely difficult for a university to establish a curriculum that will adequately prepare students for the professional challenges they will encounter. Nevertheless, bodies like ACM, IEEE and ABET do not have a formal or effective standardized Information Assurance curriculum model developed. Information Assurance educators are looking for the best ways to deliver the knowledge, skills, and expertise that is required.

With the research done at PUPR, a CBK for information assurance and security was done to set the path for the creation of Master in Information Assurance Program that can be used at other institutions to promote education at a graduate level that includes both technical and managerial focuses in the course curriculums for IA education. Through this research, the institution has been able to create a CBK that is useful for graduate and undergraduate certificates and programs, enhancing current IA programs and courses, and opening the path to future IA programs.

X. Bibliography