# Report of the Cyber Security Task Force

to the University System of Maryland, May 2011

## TABLE OF CONTENTS

# Executive Summary

University System of Maryland (USM) Chancellor Dr. William E. Kirwan in November 2010 convened a task force of representatives from USM institutions, state and federal government agencies, and private-sector businesses to examine the assets of the USM in the area of cyber security and evaluate the workforce needs of government agencies and private industry in this area.



After meeting with representatives of USM institutions as well as federal agencies, the USM Cyber Security Task Force formed two subcommittees. One subgroup (Academic Inventory) inventoried all of the academic programs and university assets related to cyber security in addition to research and collaborative relationships with faculty, government and private industry. The second subgroup (Government and Industry) concentrated on assessing the types of skills and degrees most applicable in assisting government and private industry in meeting their workforce needs.

The Task Force found within the USM a range of programs—including 53 separate bachelor's degrees, 33 master's degrees, nine doctoral degrees and 13 related undergraduate and post-baccalaureate certificates—relating to a range of needs within the cyber sector.

Four USM institutions have been designated as Centers of Academic Excellence or Research Excellence in Information Assurance by the National Security Agency and the U.S. Department of Homeland Security: Towson University, the University of Maryland, Baltimore County (UMBC), the University of Maryland, College Park (UMCP) and University of Maryland University College (UMUC). USM institutions have significant and growing research programs in the area of cyber security, many including collaborations with the public and private sectors.

There is no doubt that the demand for a skilled workforce in the area of cyber security and information assurance is significant and will continue to grow. The Task Force was able to determine qualitative standards as to academic areas needed. However, without a more extensive scientific survey, a better quantitative statement on numbers of degrees is not possible at this time.

The Government and Industry subgroup developed a survey instrument to query for the basic skill set needed for the cyber workforce. The common thread between the feedback from all employers and discussions within the Task Force is that all graduates entering the job market, regardless of their major, need a basic awareness and understanding of cyber security. The USM would benefit employers as well as current and future cyber professionals by continuing to provide high-caliber degrees in traditional technology and policy areas, and the USM should enhance traditional curriculum with hands-on training and development in cyber techniques and technologies.

The Task Force made five actionable and achievable recommendations:

1. Working with the Governor's Workforce Investment Board, conduct a comprehensive and scientific survey of employer needs.

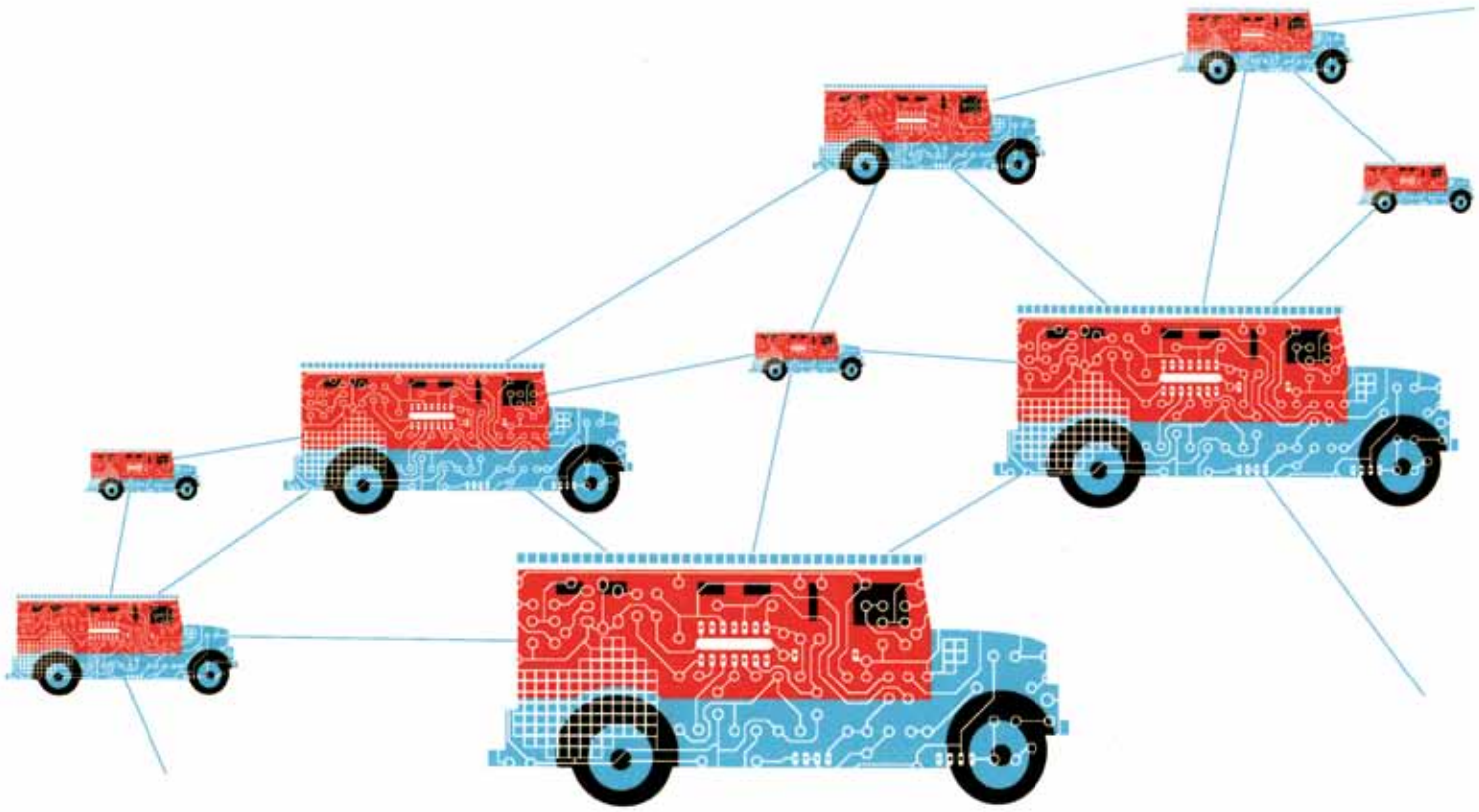
2. Enhance and extend higher educational offerings related to cyber security and information assurance.

3. Establish more partnerships among education and government and private industry and leverage the resources available.

4. Strengthen research and support innovation and technology transfer in cyber security.

5. Expand the cyber security career pipeline through collaborations between the USM and Maryland's community colleges. As part of this coordination, adopt models to increase awareness and reduce impediments to obtaining a security clearance.

The Task Force recognizes there are a number of ways to address cyber security and information assurance and believes the effort to do so should continue to expand by implementing the five recommendations proffered in this report.





# A. Introduction »

In today's globally interconnected communications and information environment, cyber security is necessary to ensure critical support for the U.S. economy, civil infrastructure, public safety and national security. Critical sectors of the national economy are now reliant on the effective and secure flow of electronic information and communications systems. Identity theft, network viruses, loss of sensitive information and other malicious activities pose serious threats in the disruption of these crucial information and communication systems. Protecting our nation's information networks requires a strong vision and leadership.

The National Security Agency defines cyber security as:

> *measures that protect and defend information and information systems by ensuring their availability, integrity, authenticity, confidentiality and non-repudiability.*

Virtually every important government, military, law enforcement and private institution concerned with the nation's security has made it clear that cyber-based threats "pose a potentially devastating impact to technological systems and operations and the critical infrastructures they support."[1]

Cyber security consists of a considerable set of multidisciplinary talents, processes, discrete technologies, capabilities and services that stem from and expand on practices of computer information and network security. Information security is now integrated, or at least should be integrated, into every information process in government and business.

Cyber security technology encompasses the software and hardware tools, techniques and risk management processes that assure the confidentiality, integrity and availability of data, thus providing the means to share information across the Internet without threat of attack or theft.

In view of the growing importance of information security, educating professionals to deal with the above-mentioned threats, especially within the University System of Maryland (USM) with its strong engineering, computer science and information systems, business, policy and legal resources, should continue to be a paramount goal.

In this report, we provide a description of existing education programs and research assets, capabilities and activities within the USM. We also provide information about the workforce needs of the public and private sectors. Finally, we conclude by making a number of recommendations on how the cyber security capabilities of the USM can be improved to serve the needs of the state and region.

# B. The National Capital Region, State of Maryland and University System of Maryland Context »



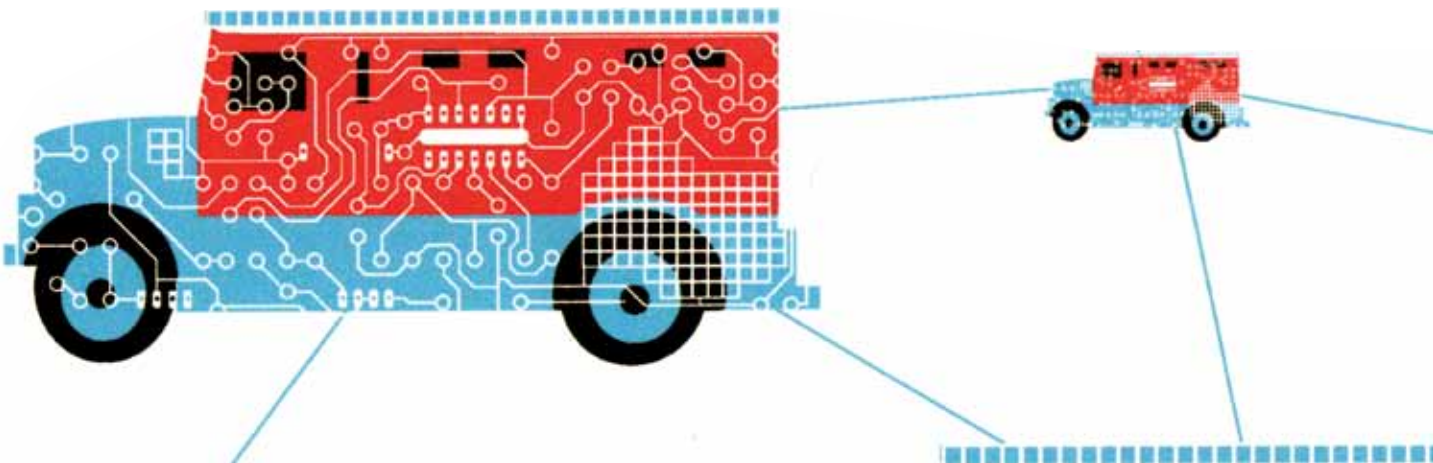
Maryland—with its vast resources of federal facilities, academic institutions, industry strengths and intellectual capital—is the *de facto* epicenter for cyber security.

Maryland is home to the National Security Agency (NSA), the U.S. Cyber Command, the Intelligence Advanced Research Projects Activity (IARPA), the National Institute of Standards and Technology (NIST), the Defense Information Systems Agency and other federal assets. Coupled with the expected Department of Defense (DOD) expansions of the intelligence and communications responsibilities at Fort George G. Meade and at Aberdeen Proving Ground, Maryland is the base for our nation's efforts to defend and protect U.S. information networks.

Additionally, cyber security assets in the National Capital region, including the new headquarters for the Department of Homeland Security, being developed just miles from the Maryland/District of Columbia border, offer even more possibilities of regional collaborations and industry clustering.

Maryland is also very fortunate to have a significant and growing cluster of private-sector companies, ranging from small start-up firms to large global cyber security firms. These technology firms serve as contractors to both government agencies as well as private-sector companies. They present large demands for an educated and trained workforce as well as tremendous opportunities for collaboration, partnerships and internships for students and higher education institutions.

These resources make Maryland a national leader in securing our country's critical cyber infrastructure. We have a robust higher education system that trains the next generation of cyber security experts, institutions that are developing innovative cyber technologies and one of the nation's most technically advanced workforces. Maryland is among the first states to have already implemented significant cyber security protection initiatives. And, we have a rapidly growing information technology industry cluster that offers the full spectrum of cyber security capabilities.



# c. Charge of the Task Force »



The following is Chancellor Kirwan's charge to the Cyber Security Task Force:

## Context

Cyber security has become one of the most significant issues of our time. It affects industry and commerce, personal finances, national security and all levels of government. Maryland enjoys a high concentration of government labs, a growing technology-based private sector and a strong system of higher education capable of of providing national leadership on cyber security issues. A recent report released by Governor O'Malley, entitled "CyberMaryland," makes the case that the state is positioned to be the hub for federal, academic and private-sector cyber security efforts. The report laid out four priorities for the state:

- Supporting the creation and growth of innovative cyber security technologies in Maryland;
- Educating new cyber security talent in the state;
- Advancing cyber security policies to position Maryland for enhanced national leadership; and
- Ensuring sustained growth and future competitiveness of the state's cyber security industry.

## Charge

The Cyber Security Task Force is charged with examining the USM institutional assets related to cyber security, determining both the research and workforce needs of the public and private sectors, and the workforce skill sets necessary to address these priorities. Further, the Task Force is charged with developing strategies for meeting those needs.

The Cyber Security Task Force will study and report on the following:

- An inventory of existing programs, degree offerings, research activities and infrastructure within USM institutions that relate to cyber security.
- The research and workforce needs if the state is to realize the goals of the "CyberMaryland" report.
- The quantified and qualitative degree requirements for jobs relating to cyber security over the next decade.
- Programmatic and facility needs to meet the identified programmatic and research demands.
- Existing research collaborations among universities, private-sector firms and government agencies on cyber security and barriers to overcome in order to develop greater collaboration in the future.


The Task Force will:

- Recommend USM strategies, and policy changes needed to meet these demands.

- Recommend actions and policies at the state level that would support the creation of a strong and vital cyber security workforce and R&D capacity in Maryland.

In responding to these issues, the Task Force should consider these questions:

- Do we have appropriate programs in place to achieve the recommended cyber security research and workforce targets?

- Do we have appropriate programs in place to recruit and employ an adequate number of cyber researchers, faculty, graduate students and postdoctoral researchers?

- Do we have appropriate programs for developing a range of cyber security competencies from security practitioners and network security engineers to information assurance specialists and subject-matter experts in specialized cyber security areas such as authentication, cryptography, artificial intelligence, computer forensics, policy and law, and others?

### Task Force Composition and Report:

The Task Force will be chaired by Nariman Farvardin, Acting President, and Senior Vice President for Academic Affairs and Provost at the University of Maryland, College Park, with membership drawn from the presidents and senior officers at USM institutions, federal and state agencies, and private-sector firms active in the area of cyber security. The Task Force is asked to complete its report for the USM by the end of February 2011.

# D. Work of the Task Force »

The Task Force began its activities on November 17, 2010. At its first meeting, the Chancellor provided the context for a coordinated effort to examine the assets of the USM in the area of cyber security and evaluate the workforce needs of government agencies and private industry in this area, and formally charged the Task Force.



The Task Force organized presentations by representatives of different USM institutions describing their various degree and certificate programs and course offerings related to cyber security. These representatives also covered some of their cyber security research programs currently underway or in various stages of planning. Furthermore, the Task Force organized discussions focusing on the scope of cyber security activities in government agencies and private industry, with a special emphasis on their workforce needs—both qualitatively and quantitatively.

To develop a more complete analysis, the Task Force created two subgroups to evaluate cyber security assets and activities in the USM institutions, and to correlate them with workforce needs and capacity in the public and private sectors. The following provide additional details on the activities of these subgroups.

### Academic Inventory Subgroup

Within the broad assignment of the Task Force, the charge to the Academic Inventory Subgroup was to examine the extent and scope of academic offerings and research programs of the USM institutions in the broad area of cyber security. Specifically, this subgroup was asked to describe USM's current production function for education and training in cyber security by identifying the relevant certificate and degree programs offered through the USM institutions and by reporting on their productivity to date. In addition, the subgroup was to formulate recommendations for enhancing the capacity of the USM to meet workforce needs.

In fulfilling this charge, the subgroup made the following two decisions:

1. The subgroup interpreted "cyber security" as a category of different competencies needed by industry and government, rather than as a sharply defined academic field. Consequently, the subgroup included in its inventory degree programs and certificates for a variety of academic programs, not simply those that have "cyber security" in the degree or certificate title. These decisions were based on programs that produce graduates who work in cyber security careers. The inventory covers both technical programs and programs that focus on policy and management. There is recognition of an emerging third community of programs that are related to cyber security, hosted within disciplines, such as criminal justice, accounting or finance, and often have a forensic character.

2. The subgroup defined the "productivity" of degree programs as the number of graduates, and chose to assess this productivity by reviewing data for the last three fiscal years. For programs that are new, the number of majors in their program as of the fall 2010 semester would serve as a baseline for estimating expected productivity. While number of doctorates graduated gives a sense of research productivity, the subgroup additionally considered research productivity broadly in terms of funding levels and an enumeration of outside collaborations.

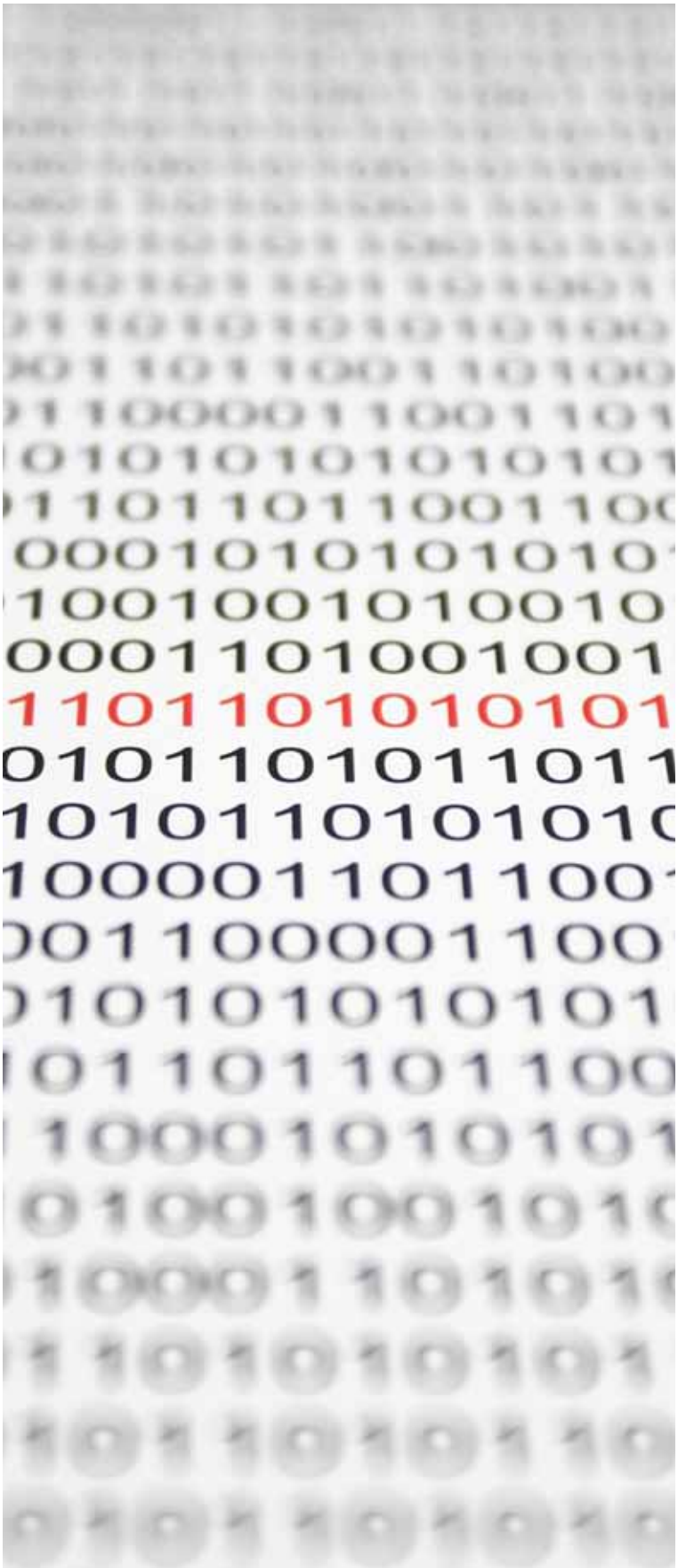
The Academic Inventory Subgroup's findings and recommendation were used to provide much-needed information on the academic and research programs within the USM and to make recommendations for improving the USM's programs in cyber security.

## Government and Industry Subgroup

The Government and Industry Subgroup was initially charged with developing a market demand for USM graduates entering the cyber security field. Early on in the subgroup's meetings it became clear that, since the USM serves the global market, this scope would not be achievable given the time frame. Consequently, the group developed a qualitative approach, in lieu of a specific quantitative measure, to address its charge. In so doing, the subgroup developed a survey instrument to query for the basic skill set needed for the cyber workforce. The survey was sent out and a small number of government and commercial respondents provided feedback as to the fundamentals needed.

In the limited amount of time available to the subgroup, it was difficult to conduct a comprehensive analysis of the type and extent of the needs of industry and government in cyber security. However, based on the discussions within the subgroup and the Task Force, additional input received from colleagues in the public and private sectors, and feedback received via the survey instrument, the Government and Industry Subgroup concluded that the needs of the cyber security industry varies significantly by sector. For example, the needs of the NSA for its core cyber security group would be very different from that of government contractors and the businesses within the private sector. Despite these differences, it appears from the survey and anecdotal evidence that the workforce needs are significant and growing. Additionally, the requirement for U.S. citizenship and clearances in some cases for government and government-related work places an additional burden on finding qualified workers graduating from USM institutions. The newly established cyber programs by USM institutions should alleviate some of the government and industry needs.

From the discussions, the process of designing the survey, and the survey results, the Government and Industry Subgroup developed a set of recommendations that formed the basis for the Task Force's recommendations provided later in this report.



# E. Current Status »



In this section, we summarize the findings of the Task Force, largely based on the work of the two subgroups, in three distinct areas: (i) academic programs currently available within USM institutions, (ii) existing research programs, collaborations and available research infrastructure and (iii) industry and government workforce needs.

## Academic Programs

Member USM institutions were asked to identify academic programs consistent with the subgroup's understanding of cyber security (see Section D, above). The result is a range of programs including 53 separate bachelor's degrees, 33 master's degrees, nine doctoral degrees and 13 related undergraduate and post-baccalaureate certificates. The programs identified include computer science, electrical engineering, computer engineering, information systems/technology, mathematics, physics, business and management, as well as different flavors of degree and certificate programs related to cyber security and information assurance. The academic program inventory is detailed in Appendix A. These programs vary widely in their admission requirements and the student populations that they serve. Programs with the same or similar titles may reflect a different emphasis or approach. Taken as a whole, they reflect expected institutional missions and aim to address a range of needs within the cyber sector.

Within the inventory, it is important to note that four USM institutions have been designated as Centers of Academic Excellence or Research Excellence in Information Assurance by the National Security Agency and the Department of Homeland Security: Towson University, the University of Maryland, Baltimore County, the University of Maryland, College Park and University of Maryland University College.

Three institutions—the University of Maryland University College, the University of Maryland, Baltimore County and Towson University—offer online degrees in competencies related to cyber security. In addition, these institutions offer certificates as well as face-to-face programs in cyber security and can scale to meet the needs of the workforce sectors that they serve.

During the 2009–10 academic year, USM institutions produced 2,184 graduates in bachelor's, master's and doctoral programs in cyber security broadly construed, i.e.,

encompassing the variety of specialized competencies important to cyber security work by industry and government. The large majority of these degrees (1,958) were in technical areas, and most were in foundational areas like computer science, mathematics and physics rather than areas where cyber security is the primary focus. Both Bowie State University and Towson University have existing undergraduate and graduate programs specifically in cyber security, and the University of Maryland, Baltimore County (UMBC) and the University of Maryland University College (UMUC) have launched new degree programs in cyber security and expect their first graduates in the 2012–13 academic year.

A few important comments are in order. First, it must be noted that almost all of these degree programs are in science, technology, engineering and mathematics (STEM) fields for which there is competitive market demand across many sectors. Second, while many of these degrees enable a graduate to be immediately employed in cyber-related work, many graduates find that they are required to "cap off" degrees with specialized training in more focused cyber security subject matter before they are adequately qualified to work on cyber security projects. UMBC, through its Center for Cybersecurity Training (*www.umbc.edu/trainctr/cyber/index.html*), delivers significant training and certification preparation to the incumbent cyber workforce as well as those seeking to enter this emerging field. The Center for Cybersecurity Training holds a Top Secret clearance and supports government agencies, the military and the commercial sector in the development of cyber-related skills, knowledge and credentials for their people. In 2010 the Center had 700 enrollments in its cyber programs and continues to expand its offerings regionally and globally through its growing online capabilities. Finally, degree data alone are not a true indication of the number of cyber security-capable individuals, since other factors, such as the need for citizenship and security clearances, are also often critical. For these reasons, both the number and kinds of degrees the USM generates, as well as other factors in defining suitability for employment in cyber security positions must be closely analyzed, and multiple strategies will be needed to increase the pipeline of cyber security-ready individuals.

## Research Programs, Collaborations and Infrastructure

There is a host of cyber security research programs, many including collaborations with the public and private sectors, in the USM institutions. The total value of current federally funded research in cyber security and affiliated fields conducted by USM institutions exceeds $100 million. The University of Maryland, College Park (UMCP) accounts for a majority of this work, followed by UMBC, Towson University and University of Maryland, Baltimore (UMB) also contributing to this research.

UMCP, ranked among the top 20 public research universities in the nation, has a variety of research programs in cyber security. It recently launched the Maryland Cybersecurity Center (MC$^2$) as a focal point of its cyber security research efforts. MC$^2$ is partnering with government and industry to provide educational programs to prepare the future cyber security workforce, and develop new, innovative technologies to defend against cyber security attacks.

MC$^2$ is taking a comprehensive approach to cyber security education, research and technology development, stressing "more-than-tech" interdisciplinary solutions. MC$^2$ brings together experts from engineering and computer science with colleagues from across the campus in fields such as accounting, economics, the social sciences and public policy to help establish broad-based cyber security initiatives. UMCP researchers are applying their expertise in key areas, including wireless and network security, secure software development, cyber supply chain security, privacy in social networks, cyber security policy, cryptography, attacker behavioral analysis, health care IT, multimedia forensics and the economics of cyber security.

UMBC is one of the emerging research centers in basic and applied information technology research, including cyber security. UMBC has established close partnerships with and obtained research funding from a variety of federal and industrial sources. These include NSF, a variety of DOD entities (e.g., the Defense Advanced Research Projects Agency, Air Force Office of Scientific Research, Office of Naval Research), the National

Oceanic and Atmospheric Administration, NIST, Northrop Grumman, Lockheed Martin, IBM and SAIC, as well as a variety of smaller companies that support DOD work, to advance cyber security-related research in the areas of situational awareness, distributed and privacy-preserving analytics/data mining, policy-driven systems, semantic information extraction, mobile security, sensor networks for security, security of cyber-physical systems such as the smart grid, secure voting, visualizing threats and human-computer interfaces for accessible/usable security. UMBC is focusing these strengths to develop a broad-based cyber security research program focused on situational awareness and threat detection. UMBC has a core set of research groups across departments, and envisions forming an interdisciplinary center that includes many departments in the College of Engineering and Information Technology as well as faculty from other departments such as Sociology, Economic, Public Policy and Geography. The NSF-supported Center for Hybrid Multicore Productivity Research is also involved in research on situational awareness, response and mitigation of a variety of extreme events.

UMB at the Center for Health and Homeland Security (CHHS) provides policy guidance and planning services to more than 40 public and private institutions. CHHS employs nearly 70 full-time professionals dedicated to homeland security research, planning, training and exercises. CHHS provides homeland security consulting services on a range of issues, including cyber security. The founder/director of CHHS, Michael Greenberger, also serves as the Chairman of the Governor's Emergency Management Advisory Council, an organization that, because of Governor O'Malley's interest, will have cyber security on its agenda. The cyber security work of both CHHS and the UMB School of Law is focused on the laws and policies of this rapidly developing field. Specifically, this work focuses on the legislation, administrative guidance and policy research related to cyber security.

A summary of current or recently completed research at USM institutions appears in Appendix B. USM institutions' research in cyber security includes extensive collaboration with the public and private sectors. Specifically, UMCP has partnerships with SAIC, Lockheed Martin, Google, Security Technology Institute and Tenable Network Security. Adjacent to the UMCP campus are two large DOD-funded research labs, and the University's research park is home to the headquarters for IARPA and the DOD-funded Center for Advanced Study of Language. UMBC has partnerships with SAIC, Northrup Grumman, Lockheed Martin and IBM, among others, and its research park houses seven cyber security companies.

One could conclude from the above observations that the USM institutions have significant and growing research programs in cyber security and that there are active collaborations between the faculty and researchers of the USM institutions and appropriate government and private-sector entities. In addition, UMCP, UMBC, UMB and Towson University are actively working to expand their cyber security research programs.

## Workforce Needs and Associated Education Requirements

Based on the limited responses to the survey (See Appendix C), one could draw the conclusion that employers seek a technical foundation in their cyber security employees, though the importance of the various skills may vary by the organization or position. The debate of certifications continues: some organizations would rather have a technical basis in their cyber security employees and teach them the skills, while others would like to see them come in with one or more cyber-related certifications. The latter preference is typically with services-based companies that can deploy graduates into consulting situations. The common thread between the feedback from all employers and discussions within the Task Force is that all graduates entering the job market, regardless of their major, have to be prepared with a basic awareness and understanding of cyber security. In the case of student preparation for technical cyber security-related positions, there has to be a basic technical foundation.

A continuum of skills and education, analytical and technical, is necessary to support the cyber defense environment. The degrees and knowledge, skills and abilities required of candidates fall into two categories: Analyst and Technologist. (See Chart 1.)

Analysts fall into several job titles: Defense Analyst, Policy Analyst, Intelligence Analyst, Threat Analyst and Security Analyst. Traditionally, analysts have earned degrees in the following areas: history, social studies, political science, business, military history and tactics or law. Each of these degree programs helps candidates develop the necessary skills and abilities for success, including critical thinking and analysis, research and data mining, writing and public speaking, policy development and subject-matter expertise in areas of interest.

Technologists fill traditionally technical jobs: Software Developer, Software Engineer, Systems Engineer, Security Engineer, Test Engineer and Information Security/Assurance Engineer. Technologists earn degrees in math, computer science, physics, information technology, management information systems and engineering. These degree programs hone a graduate's critical thinking ability, provide skills in process development and develop expertise in technical systems, hardware and software.

Currently, most job titles, even for cyber roles, do not carry a specific "cyber" job title. Industry is beginning to build "cyber"

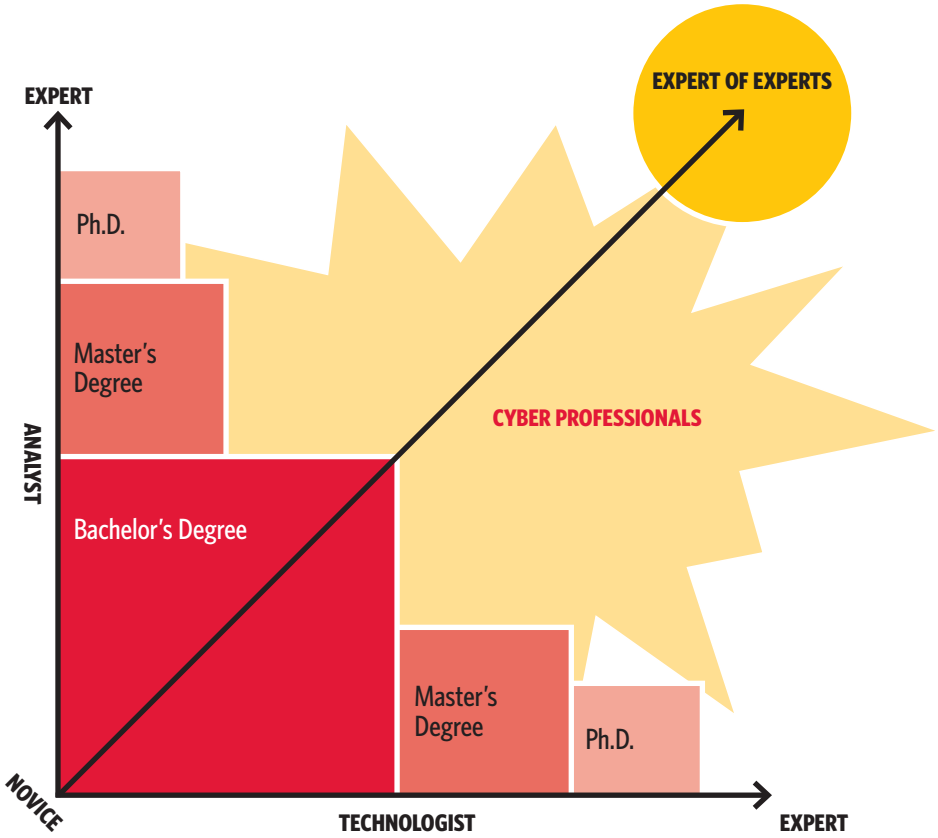



**Chart 1:** Cyber professionals include traditional analysts and technologists with hands-on training and development in cyber techniques and technologies.

job descriptions that encompass the underlying analyst and technology base, plus cyber knowledge, skills and abilities.

In addition to specific degrees, there are common traits that strongly correlate to success in these roles: the ability to work in a team, a high level of ethics and intellectual ability.

Positions with, or that support, the U.S. government, especially the DOD or intelligence communities, often require U.S. citizenship, the ability to obtain and maintain high-level U.S. government security clearance and a commitment to protect the United States and its citizens.

In a global economy, governments, companies and industries are sustained by electronic infrastructure and systems. All need talented cyber professionals with the knowledge, skills and abilities to protect and defend infrastructures, information and systems by ensuring their ability, integrity, authentication, confidentiality and non-repudiation. Each need a diversity of expertise from novice to the cyber expert. With the constant and quick development of technologies and new threats every day, these cyber professionals need continued education, development and research in their fields. In an effort to assist in the encouragement and affordability of developing a trained workforce in these areas of national need, the federal government has 11 scholarship and loan forgiveness programs that may be applicable to areas of study related to cyber security and information assurance. A listing of these programs is included in Appendix D.

The USM would benefit employers as well as current and future cyber professionals by continuing to provide high-caliber degrees in traditional technology and policy areas. The cyber security areas with growing workforce demands include:

- Network penetration testing and techniques
- Evidence seizure
- Forensic analysis and data recovery
- Intrusion analysis and incident response/reporting
- Intrusion detection and network surveillance/monitoring
- Network protocols, devices and multiple operating systems
- Secure architecture
- Policy and legal development and analysis
- Law enforcement and counterintelligence assessments
- Data collection and analysis (including data mining)
- Threat analysis
- Malware analysis
- Incident investigations, reporting and vulnerability assessments
- Defensive solution development

# F. Recommendations »



Maryland's institutions of higher education are a critical asset for sustaining and elevating the state's position as a national leader in cyber security. The following recommendations encapsulate strategies and actions for advancing the State of Maryland's cyber security priorities, as outlined in the recent "CyberMaryland" report:[2]

- Ensuring sustained growth and future competitiveness of the state's cyber security industry.
- Educating new cyber security talent in the state.
- Supporting the creation and growth of innovative cyber security technologies in Maryland.
- Advancing cyber security policies to position Maryland for enhanced national leadership.

After extensive discussions within the Task Force, it became apparent that cyber security remains an important area, both in terms of education, training and workforce development, and in the research challenges and opportunities it presents. The following constitute the Task Force's recommendations.

### RECOMMENDATION 1: Conduct a Survey

The USM should conduct a comprehensive and scientific survey of government and industry workforce and skill needs in the area of cyber security. This may be done in collaboration with the Governor's Workforce Investment Board, which has launched an initiative in this area. The response to this survey should be used to develop a thorough assessment of the type of skills needed for the cyber security workforce, as well as the anticipated number of cyber employees needed in the short and long terms. The specific findings of this recommendation will determine the specific numerical targets for many of the subsequent recommendations.

Without a more comprehensive and scientific survey, the Task Force did not believe it had enough data to set specific quantitative goals on how USM degree production should be increased. Instead, the Task Force has identified a few areas in which an improvement in the education and research programs within the USM would significantly benefit government and industry and will solidify Maryland's position as a leader in cyber security.

### RECOMMENDATION 2: Enhance and Extend Educational Offerings

The Task Force has identified a number of actions that would lead to enhancing the educational programs of the USM institutions in the area of cyber security, allowing the USM to better respond to the government and industry cyber workforce needs.

a. **Cyber Security Courses:** As the need for technical expertise in cyber security increases, it would be desirable for the primary degree programs that contribute to cyber security workforce, namely, computer science, electrical and computer engineering, mathematics and information systems, to offer more courses in cyber security, information assurance and related fields. This will enable graduates of these degree programs to complete their degree requirements with a stronger emphasis on cyber security, resulting in less on-the-job training. A related recommendation is to add, where appropriate, more cyber security emphasis to existing courses.

b. **Certificates, Combined B.S.-M.S. and Professional Master's Degrees in Cyber Security:** To address the growing need for a cyber security workforce, USM institutions may consider establishing certificate, combined B.S.-M.S. and new professional master's degree programs in the technical, policy and legal aspects of cyber security. These programs may be tailored to address the needs of government and industry employers. Clearly, the creation of such programs must be in response to a well-established market demand.

c. **Specialization in Cyber Security:** The Task Force concluded that while some sectors of the cyber workforce must have a solid grounding in technical fields, there is a growing need for professionals in non-technical fields to have an awareness of cyber security. Examples of such disciplines include: accounting, finance, economics, media, sociology, psychology, criminal justice, political science and public policy. The Task Force, therefore, recommends that the USM consider establishing a cyber security specialization for students who are interested in gaining a modest level of knowledge in certain aspects of cyber security, with some focus on areas particularly relevant to the their area of study. In this manner, cyber security can be integrated into the broader curriculum, allowing a higher level of literacy in cyber security across different disciplines. Such specialization may be offered through a minor or an undergraduate certificate program.

While the Task Force is confident in the merit of the above-mentioned recommendations, it cannot make specific numerical recommendations at this point. We believe the magnitude of these programs and the number of students they serve should be determined after completing a careful and comprehensive analysis of the response to the survey of Recommendation 1. Also, we believe that the particular course offerings and their combinations into specializations should be undertaken in consultation with government and industry groups.

Needless to say, there will be a cost associated with implementing the specific elements of Recommendation 2. This includes funding for additional faculty at both the research and comprehensive universities as well as additional teaching assistants and adjunct faculty, particularly from the DOD, civilian government agencies and the private sector. It also includes investments that would assist with the process of reviewing curricula, adding appropriate courses to strengthen their cyber focus and developing new programs.





### RECOMMENDATION 3: Leverage Partnerships

The USM should make every effort to encourage partnerships within the USM and between the USM and the public and private sectors in order to enhance communication, strengthen collaboration and leverage resources in cyber security.

a. Form a consortium that would facilitate closer and organized communication among the USM, DOD, federal and state civilian agencies and the private sector about trends in cyber security, needed workforce competencies and needed research, offering a mechanism for pooling resources for targeted investments in education and research.

b. Establish government- and industry-sponsored cyber security undergraduate internships and graduate assistantships, facilitating the interaction of students in USM institutions with its partner organizations. These internships and assistantships will be used both to entice more students to the cyber security field and to enable appropriate students to start the process of security clearance while still enrolled.

c. Promote collaborations that include devising standards and criteria for academic programs or new industry certifications. Organize and promote cyber competitions and work camps to attract interest in cyber security and to provide an opportunity to scout talent.

d. Increase cross-collaborations between the universities within the USM, such as between the School of Medicine (and its associated hospitals) and the engineering and computer science teams at the other campuses to address ongoing concerns and problems in clinical care. Similar partnerships should be established with other universities in the state and region as appropriate.

### RECOMMENDATION 4: Strengthen Research and Support Innovation and Technology Transfer in Cyber Security

The Task Force noted that Maryland has tremendous expertise in cyber security by way of the federal government defense labs, the strength of local industry and the breadth of cyber security research in our universities. Most of the current corporate expertise and activities in cyber security are directed toward supporting the government. What has been missing is broad commercialization of this expertise into mainstream products and services aimed at individuals and the non-defense sector. This was noted in the "CyberMaryland" report, which laid out four priorities for the state, and first among them was supporting the creation and growth of innovative cyber security technologies in Maryland. Specific programs to achieve this goal could include:

a. Create a mechanism to support basic and applied research in cyber security. This recommendation requires additional

investment to recruit personnel, including "star" faculty specializing in different aspects of cyber security. The addition of such faculty will not only strengthen the USM's research programs in this important field, but will further credential USM in cyber security and magnify its ability to attract other promising faculty, federal research support and other resources. A significant byproduct of this effort will be attracting talented doctoral students and postdoctoral researchers to the USM, which, in turn, provides a pipeline for a highly sophisticated cyber security workforce to the government and industry labs. Furthermore, the USM should endeavor to strengthen collaborative research between USM institutions and the government laboratories engaged in cyber research. This could be implemented through a Cooperative Research and Development Agreement or Partnership Intermediary Agreement with the federal government that would directly benefit from the research.

b. Create a strong physical infrastructure for cyber security research and education. The infrastructures for research and education are very similar, so that through judicious investment both needs can be satisfied. The USM's cyber security programs need to take place in an environment where the experience is as close to the real world as possible, i.e., analogous to a medical teaching hospital, where cyber diseases are characterized, diagnosed and treated. Dedicated laboratory facilities for cyber security are severely lacking at USM institutions. Desirable laboratories would provide means to focus on areas such as: network intrusion detection and mitigation; network, software and data forensics; complex network visualization; reverse software engineering; mobile device security; risk analysis, supply chain security; identity and biometrics; and emergency response. The USM in its new Strategic Plan has called for construction of one million more square feet of research space in the next decade. Given the opportunities to develop robust partnerships with the growing federal and private-sector investments in cyber security, a significant fraction of this new research space effort should be devoted to developing specific cyber security lab facilities. Additionally, the USM should explore ways to finance the acquisition of shared core computer equipment and test beds dedicated to cyber research. We encourage the formation of partnerships involving government, industry and our universities to both define the architecture of our academic cyber security laboratories and to secure the resources required. In addition, we recommend that the USM, working with state and federal governments and the private sector, develop a set of distributed security research facilities that would support extremely large storage facilities, with specialized hardware for data mining. These facilities should be linked by extremely high-speed communications to test the latest network technologies used for security.

c. Spearhead the establishment of a state-sponsored fund to support cyber security research initiatives, similar to what California did in 2004 with Proposition 71, which was designed to support biotechnology research. This fund would be designed to promote collaborative projects between campuses and to invest in research infrastructure that can be leveraged to support additional outside funding.

d. Undertake a focused effort to support the creation of more cyber security companies, consistent with the overall USM goal of creating 325 companies in the next decade in Maryland. Such efforts might include attracting experienced cyber management that could help launch several cyber companies and work with USM institutions to attract cyber security seed and venture funding.

e. Expand our university incubator facilities to support the efforts of the start-up ventures in cyber security through public-private initiatives similar to what Northrup Grumman is doing at UMBC with its Cyinc, an incubator for cyber security technologies that subsidizes the cost of moving into the incubator for companies with early-stage cyber security products.

f. Work with the Maryland Venture Fund to expand its support and to provide incentives for supporting start-up companies in cyber security. We recommend that the USM form an advisory board of cyber security experts to review new cyber security technologies and organize a semi-annual program to showcase basic and applied research in cyber security that is done at USM institutions for angel investors, venture capitalists and entrepreneurs to help move basic research from the lab to the marketplace.

g. Explore the merits and possibilities of enhancing the budget of the existing USM Maryland Industrial Partnerships (MIPS) program for a cyber-related competition. MIPS has a strong track record of connecting USM faculty with industry needs. Taking a portion of the existing fund for a cyber-only competition would help build the cyber industry in Maryland and lead to more cyber-related partnerships.

h. Create a Small Business Innovation Research/Small Business Technology Transfer (SBIR/STTR) effort to link industry with academia in SBIR and STTR funding opportunities.

SBIR and STTR funding from the DOD and other federal agencies remains a significant opportunity for university researchers to form partnerships with industry. A program to facilitate this process, perhaps in concert with the Maryland Technology Development Corporation, should be implemented.

i. Create contests (with prizes) to encourage students and faculty within the USM to address and solve problems of cyber security. Some of these efforts might lead to the start-ups mentioned above. Some might lead to intellectual property that could be licensed to established companies.

## RECOMMENDATION 5. Expand the Career Pipeline

Form a comprehensive partnership between the USM and Maryland Association of Community Colleges (MACC) in cyber security. Create clear pathways for community college students to pursue four-year degrees in a variety of cyber-related fields at institutions across USM. A statewide cyber security 2 + 2 articulation agreement may be considered, mirroring similar agreements in teaching, nursing and engineering. The USM and MACC should activate a coordinating committee to take on the recommendation as an action item. The degree pathways should be described and maintained on the USM and MACC websites and be emphasized by community colleges in their advisement activity.

Clearly, many positions in fields related to cyber security and information assurance require some level of security clearance. The Task Force discussed the difficulties in finding individuals who are eligible for the proper level of security clearance required and feels that institutions may wish to adopt models such as the one employed at the University of Maryland, Baltimore County (UMBC). UMBC advises freshmen who are interested in majoring in areas related to cyber security to be very cognizant of personal issues and actions that may impede their ability to obtain the security clearance needed to be employed in the fields related to cyber security. In addition, to the extent possible, USM institutions should work with the Maryland State Department of Education to disseminate information to high school and even middle school students as to the consequences that certain decisions and activities may have on their future ability to obtain the necessary clearances to become employed in the field of their choice related to cyber security.

# G. Membership of the Task Force »

**Nariman Farvardin, Chairman**
Senior Vice President for Academic Affairs & Provost
University of Maryland, College Park
*farvar@umd.edu*

USM Board of Regents
**Linda Gooden**
Executive Vice President, Information Systems & Global Solutions
Lockheed Martin
*linda.gooden@lmco.com*
301.240.7200

University of Maryland, College Park
**Patrick Gerard O'Shea**
Professor and Chair, Department of Electrical and Computer Engineering
*poshea@umd.edu*
301 405 3683

**Michael W. Hicks**
Associate Professor, Computer Science
*mhicks2@umd.edu*
301.405.2710

**Lawrence A. Gordon**
Professor, Accounting
*lagordon@umd.edu*
301.405.2255

University of Maryland University College
**Greg von Lehmen**
Provost
*gvlehmen@umuc.edu*
301.985.7174

University of Maryland, Baltimore County
**Jack Suess**
Vice President of Information Technology and Chief Information Officer
*jack@umbc.edu*
410.455.2582

University of Maryland, Baltimore
**Reuben Mezrich, M.D.**
Professor and former Chair, Department of Diagnostic Radiology and Nuclear Medicine
*rmezrich@umm.edu*
410.328.3477

University of Baltimore
**Joseph S. Wood**
Provost and Senior Vice President of Academic Affairs
*jswood@ubalt.edu*
410 837 5244

Bowie State University
**Al Valbuena**
Chief Information Officer
*avalbuena@bowiestate.edu*
301.860.3957

Towson University
**Michael O'Leary**
Professor and Director, Center for Applied Information Technology
*moleary@towson.edu*
410.704.4757

National Security Agency
**Boyd Livingston**
Technical Director of Research
*btlivin@alum.mit.edu*
301.688.0701

**David J. Chang**
Deputy Chief, Data Network Technologies Office
*david.chang1@us.army.mil*

Maryland Department of Business and Economic Development
**Adam Suri**
Director
*asuri@ChooseMaryland.org*
410.767.6680

ManTech
**Sally Sullivan**
Executive Vice President, Business Development
*Maggie.Conde-Jimenez@ManTech.com*
703.218.8262

Lockheed Martin
**Retired Air Force Lt. Gen. Charles Croom**
*charles.e.croom@lmco.com*
301.240.6942

Contractor
**Kevin Powderly**
Chairman, CyberCore Technologies
*kpowderly@cybercoretech.com*
410.560.7177

USM Staff
**P.J. Hogan**
*pjhogan@usmd.edu*
301.445.1927

**Suresh Balakrishnan**
*suresh@usmd.edu*
301.445.2783

**Brian Darmody**
*bdarmody@umd.edu*
301.405.1990

**Janice Doyle**
*jdoyle@usmd.edu*
301.445.1906

# Endnotes »


1 | Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency, A Report of the CSIS Commission on Cyber Security for the 44th Presidency,* December 2008.

Government Accountability Office, *National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture*, Testimony before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, U.S. House of Representatives Committee on Homeland Security, March 10, 2009.

Government Accountability Office, *Cybersecurity: Continued Attention Is Needed to Protect Federal Information Systems from Evolving Threats*, Testimony before the U.S. House of Representatives Committee on Homeland Security, June 16, 2010.

Obama, Barack, Remarks by the President on Securing Our Nation's Cyber Infrastructure, available at www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure, May 29, 2010.

Kelliher, Joseph T., Testimony by the Chairman of the Federal Energy Regulatory Commission before the U.S. House of Representatives Committee on Energy and Commerce Subcommittee on Energy and Air Quality, September 11, 2008.

Chabinsky, Steven R., Statement of Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation before the U.S. Senate Judiciary Committee Subcommittee on Terrorism and Homeland Security, November 17, 2009.

Wardrop, Murray and Gardham, Duncan, "*Cyber attack threat 'could be next Pearl Harbor,'*" The Telegraph, October 18, 2010.

2 | Maryland Department of Business and Economic Development, *CyberMaryland*, January 11, 2010.




# Appendix A »

## CYBER SECURITY ACADEMIC PROGRAM INVENTORY

| SCHOOL | DEGREE TITLE | COURSE DESCRIPTIONS LINK |
|---|---|---|
| **BOWIE STATE UNIVERSITY** | B.S. in Technology—Computer Networking and Security | www.bowiestate.edu/UploadedFiles/admissions/2009-2010%20Academic%20Catalog.pdf |
| | B.S. in Technology—Computer Networking and System Administration | www.bowiestate.edu/UploadedFiles/admissions/2009-2010%20Academic%20Catalog.pdf |
| | B.S. in Technology—Data Development and Administration | www.bowiestate.edu/UploadedFiles/admissions/2009-2010%20Academic%20Catalog.pdf |
| | B.S. in Technology—Internet Technology and Multimedia | www.bowiestate.edu/UploadedFiles/admissions/2009-2010%20Academic%20Catalog.pdf |
| | M.S. in Computer Science | www.bowiestate.edu/UploadedFiles/academics/graduate_studies/2009-2010%20Graduate%20Catalog%20Complete.pdf |
| | D.A.S. in Computer Science | www.bowiestate.edu/UploadedFiles/academics/graduate_studies/2009-2010%20Graduate%20Catalog%20Complete.pdf |
| | B.S. in Mathematics—Pure Mathematics | www.bowiestate.edu/UploadedFiles/admissions/2009-2010%20Academic%20Catalog.pdf |
| | B.S. in Mathematics—Applied and Computational | www.bowiestate.edu/UploadedFiles/admissions/2009-2010%20Academic%20Catalog.pdf |
| | M.A. in Mathematics—Applied and Computational | www.bowiestate.edu/UploadedFiles/academics/graduate_studies/2009-2010%20Graduate%20Catalog%20Complete.pdf |
| | M.S. in Information Assurance—Network Security Concentration | www.bowiestate.edu/academics/departments/mis/academic/msia/ |
| | M.S. in Information Assurance—Web Security Concentration | www.bowiestate.edu/academics/departments/mis/academic/msia/ |
| | M.S. in Information Assurance—Information Assets Concentration | www.bowiestate.edu/academics/departments/mis/academic/msia/ |
| **COPPIN STATE UNIVERSITY** | B.S. in Computer Science | www.coppin.edu/MathCOSC/COSCMajor.aspx |
| | B.S. in Mathematics | www.coppin.edu/MathCOSC/MathMajor.aspx |
| **FROSTBURG STATE UNIVERSITY** | B.S. in Computer Information Systems | www.frostburg.edu/dept/pdf/cis.pdf |
| | B.S. in Computer Science | www.frostburg.edu/dept/pdf/comp.pdf |
| | Undergraduate Certificate in Computing Technology | www.frostburg.edu/dept/pdf/comp.pdf#page=3 |
| | Undergraduate Certificate in Networking | www.frostburg.edu/dept/pdf/comp.pdf#page=3 |
| | Undergraduate Certificate in Programming | www.frostburg.edu/dept/pdf/comp.pdf#page=3 |
| | Undergraduate Certificate in Software Development | www.frostburg.edu/dept/pdf/comp.pdf#page=3 |
| | B.S. in Engineering with Electrical Concentration | www.frostburg.edu/dept/engn/pdf/BSEreq.pdf |
| | B.S. in Information Technology | www.frostburg.edu/dept/pdf/infot.pdf |
| | B.S. in Mathematics | www.frostburg.edu/dept/pdf/math.pdf |
| | M.S. in Applied Computer Science | www.frostburg.edu/grad/pdf/2010-2012/110cosc.pdf |

| SCHOOL | DEGREE TITLE | COURSE DESCRIPTIONS LINK |
|---|---|---|
| | B.S./M.S. Collaborative Program in Applied Physics | www.frostburg.edu/dept/pdf/aphysic.pdf |
| | B.S. in Physics | www.frostburg.edu/dept/pdf/physic.pdf |
| **SALISBURY UNIVERSITY** | B.S. in Computer Science | www.salisbury.edu/checklists/2010%20Checklists/Henson%202010-2011/COSC%2010-11.pdf |
| | B.S. in Information Systems | www.salisbury.edu/InfoSys/degree/default.asp |
| | B.S. in Mathematics | www.salisbury.edu/checklists/2010%20Checklists/Henson%202010-2011/MATH%20APPL%2010-11.pdf |
| | B.S. in Physics | www.salisbury.edu/physics/html/phy.html |
| **TOWSON UNIVERSITY** | B.S. in Computer Science—Computer Security | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Computer Science and Mathematics—Computer Security | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | M.S. in Computer Science—Computer Security | grad.towson.edu/program/master/cosc-cmse-ms/dr-cmse.asp |
| | M.S. in Applied Information Technology | grad.towson.edu/program/master/ait-ms/dr-ait-ms.asp |
| | Post-baccalaureate Certificate in Information Security and Assurance | grad.towson.edu/program/certificate/ifsa-pbc/dr-ifsa.asp |
| | M.S. in Integrated Homeland Security Management—Information Assurance | www.towson.edu/main/academics/coursesandcatalogs/documents/GraduateCatalog2010.pdf |
| | B.S. in Computer Science | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Computer Science and Mathematics | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Information Systems | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Information Systems and Business Administration | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Information Systems and e-Business | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Information Technology | www.towson.edu/cosc/InformationTechnology.asp |
| | B.S. in Physics | www.towson.edu/physics/physics/about.asp |
| | B.S. in Mathematics—Pure Mathematics | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in Mathematics—Applied Mathematics | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | B.S. in e-Business | www.towson.edu/main/academics/ugrad/documents/TU_Undergrad_Catalog_2011.pdf |
| | M.S. in Integrated Homeland Security Management | www.towson.edu/main/academics/coursesandcatalogs/documents/GraduateCatalog2010.pdf |
| | D.Sc. in Information Technology | www.towson.edu/main/academics/coursesandcatalogs/documents/GraduateCatalog2010.pdf |
| | M.S. in Applied and Industrial Mathematics | www.towson.edu/main/academics/coursesandcatalogs/documents/GraduateCatalog2010.pdf |
| **UNIVERSITY OF BALTIMORE** | B.S. in Applied Information Technology | www.ubalt.edu/cla_template.cfm?page=1550 |
| | B.S. in Simulation and Digital Entertainment | www.ubalt.edu/cla_template.cfm?page=1623 |
| | B.S. in Information Systems and Technology Management | www.ubalt.edu/template.cfm?page=745 |

| SCHOOL | DEGREE TITLE | COURSE DESCRIPTIONS LINK |
|---|---|---|
| **UNIVERSITY OF MARYLAND, BALTIMORE COUNTY** | B.S. in Computer Science | www.umbc.edu/catalog/2010/display.php?major=18 |
| | B.S. in Computer Engineering | www.umbc.edu/catalog/2010/display.php?major=18 |
| | B.S. in Information Systems | www.umbc.edu/catalog/2010/display.php?major=20 |
| | B.A. in Business Technology Administration | www.umbc.edu/catalog/2010/display.php?major=20 |
| | B.S. in Mathematics | www.umbc.edu/catalog/2010/display.php?major=26 |
| | B.S./B.A. in Physics | physics.umbc.edu/ |
| | Undergraduate Auditing Certificate | www.umbc.edu/catalog/2010/display.php?major=26 |
| | M.S. in Computer Science | www.umbc.edu/gradschool/gradcatalog/programs/computer_science.html |
| | M.S. in Computer Engineering | www.umbc.edu/gradschool/gradcatalog/programs/computer_eng.html |
| | M.S. in Electrical Engineering | www.umbc.edu/gradschool/gradcatalog/programs/electrical |
| | M.S. in Information Systems | www.is.umbc.edu |
| | M.P.S. in Cybersecurity | www.umbc.edu/gradschool/gradcatalog/programs/cybr.html |
| | M.S. in Engineering Management | www.umbc.edu/gradschool/gradcatalog/programs/engineering_ |
| | M.S. in Systems Engineering | www.umbc.edu/gradschool/gradcatalog/programs/sys_eng.html |
| | Master's Certificate in Cybersecurity Strategy and Policy | www.umbc.edu/cyber/programcert.html |
| | Ph.D. in Computer Science | www.umbc.edu/gradschool/gradcatalog/programs/computer_science.html |
| | Ph.D. in Computer Engineering | www.umbc.edu/gradschool/gradcatalog/programs/computer_science |
| | Ph.D. in Information Systems | www.is.umbc.edu |
| **UNIVERSITY OF MARYLAND, COLLEGE PARK** | B.S. in Computer Science | undergrad.cs.umd.edu/current-students/degree-requirements-for-cs-major/ |
| | Minor in Computer Science | undergrad.cs.umd.edu/current-students/degree-requirements-for-cs-minor/ |
| | M.S. in Computer Science | www.cs.umd.edu/Grad/policy-manual.shtml#7.MS-degree-requirements |
| | Ph.D. in Computer Science | www.cs.umd.edu/Grad/policy-manual.shtml#8.PhD-degree-requirements |
| | B.S. in Computer Engineering | www.ece.umd.edu/Academic/Under/encp.html |
| | Combined B.S./M.S. in Electrical and Computer Engineering | www.ece.umd.edu/Academic/Grad/BS_MS/index.php |
| | B.S. in Electrical Engineering | www.ece.umd.edu/Academic/Under/bsee.html |
| | M.S. in Electrical Engineering | www.ece.umd.edu/gradhandbook/5.php3 |
| | Ph.D. in Electrical Engineering | www.ece.umd.edu/gradhandbook/6.php3 |
| | M.S. in Telecommunications | www.telecom.umd.edu/current/degreereqs |
| | M.Eng. In Computer Engineering | www.oaee.umd.edu/grad/enee.html |
| | M.Eng. In Communications and Signal Processing | www.oaee.umd.edu/grad/enee.html |
| | Graduate Certificate in Engineering—Computer Engineering | www.oaee.umd.edu/grad/enee.html |
| | Graduate Certificate in Engineering—Communications and Signal Processing | www.oaee.umd.edu/grad/enee.html |
| | Graduate Certificate in Engineering—Software Engineering | www.oaee.umd.edu/grad/enee.html |
| | B.S. in Mathematics | www.math.umd.edu/undergraduate/majors/CourseRequirements.html |
| | Combined B.S./M.S. in Mathematics | www.math.umd.edu/undergraduate/majors/bsma.html |
| | Minor in Mathematics | www.math.umd.edu/undergraduate/opportunities/minors.html |
| | M.A. in Mathematics | www.math.umd.edu/graduate/programs/math.policies.html |

| SCHOOL | DEGREE TITLE | COURSE DESCRIPTIONS LINK |
|---|---|---|
| | Ph.D. in Mathematics | www.math.umd.edu/graduate/programs/math.policies.html |
| | B.S. in Business | www.rhsmith.umd.edu |
| | M.B.A. | www.rhsmith.umd.edu/mba/ |
| | M.S. in Human-Computer Interaction | ischool.umd.edu/content/hcim |
| | Master of Information Management | ischool.umd.edu/content/mim-cp |
| | M.S. in Systems Engineering | www.isr.umd.edu/students/msse.htm |
| | Master of Public Policy | www.publicpolicy.umd.edu/degree-programs/master-of-public-policy |
| | B.S. in Physics | umdphysics.umd.edu/ |
| | M.S. in Physics | www.gradschool.umd.edu/catalog/courses/phys.htm |
| | Ph.D. in Physics | www.gradschool.umd.edu/catalog/courses/phys.htm |
| | M.S., Ph.D., Certificates in Applied Mathematics | www.amsc.umd.edu/programs/ |
| **UNIVERSITY OF MARYLAND EASTERN SHORE** | B.S. in Mathematics | www.umes.edu/MCS/Content.aspx?id=23390 |
| | B.S. in Electrical Engineering | www.umes.edu/MCS/Content.aspx?id=23390 |
| | B.S. in Engineering Technology | www.umes.edu/Engineering/Default.aspx?id=12538 |
| | B.S. in Computer Science | www.umes.edu/MCS/Content.aspx?id=23390 |
| | M.S. in Applied Computer Science | www.umes.edu/MCS/Content.aspx?id=23390 |
| **UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE** | M.S. in Cybersecurity | www.umuc.edu/programs/grad/csec/index.shtml |
| | M.S. in Cybersecurity Policy | www.umuc.edu/programs/grad/csec/policy.shtml |
| | M.S. in Information Technology—Information Assurance | www.umuc.edu/programs/grad/msit/information_systems_assurance.shtml |
| | Post-baccalaureate Certificate—Foundations of Cybersecurity | www.umuc.edu/programs/grad/certificates/cs_foundations.shtml |
| | Post-baccalaureate Certificate—Cybersecurity Technology | www.umuc.edu/programs/grad/certificates/cs_technology.shtml |
| | Post-baccalaureate Certificate—Cybersecurity Policy | www.umuc.edu/programs/grad/certificates/cs_policy.shtml |
| | B.S. in Cybersecurity | www.umuc.edu/programs/undergrad/csia/index.shtml |
| | B.S. in Computer Information Technology | www.umuc.edu/programs/undergrad/cmit/ |
| | B.S. in Computer Science | www.umuc.edu/programs/undergrad/cmsc/ |
| | Undergraduate Certificate in Information Assurance | www.umuc.edu/programs/undergrad/certificates/info_assurance.shtml |

# CYBER SECURITY DEGREES AND CERTIFICATES AWARDED 2009–10 ACADEMIC YEAR

## Overview by Institution

| SCHOOL | BACHELOR'S | MASTER'S | DOCTORAL | UG CERTIFICATE | GR CERTIFICATE | TOTAL |
|---|---|---|---|---|---|---|
| **BOWIE STATE UNIVERSITY** | 6 | 31 | 0 | 0 | 0 | 37 |
| **COPPIN STATE UNIVERSITY** | 7 | 0 | 0 | 0 | 0 | 7 |
| **FROSTBURG STATE UNIVERSITY** | 17 | 5 | 0 | 2 | 0 | 24 |
| **SALISBURY UNIVERSITY** | 55 | 0 | 0 | 0 | 0 | 55 |
| **TOWSON UNIVERSITY** | 154 | 77 | 9 | 0 | 27 | 267 |
| **UNIVERSITY OF BALTIMORE** | 52 | 0 | 0 | 0 | 0 | 52 |
| **UNIVERSITY OF MARYLAND BALTIMORE COUNTY** | 337 | 54 | 11 | 0 | 0 | 402 |
| **UNIVERSITY OF MARYLAND, COLLEGE PARK** | 425 | 279 | 92 | 0 | 25 | 821 |
| **UNIVERSITY OF MARYLAND EASTERN SHORE** | 17 | 9 | 0 | 0 | 0 | 26 |
| **UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE** | 203 | 264 | 0 | 24 | 2 | 493 |
| **TOTAL** | **1273** | **719** | **112** | **26** | **54** | **2184** |

## Overview by Area

| SCHOOL | TECHNICAL | CYBER POLICY | OTHER PROGRAMS | |
|---|---|---|---|---|
| **BOWIE STATE UNIVERSITY** | 37 | 0 | 0 | |
| **COPPIN STATE UNIVERSITY** | 7 | 0 | 0 | |
| **FROSTBURG STATE UNIVERSITY** | 24 | 0 | 0 | |
| **SALISBURY UNIVERSITY** | 55 | 0 | 0 | |
| **TOWSON UNIVERSITY** | 251 | 0 | 16 | |
| **UNIVERSITY OF BALTIMORE** | 52 | 0 | 0 | |
| **UNIVERSITY OF MARYLAND BALTIMORE COUNTY** | 351 | 0 | 51 | * |
| **UNIVERSITY OF MARYLAND, COLLEGE PARK** | 664 | 31 | 126 | |
| **UNIVERSITY OF MARYLAND EASTERN SHORE** | 26 | 0 | 0 | * |
| **UNIVERSITY OF MARYLAND UNIVERSITY COLLEGE** | 491 | 2 | 0 | ** |
| **TOTAL** | **1958** | **33** | **193** | |

* UMBC lists Master's of Engineering Management in both the technical and other groups, in the aggregated statistics it appears in the technical category only.

** Both UMBC and UMUC have new cyber security degrees and certificates that will start producing graduates in 2012-13.

# Appendix B »

## DETAILS OF RESEARCH ACTIVITIES AT SELECTED USM INSTITUTIONS

### UNIVERSITY OF MARYLAND, COLLEGE PARK

#### Theoretical Foundations of Cyber Security

University of Maryland (UMCP) researchers employ mathematical analysis of security problems in designing and analyzing cryptographic protocols and tools, and advanced concepts such as quantum computing and quantum cryptography. This research includes the development of exposure-resistant cryptosystems that could remain secure, even if the secret key is exposed. The threat of key exposure is becoming more acute as cryptographic algorithms are increasingly deployed on small, mobile and easily compromised devices.

**J. Robert Anderson, Professor, Physics**
*umdphysics.umd.edu/about-us/people/faculty/111-anderson.html*
Quantum computing using superconducting devices; magnetic semiconductors. Current active funding: $4,700,000

**Alexander Barg, Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.ece.umd.edu/~abarg/*
Coding theory, cryptographic primitives and protocols, information theory, discrete mathematics, anti-collusion fingerprinting, information-theoretic security. Current active funding: $800,000

**Jonathan Katz, Associate Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies**
*www.cs.umd.edu/~jkatz/*
Cryptography, computer and network security, theoretical computer science. Current active funding: $1,700,000

**Christopher Lobb, Professor, Physics**
*umdphysics.umd.edu/about-us/people/faculty/169-lobb.html*
Quantum computing using superconducting devices, phase transitions in superconductors, properties of Josephson-junction arrays, single-electron transistors. Current active funding: $6,700,000

**Christopher Monroe, Bice Zorn Professor, Physics**
*umdphysics.umd.edu/about-us/people/faculty/178-monroe.html*
Quantum computing objects for factoring the extremely large numbers that serve as the "public keys" in current encryption and data-protection schemes. Current active funding: $1,500,000

**Prakash Narayan, Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.ece.umd.edu/~prakash/*
Network information and coding theory, information theoretic network security, cryptography, communication theory, information theory and statistics, statistical signal processing. Current active funding: $600,000

**Steven L. Rolston, Professor, Physics**
*jqi.umd.edu/*
Ultracold plasmas, quantum information, optical lattices, quantum computation. Current active funding: $15,900,000

**Aravind Srinivasan, Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies**
*www.cs.umd.edu/~srin/*
Network modeling; algorithms, randomized computation and combinatorial optimization; networking and distributed algorithms; social networks and epidemiology. Current active funding: $800,000

**Uzi Vishkin, Professor, Electrical and Computer Engineering/ University of Maryland Institute for Advanced Computer Studies**
*www.umiacs.umd.edu/~vishkin/index.shtml*
Parallelism in computing, design and analysis of algorithms, parallel computer architecture, pattern matching, security under concurrency. Current active funding: $700,000

**Edo Waks, Assistant Professor, Electrical and Computer Engineering**
*www.ece.umd.edu/meet/faculty/waks.php3*
Secure quantum communication and quantum networking, quantum computation, semiconductor and photonic implementations of quantum technology. Current active funding: $2,000,000

**Frederick Wellstood, Professor, Physics**
*umdphysics.umd.edu/about-us/people/faculty/149-wellstood.html*
Quantum computing using superconducting devices. Current active funding: $1,000,000

## Cyber Supply Chain Security

The cyber supply chain can be described as the mass of IT systems—hardware, software and public and classified networks—that together enable the uninterrupted operations of government agencies, companies and international organizations. Attacks on the cyber supply chain can include malware inserted into software or hardware, vulnerabilities found by hackers, as well as compromised systems that are unwittingly brought in-house. Cyber supply chain protection requires new levels of collaboration among security, IT and supply chain managers, taking into account the roles of developers, vendors, customers and users.

**Sandor Boyson, Research Professor, Robert H. Smith School of Business/Institute for Systems Research**
*rhsmith.umd.edu/lbpp/faculty/boyson.aspx*
Cyber-supply chain risk management, logistics best practices, net-centricity management practices. Current active funding: $90,000

**Howard Frank, Professor and Former Dean, Robert H. Smith School of Business**
*www.smith.umd.edu/about/leadership/pastdeans/HowardFrank.aspx*
Information technology, supply chain management, e-commerce

## Cyber Security Policy

The Center for International Security Studies at Maryland (CISSM) is attempting to develop and circulate suggestions for protective cyber security regulation—namely, formal prohibition of destructive attacks on critical infrastructure assets supported by mutually developed protocols for robust defense. The term critical infrastructure would include power grids, air traffic control systems, financial market operations, emergency response systems and hospitals. This arrangement would be a partial solution to the global problem, but it could provide meaningful protection against the most destructive possibilities and lay the groundwork for more comprehensive cooperation in the future.

**Kenneth R. Fleischmann, Associate Professor, College of Information Studies**
*www.ischool.umd.edu/people/fleischmann/*
Role of human values in the design and use of information technology; simulations and modeling; computational social science; computing and information ethics education; ethics of cyber security research, education and practice. Current active funding: $400,000

**Jacques Gansler, Professor and Roger C. Lipitz Chair, School of Public Policy**
*www.publicpolicy.umd.edu/directory/gansler*
National security, globalization, supply chain management, information systems. Current active funding: $4,900,000

**Paul Jaeger, Assistant Professor, College of Information Studies**
*ischool.umd.edu/provost/jaeger.shtml*
Information law and policy, e-government, access for underserved populations, and social theory of information. Current active funding: $700,000

**William Lucyshyn, Director of Research and Senior Research Scholar, Center for Public Policy and Private Enterprise**
*www.publicpolicy.umd.edu/directory/lucyshyn*
Cyber security policy and cyber supply chain, economics of cyber security

**Christopher McGoff, Professor, School of Public Policy**
*www.puaf.umd.edu/directory/mcgoff/*
Coordinating disaster response, cyber security policy

**William Nolte, Research Professor, School of Public Policy**
*www.publicpolicy.umd.edu/directory/nolte*
Intelligence, homeland security, intelligence/policy relationships. Current active funding: $600,000

**Matthias Ruth, Professor and Director, Center for Integrative Environmental Research, Co-director of the Master's in Engineering and Public Policy Program, School of Public Policy**
*www.publicpolicy.umd.edu/directory/ruth*
Cyber security economics and policy. Current active funding: $1,200,000

**John Steinbruner, Professor and Director, Center for International Security Studies, School of Public Policy**
*www.cissm.umd.edu/people/profile.php?id=1*
Cyber security policy. Current active funding: $200,000

## Digital Forensics

University of Maryland researchers are developing more secure ways to transmit data, particularly multimedia files such as digital images and videos. They are working to ensure that authentic information is delivered and used only by authorized users for authorized purposes.

**Rama Chellappa, Minta Martin Professor of Engineering, Electrical and Computer Engineering/University of Maryland Institute for Advanced Computer Studies**

*www.cfar.umd.edu/~rama/*

Computer vision and image processing; signal and image processing, robust and secure biometrics; pattern recognition; statistical inference; computer vision and image analysis; AI in computer vision; neural networks for computer vision. Current active funding: $1,700,000

**Carol Espy-Wilson, Professor, Electrical and Computer Engineering/Institute for Systems Research**

*terpconnect.umd.edu/~espy*

Speech forensics; automatic extraction of forensic evidence from speech recordings (e.g., speaker recognition, acquisition device identification); content authentication from speech recordings (e.g., tampering detection, time-stamping based on power network interference). Current active funding: $1,000,000

**K.J. Ray Liu, Distinguished Scholar-Teacher, Professor and Associate Chair for Graduate Studies and Research, Electrical and Computer Engineering**

*www.cspl.umd.edu/kjrliu/*

Wireless communications and networking; multimedia communications and signal processing; information forensics and security; biomedical imaging and bioinformatics; and signal processing algorithms and architectures. Current active funding: $700,000

**Min Wu, Associate Professor, Electrical and Computer Engineering/ University of Maryland Institute for Advanced Computer Studies**

*www.ece.umd.edu/~minwu/*

Information forensics and security; multimedia data and device forensics; tampering and forgery detection; content protection, anti-collusion fingerprinting and traitor tracing; multimedia data hiding; privacy/confidentiality preserving search of information; software and hardware co-design for trusted computing platform. Current active funding: $1,100,000

## Economics of Cyber Security

While some organizations have vast security resources, business executives must often make security decisions based on cost. Economists from the Robert H. Smith School of Business have developed quantitative methods that can inform these important decisions.

**Lawrence A. Gordon, Ernst & Young Alumni Professor, Robert H. Smith School of Business/University of Maryland Institute for Advanced Computer Studies**

*www.rhsmith.umd.edu/faculty/lgordon/index.htm*

Cyber security economics, information security, cyber security risk management.

**Martin Loeb, Professor and Deloitte & Touche Faculty Fellow, Robert H. Smith School of Business**

*www.rhsmith.umd.edu/faculty/mloeb/*

Accounting and information assurance, cyber security economics and regulation.

## Software Security

UMCP researchers are working on code analysis and code development, creating interfaces, tools and analytic programs that allow programmers to write code that minimizes security flaws. The work aims to provide developers with instant feedback that audits code for potential threats as they write it, so security vulnerabilities are identified early in the development process. Researchers are also developing software architecture that improves the security and performance of distributed computing. They are designing a multilevel security scheme that automatically adjusts data and code according to the degree of trust established between systems.

**Jeff Foster, Associate Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies**

*www.cs.umd.edu/~jfoster/*

Software security, web security, program analysis, language-based security. Current active funding: $800,000

**Michael Hicks, Associate Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies**

*www.cs.umd.edu/~mwh/*

Software security, web security, program analysis, language-based security, system security. Current active funding: $1,400,000

**Carl Landwehr, Senior Research Scientist, Institute for Systems Research**

*www.isr.umd.edu/faculty/gateways/landwehr.htm*

Computer security, editor-in-chief of IEEE *Security & Privacy* magazine; trustworthy computing, including high-assurance software

development, understanding software flaws and vulnerabilities, token-based authentication, system evaluation and certification methods, multilevel security and architectures for intrusion-tolerant systems

**Ankur Srivastava, Associate Professor, Electrical and Computer Engineering, Institute for Systems Research**
*www.ece.umd.edu/~ankurs/*
Developing adaptable computer systems that can learn about the nature of attack and autonomously modify design and behavior. Current active funding: $1,000,000

## Threat Analysis and Quantification

UMCP researchers analyze incident data using software reliability models, time series and epidemiological models to predict incident trends. Intrusion detection system alerts are analyzed to identify low and slow attacks, as well as other attacks that security administrators cannot identify solely by reviewing the ranking of the most frequent event occurrences. The developed methods can be integrated into an automated graphical user interface-based central monitoring system.

**Michel Cukier, Associate Professor, Reliability Engineering/ Institute for Systems Research**
*www.enre.umd.edu/faculty/cukier.htm*
Malware, quantification of cyber security, malcode analysis, intrusion detection system evaluation, honeypots, network security, security data collection and analysis. Current active funding: $300,000

**David Yates, Assistant Professor, College of Information Studies**
*ischool.umd.edu/people/yates/*
Social aspects of privacy and security, organizational use of collaborative technologies for innovation, social creativity and social influence in virtual contexts.

## Wireless Network Security

UMCP researchers oversee projects ranging from wireless networking security to trustworthy computing and traditional operating systems security. One project is the development of secure "co-pilot" systems: independent auditing platforms that can detect and respond to security violations. These auditors are hard-wired into independent embedded processors, which allow them to react to problems even if a network host is compromised. Programmed with sophisticated event-recognition policies, these prescient "oracles" can predict the onset of an attack based on triggering events in network traffic. In this way, a co-pilot system can respond at the initial signs of an attack before a virus or worm can compromise critical components.

**Ashok K. Agrawala, Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies/Electrical and Computer Engineering**
*www.cs.umd.edu/users/agrawala/index.shtml*
Design and evaluation of systems, real time systems, networks, wireless systems, system integration, information dynamics, location determination, synchronization. Current active funding: $200,000

**William A. Arbaugh, Associate Professor, Computer Science/ University of Maryland Institute for Advanced Computer Studies**
*www.cs.umd.edu/~waa/UMD/Home.html*
Wireless networks; information system security, embedded systems, operating systems, and networking. Current active funding: $200,000

**John S. Baras, Professor, Electrical and Computer Engineering/ Institute for Systems Research**
*www.isr.umd.edu/~baras/*
Network security; security and information assurance in wireless networks; key generation and management for group communications; trust dynamics and management; trust and social networks over the Web, high-integrity recommendation and reputation systems; security metrics; mathematical modeling of multiple security and other performance metrics in networks; malware detection; virus dynamics and defenses against them. Current active funding: $9,300,000

**Bobby Bhattacharjee, Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies**
*www.cs.umd.edu/~bobby/*
Network security, social network privacy. Current active funding: $1,000,000

**Anthony Ephremides, Cynthia Kim Eminent Professor of Information Technology, Electrical and Computer Engineering/Institute for Systems Research**
*www.ece.umd.edu/ephremides/*
Wireless security; covert channels and wireless information-theoretic security. Current active funding: $1,000,000

**Victor Granatstein, Professor, Electrical and Computer Engineering**
*www.ece.umd.edu/faculty/vlg.html*
Physical layer security; detection and mitigation of upsets initiated by external RF signals that impact device level functions. Current active funding: $2,300,000

**Jeff Hollingsworth, Professor and Associate Chair, Computer Science/University of Maryland Institute for Advanced Computer Studies/Electrical and Computer Engineering**
*www.cs.umd.edu/users/hollings/*

Parallel computing, operating systems, distributed systems, auto-tuning software, software engineering for high performance computing, mining software repositories. Current active funding: $2,200,000

**Mehdi Kalantari Khandani, Assistant Research Scientist, Electrical and Computer Engineering**
*www.ece.umd.edu/meet/faculty/research/kalantari.php3*
Distributed Denial of Service (DDOS) attacks; ultrafast detection of DDOS attack on high-bandwidth traffic. Current active funding: $500,000

**P.S. Krishnaprasad, Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.isr.umd.edu/~krishna/*
Control and signal processing; networked physical systems; collective behavior; evolutionary games; strategies for cyber physical security. Current active funding: $400,000

**Richard Hyong-Jun La, Associate Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.enee.umd.edu/~hyongla*
Communication networks, including anomaly detection, game theory, complex networks. Current active funding: $700,000

**Armand Makowski, Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.isr.umd.edu/People/faculty/Makowski.html*
Wireless security, wireless sensor networks. Current active funding: $400,000

**Neil Spring, Assistant Professor, Computer Science/University of Maryland Institute for Advanced Computer Studies**
*www.cs.umd.edu/~nspring/*
Privacy in social networks, social networking, wireless networks. Current active funding: $1,300,000

**Sennur Ulukus, Associate Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.ece.umd.edu/meet/faculty/ulukus.php3*
Wireless network security; information-theoretic security; physical-layer security; Information theory, communication theory and signal processing used to secure wireless communication networks in the physical layer. Current active funding: $1,200,000

**Mikhail Vorontsov, Research Professor, Institute for Systems Research**
*www.iol.umd.edu/People/person.php?id=mvorontsov*
Optical communications (physical layer), adaptive optics, imaging through turbulence, laser beam control, computer optics, nonlinear spatio-temporal dynamics, wavefront sensing and control, parallel image processing and correction, optical synergetics. Current active funding: $400,000

## Understanding Motivations for Cyber Crime

Motivations for cyber attacks can range from identity theft to financial gain to vengeance to vandalism. This research provides an experimental method for studying cyber attacks and understanding attackers' motivations by designing in advance targets likely to attract offenders with specific motivations. By studying the frequency of attacks, entry points, attack methods and resiliency of attackers, UMCP researchers are developing etiological explanations for different types of cybercrime.

**Gary LaFree, Professor and Director, National Consortium for the Study of Terrorism and Responses to Terrorism (START)**
*www.start.umd.edu/start/*
Behavioral and social aspects of cyber criminals. Current active funding: $15,400,000

**David Maimon, Professor, Criminology and Criminal Justice**
*www.ccjs.umd.edu/faculty/faculty.asp?p=209*
Behavioral and social aspects of cyber criminals.

## Behavioral Aspects of Cyber Security

UMCP researchers are exploring trusted systems and social networks, and analyzing how people use online social networks like Twitter and Facebook. This analysis examines how information spreads through social networks, how users behave in social networks and the dynamics of human-computer interaction.

**Jennifer Golbeck, Assistant Professor, College of Information Studies**
*www.cs.umd.edu/~golbeck/*
Social networks, trust, intelligent systems, semantic web. Current active funding: $900,000

**Jonathan Z. Simon, Associate Professor, Electrical and Computer Engineering/Biology**
*www.isr.umd.edu/Labs/CSSL/*
Audio CAPTCHAS, human vs. bot detection using sounds, automated challenge-response tests. Current active funding: $1,700,000

### Systems Security

Cyber attackers are well-organized and -financed, and increasingly sophisticated in their approaches. UMCP researchers are looking at new approaches to security at a systems level. Much of this research focuses on systemwide solutions for secure information transfer in a network through the development of a rigorous theoretical framework for the evaluation of security policies and adversarial attacks against them. Concrete methods for detecting and countering such attacks are validated by software experimentation.

**Carl Landwehr, Senior Research Scientist, Institute for Systems Research**
*www.isr.umd.edu/faculty/gateways/landwehr.htm*
Computer security, editor-in-chief of IEEE *Security & Privacy* magazine; trustworthy computing, including high assurance software development, understanding software flaws and vulnerabilities, token-based authentication, system evaluation and certification methods, multilevel security and architectures for intrusion tolerant systems

**Ali Mosleh, Professor, Mechanical Engineering**
*www.enme.umd.edu/facstaff/fac-profiles/mosleh.html*
Methodology for information systems security risk management. Current active funding: $500,000

**Prakash Narayan, Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.ece.umd.edu/~prakash/*
Network information and coding theory, information theoretic network security, cryptography, communication theory, information theory and statistics, statistical signal processing. Current active funding: $700,000

**Gang Qu, Associate Professor, Electrical and Computer Engineering/Institute for Systems Research**
*www.ece.umd.edu/~gangqu/*
Research data security; technical protection of intellectual property; watermarking and information hiding; hardware-assisted security systems; trustworthy computing and design of trusted integrated circuits and systems; energy-efficient implementation of security protocols and systems. Current active funding: $100,000

**Donald Riley, Professor, Robert H. Smith School of Business**
*www.rhsmith.umd.edu/faculty/driley/riley.htm*
High-performance networks, information systems security management, information assurance and network security

## UNIVERSITY OF MARYLAND, BALTIMORE COUNTY

### Systems, Sensors and Network-Level Issues

Securing our cyber infrastructure must start with securing the communication networks, the operating systems of the processors they connect and the sensors that provide them with data. This is true for both traditional wired and wireless networks as well as emerging modalities such as near-field communication systems.

**Gary Carter, Professor, Electrical Engineering**
*www.cs.umbc.edu/people/faculty/gary-m-carter/*
High-speed/long-distance optical communications, photonics, optoelectronics.

**Anupam Joshi, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/anupam-joshi/*
Security and privacy issues related to mobility, sensor networks, ad-hoc networks.

**Kostas Kalpakis, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/konstantinos-kalpakis/*
Security and information management in federated multimedia systems; ad-hoc networks; sensor networks.

**Curtis Menyuk, Professor, Electrical Engineering**
*www.cs.umbc.edu/people/faculty/curtis-r-menyuk/*
Optical fiber communications and switching; solid-state device simulations; nonlinear optics.

**Dhananjay Phatak, Associate Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/dhananjay-phatak/*
Security and performance of mobile, ad-hoc and high-performance computing networks.

**Deepinder Sidhu, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/deepinder-sidhu/*
Network protocols; security; distributed computing and systems; mobile agents.

**Gymama Slaughter, Assistant Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/gymama-slaughter/*
Biologically inspired computing; wireless networks and communication; sensor networks.

**Mohamed Younis, Associate Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/mohamed-younis/*
Wireless and sensor networks; embedded systems; fault-tolerant computing.

**Yelena Yesha, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/yelena-yesha/*
Distributed computing and assured information systems.

## Machine-Understandable Policy Issues

Hard-coded rules to manage security, confidentiality and trust can lead to rigid and inflexible systems that are hard to understand, difficult to maintain and unable to adapt to their environments and context. Systems that are driven by high-level, executable policies promise to reduce these problems and produce adaptable systems that can evolve with changing situations.

**Tim Finin, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/tim-finin/*
The application of AI, the semantic Web and intelligent agents to create intelligent interfaces and autonomous systems.

**Anupam Joshi, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/anupam-joshi/*
The use of AI, the semantic Web and intelligent agents to support automated policy enforcement in intelligent networked systems, particularly mobile computing.

## Algorithms and Formal Models

Better modeling and analysis of large-scale networks—communication, social or belief—require the development of appropriate formal models and new algorithms that operate on them.

**Richard Chang, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/richard-chang/*
Computational complexity theory.

**John Dorband, Research Associate Professor, Computer Science**
*www.cs.umbc.edu/people/research-faculty/john-e-dorband/*
Application of high-performance and parallel computing to scientific problems.

**Tim Finin, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/tim-finin/*
Machine learning and artificial intelligence.

**Hillol Kargupta, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/hillol-kargupta/*
Algorithm and experimental system development of distributed and ubiquitous data mining.

**Yun Peng, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/yun-peng/*
Probablistic reasoning in the semantic Web and intelligent systems.

**Sridevi Sampath, Assistant Professor, Information Systems**
*userpages.umbc.edu/~sampath/*
Software verification and testing; software engineering.

**Yaacov Yesha, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/yaacov-yesha/*
Algorithms for parallel computing, computational complexity and distributed systems.

## Trojans, Trusted Platforms and Hardware Security

Secure computer systems must be secured from the ground up, starting with the hardware itself and working up the stack to create a trusted platform free of serious malware like trojans and root kits.

**Chintan Patel, Asst. Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/chintan-patel/*
VLSI design and embedded systems.

**Dhananjay Phatak, Associate Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/dhananjay-phatak/*
Mobile and high-performance computing and networks, algorithms, architectures and their VLSI implementations.

**John Pinkston, Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/john-pinkston/*
Cryptography; information and coding theory; signal processing.

**Ryan Robucci, Assistant Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/ryan-robucci/*

**Alan Sherman, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/alan-t-sherman/*
Security of voting systems; cryptology; information assurance; discrete algorithms.

## Privacy and Trust Issues in Cyber Security

Privacy and trust are important aspects of security that are often multidimensional, application-dependent and sensitive to context. Modeling and reasoning about the concepts often require significant computation and analysis.

**Zhiyuan Chen, Associate Professor, Information Systems**
*userpages.umbc.edu/~zhchen/*
Privacy-preserving data mining and data management.

**Tim Finin, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/tim-finin/*
The application of AI, the semantic Web and intelligent agents to enhance privacy and trust.

**Aryya Gangopadhyay, Professor, Information Systems**
*sites.google.com/site/homearyya/*
Privacy preserving data mining, knowledge discovery in structured and unstructured data, health information systems.

**Anupam Joshi, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/anupam-joshi/*
The application of AI, the semantic Web and intelligent agents to enhance privacy and trust, especially in mobile systems.

**Hillol Kargupta, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/hillol-kargupta/*
Privacy-preserving data mining; privacy in multiparty-distributed data mining.

**Ant Ozok, Associate Professor, Information Systems**
*userpages.umbc.edu/~ozok/*
Human-centered computing, cross-cultural usability, e-commerce, mobile commerce, survey design, online communities.

**A. Gunes Koru, Associate Professor, Information Systems**
*koru.ifsm.umbc.edu:8080/Plone*
Privacy-preserving data mining; open-source software engineering.

## Cryptography and Quantum Security

Cryptography provides the foundation for much of today's security and privacy technology. Novel algorithms, protocols and attacks are being studied for new applications and end-to-end scenarios. Quantum cryptography is exploring the use of quantum computations to perform cryptographic tasks or to break cryptographic systems.

**Sam Lomonaco, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/samuel-lomonaco/*
Quantum computation, topology and other areas of computer science and mathematics.

**Alan Sherman, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/alan-t-sherman/*
Security of voting systems; cryptanalysis; applications of cryptography; information assurance education; theoretical foundations of cryptology.

**A. Brooke Stephens, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/brooke-stephens/*
Numerical analysis; cryptography; distributed systems.

## Usable and Accessible Cyber Security

Security and privacy mechanisms in user-oriented systems must be easy to understand and use or risk introducing new vulnerabilities. Developing intuitive security frameworks, visualization techniques and easy-to-use interfaces is extremely important.

**Amy Hurst, Assistant Professor, Information Systems**
*www.amyhurst.com/*
Intelligent user interface, human-centered computing, accessibility.

**Ravi Kuber, Assistant Professor, Information Systems**
*userpages.umbc.edu/~rkuber/*
Human-centered computing, universal access to technology, haptic and multimodal interface design and evaluation.

**Andrew Sears, Professor, Information Systems**
*userpages.umbc.edu/~asears/*
Human-centered computing, universal access to technology, interface design, mobility.

**Zeynep Tufekci, Assistant Professor, Sociology and Anthropology**
*userpages.umbc.edu/~zeynep/*
Social impacts of technology, privacy, social media.

## Secure and Verifiable Voting

**Donald F. Norris, Professor, Public Policy**
*www.umbc.edu/pubpol/dnorris.php*
Public policy, government information technology systems, secure voting methods.

**Dhananjay Phatak, Associate Professor, Computer Engineering**
*www.cs.umbc.edu/people/faculty/dhananjay-phatak/*
Mobile and high-performance computing and networks, algorithms, architectures and their VLSI implementations.

**Alan Sherman, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/alan-t-sherman/*
Security of voting systems, cryptanalysis, applications of cryptography, information assurance education, theoretical foundations of cryptology.

## Threat Visualization

Humans are very good at detecting visual patterns. Fast parallel processing and appropriate data visualization techniques allow people to quickly find trends, patterns and anomalies in large security-related data sets.

**Anita Komlodi, Associate Professor, Information Systems**
*userpages.umbc.edu/~komlodi/*
Human-centered computing, information storage and retrieval; computer-supported cooperative work.

**Wayne Lutters, Associate Professor, Information Systems**
*userpages.umbc.edu/~lutters/*
Computer-supported cooperative work, human-centered computing, knowledge management, online communities.

**Marc Olano, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/marc-olano/*
Interactive computer graphics.

**Penny Rheingans, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/penny-rheingans/*
Visualization techniques to represent large amounts of information using color, texture, motion, and interactivity

## Analytics for Unstructured Data and Social Media

The data underlying intelligence and cyber security problems are often provided in unstructured or semistructured forms as graphs, text, images or video. Novel techniques are required to represent, manage and process such data.

**Zhiyuan Chen, Associate Professor, Information Systems**
*userpages.umbc.edu/~zhchen/*
Privacy-preserving data mining and data management.

**Marie desJardins, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/marie-desjardins/*
Machine learning, planning, multi-agent systems, interactive AI techniques, information management, reasoning with uncertainty, decision theory.

**Aryya Gangopadhyay, Professor, Information Systems**
*sites.google.com/site/homearyya/*
Privacy-preserving data mining, knowledge discovery in structured and unstructured data, health information systems.

**Vandana Janeja, Assistant Professor, Information Systems**
*userpages.umbc.edu/~vjaneja/*
Data mining, anomaly detection, spatial databases.

**Anupam Joshi, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/anupam-joshi/*
The use of AI, the semantic Web and intelligent agents to analyze social media information to aid in decision making.

**George Karabatis, Associate Professor, Information Systems**
*userpages.umbc.edu/~georgek/*
Database systems, semantic integration of enterprise systems, data integration, mobile data management.

**Kotas Kalpakis, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/konstantinos-kalpakis/*
Using analytics from ad-hoc networks, sensor networks, multimedia systems, and federated systems for security and information management.

**Hillol Kargupta, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/hillol-kargupta/*
Privacy-preserving data mining; privacy in multiparty-distributed data mining.

**Tim Oates, Associate Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/tim-oates/*
Machine learning, robotics, artificial intelligence.

**Yun Peng, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/yun-peng/*
Probablistic reasoning in the semantic Web and intelligent systems.

**Dongsong Zhang, Associate Professor, Information Systems**
*userpages.umbc.edu/~zhangd/*
Information extraction and retrieval; information personalization and privacy; mobility.

**Lina Zhou, Associate Professor, Information Systems**
*userpages.umbc.edu/~zhoul/*
Deception detection, intelligent user interfaces, social network analysis.

## Information Extraction and Retrieval from Speech and Text

Much intelligence information is found in by analyzing the natural language found in text and spoken language. Natural language processing techniques are employed to automatically recognize and extract the entities, relations and facts encoded in these sources, providing data to populate knowledge bases and drive further analysis.

**Tim Finin, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/tim-finin/*
Machine learning and artificial intelligence for information retrieval.

**Aryya Gangopadhyay, Professor, Information Systems**
*sites.google.com/site/homearyya/*
Privacy-preserving data mining; knowledge discovery in structured and unstructured data; health information systems.

**Anupam Joshi, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/anupam-joshi/*
The use of AI, the semantic Web and intelligent agents to analyze social media information to aid in decision making.

**Anita Komlodi, Associate Professor, Information Systems**
*userpages.umbc.edu/~komlodi/*
Human-centered computing, user-interface design, information retrieval.

**Jacob Kogan, Professor, Mathematics**
*www.math.umbc.edu/~kogan/*
Computational information retrieval.

**Charles K. Nicholas, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/charles-nicholas/*
Information retrieval, document processing systems, software engineering.

**Sergei Nirenburg, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/sergei-nirenburg/*
Natural language processing, artificial intelligence, knowledge-based systems, machine translation, ontological semantics, computational linguistics.

**Lina Zhou, Associate Professor, Information Systems**
*userpages.umbc.edu/~zhoul/*
Deception detection, intelligent user interfaces, social network analysis.

## Situational Awareness

Situational awareness involves building automated or semiautomated systems that are aware of what is happening in their environment and can understand how information, events and their own actions will impact the goals and objectives, both now and in the near future.

**Tim Finin, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/tim-finin/*
The use of the semantic Web, machine learning and artificial intelligence for autonomous computing.

**Milton Halem, Research Professor, Computer Science**
*mc2.umbc.edu/staff/halem.php*
Web services and high-performance computing in support of autonomous systems.

**Anupam Joshi, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/anupam-joshi/*
The use of AI, the semantic Web and intelligent agents for autonomous systems.

**Charles K. Nicholas, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/charles-nicholas/*
Information retrieval, document processing systems, software engineering for autonomous computing.

**Yelena Yesha, Professor, Computer Science**
*www.cs.umbc.edu/people/faculty/yelena-yesha/*
Distributed computing, high-performance computing, assured information systems for autonomous systems.

## TOWSON UNIVERSITY

### Foundations of Cyber Security

Towson University researchers employ mathematical techniques for designing and analyzing various tools that are used in the design and analysis of cryptographic protocols. Researchers are also building bare machine computing systems without any operating system or kernel, including secure Web and email servers, SIP servers and clients, and an IPv4/v6 gateway in collaboration with NSA.

**Ramesh Karne, Professor, Computer and Information Sciences**
*triton.towson.edu/~karne/*
Bare machine computing and secure bare machine systems.

**Alex Wijesinha, Professor, Computer and Information Sciences**
Computer networks including wireless networks, network security and network performance, VoIP and network protocols for bare machines.

**Marius Zimand, Professor, Computer and Information Sciences**
*triton.towson.edu/~mzimand/*
Cryptography and computational complexity, improving the cryptographic quality of sources of pseudo-randomness. Current active funding: $224,000

### Network Security and Forensics

Researchers at Towson University are working toward the design of techniques to provide secure, efficient and reliable network protection, including the development of watermarking techniques to track anonymous attacks, detection algorithms and systems against worm and botnet attacks, and applications to secure national smart grid and health-care information systems

**Subrata Acharya, Assistant Professor, Computer and Information Sciences**
Computer security, distributed systems, secure information systems, information security management, secure health informatics, trustworthy computing, privacy and ethical issues in computer security. Current active funding: $234,000

**Wei Yu, Assistant Professor, Computer and Information Sciences**
*pages.towson.edu/wyu/*
Invisible traceback for network forensics, security and privacy issues in large-scale data publishing/sharing, secured cyber physical systems, and stealthy worm/botnet detection and defense. Current active funding: $181,000

### Usability, Accessibility and Security

Security mechanisms, no matter how robust the design is intended to be, cannot assure information security if they are not easily usable and accessible by the general public. Towson University researchers are working to close that gap in a number of ways, including through the development of CAPTCHA systems suitable for visually impaired users.

**Heidi Feng, Associate Professor, Computer and Information Sciences**
*pages.towson.edu/jfeng/*
Usable and accessible security and privacy applications and procedures, hands-free speech-based interaction techniques for individuals with physical disabilities, and the adoption of information technology in the business section. Current active funding: $377,000

**Jonathan Lazar, Professor, Computer and Information Sciences**
*triton.towson.edu/~jlazar/index.html*
Usable security, accessible security for people with disabilities, human cognitive limits in computer security, public policy and usable security, human interaction proofs. Current active funding: $350,000

### Cyber Security Education

Towson University faculty have been at the forefront of pedagogical research, active and applied learning in cyber security education and have aimed to bring state-of-the-art cyber security research into classroom. They are developing new techniques for teaching secure coding from the very beginning and security injection modules to be incorporated across the undergraduate curriculum.

**Shiva Azadegan, Professor, Computer and Information Sciences**
*pages.towson.edu/azadegan/*
Computer security, information assurance, digital forensics and operating systems. Current active funding: $400,000

**Siddharth Kaza, Assistant Professor, Computer and Information Sciences**
*triton.towson.edu/~skaza/*
Social network analysis, data mining and security informatics. Current active funding: $400,000

# Appendix C »

## SURVEY RESULTS: CYBER SECURITY SKILLS FOR NEW GRADUATES

1. Please rate the importance of each technical skill for a new incoming cyber security hire, who is a recent graduate. Please rate the importance from 1 to 5, with 5 being "Very Important" and 1 being "Not Necessary."

| TECHNICAL SKILL | 1 NOT NECESSARY | 2 | 3 | 4 | 5 VERY IMPORTANT | RATING AVERAGE | RESPONSE COUNT |
|---|---|---|---|---|---|---|---|
| **LOW-LEVEL SOFTWARE, I.E. ASSEMBLY, C** | 7.1% (1) | 14.3% (2) | 14.3% (2) | 28.6% (4) | 35.7% (5) | 3.71 | 14 |
| **ALGORITHM COURSE** | — | — | 71.4% (10) | 14.3% (2) | 14.3% (2) | 3.43 | 14 |
| **NETWORKING PROTOCOL** | — | — | — | 57.1% (8) | 42.9% (6) | 4.43 | 14 |
| **OS INTERNALS** | — | — | 14.3% (2) | 42.9% (6) | 42.9% (6) | 4.29 | 14 |
| **SECURE SOFTWARE METHODOLOGY** | — | 7.1% (1) | 7.1% (1) | 35.7% (5) | 50.0% (7) | 4.29 | 14 |
| **MALWARE INTERACTION** | — | 14.3% (2) | 7.1% (1) | 28.6% (4) | 50.0% (7) | 4.14 | 14 |
| **SECURE ARCHITECTURE** | — | — | 7.1% (1) | 35.7% (5) | 57.1% (8) | 4.50 | 14 |
| **ANALYSIS OF DATA** | — | — | 28.6% (4) | 35.7% (5) | 35.7% (5) | 4.07 | 14 |

2. Please include any additional technical skills that you feel are important for a new graduate.

Must have a grounding on networks—legacy and developing (Cloud)

Forensic analysis skills (for some positions—if not already included in your "Analysis of Data" category) and thorough understanding of enclaving approaches and strategies using various means to segregate domains/enclaves with differing security requirements/vulnerability profiles.

Scripting skills, eg Python, Perl
Digital forensic analysis fundamentals
Data visualization/presentation (perhaps already covered by "Analysis of Data")

Kernel development. Hardware package configuration.

IT project management, and systems/requirements engineering and software engineering skills.

Information security architecture. Graduates should know something about data security.

Strong working knowledge of Unix-based OS, Scripting languages including Perl, Python, Ruby and Shell.
Kernel-level software coding skills.

Network protocols from LAN through WAN as well as emerging technologies/standards, RFC review of draft standards facing general adoption, hands-on practical experience with a variety of network technologies, operating systems and internals, and reverse engineering of software (compiled binaries and source code).

Systems engineering and analysis.

Knowledge discovery/data mining, high-performance computing systems, e.g. parallel processing systems, cloud computing systems, etc., virtualization of the IT infrastructure and how it is secured.

### 3. Please indicate any certifications that you feel would be beneficial for a new graduate to have coming into the workforce.

Software Assurance

Certifications are a mixed bag—too narrow a focus can be counterproductive early in one's career and many customers require/desire very specific certifications based on their support architecture and product preferences. Would prefer that new (undergrad-level) hires have broader certifications such as ITAC/ITAP or an enterprise architecture-level certification to ensure useful context for more narrowly focused technical certifications that can come later.

None. I value their degree, their accomplishments to date, and most of all their aptitude to solve new problems. Certifications are not what I look for in a college hire.

CISSP. ISSA.

Microsoft Office Information Security Certification

CISSP

CCNA, Red Hat Certifications such as RHCT/RHCSA

CISSP

CISSP, CEH, GIAC, GSE

None

### 4. Please indicate any non-technical skills that would be beneficial for the new graduate.

Teamwork is always a requirement—but the basics of communicating clearly are always essential.

Business analysis skills—too few new graduates are able to balance the real-life business demands of revenue, profit and flexible, responsive support for paying customers with security requirements and goals—a broader perspective is of great use in properly balancing security objectives with business reality.

Influencing change—cyber security is heavily led by those on the frontlines.
Communication—clear, concise presentation, writing skills.
Innovation/problem solving—the essence of cyber security is to solve a new problem every day.
Intelligence analysis—to excel at cyber security requires intelligence analysis disciplines.

Collaborative team environments. Cross-functional enterprise domain experience.

Technical writing/communication, cyber law, and computer/information forensic science skills.

Communciations and understanding of laws and regulations governing information security.

Ability to interface with our clients/government customers. Strong communication skills. Strong writing skills.

Oral and written communications skills.

Critical thinking, business operations, risk-based decision making.

Soft skills (report writing and speaking).



## 5. Please indicate any skills required by executive-level cyber/information assurance professionals.

Need to understand how the technical connects to process and policy. Mostly, they have to be able to relate business accumen to the discipline of security … they go hand in hand.

Executive-level IA professionals, by definition, must have solid business background and insight. While technical credentials are essential, senior-level IA and cyber types must be able to find the elusive balance between business needs and security. At this senior level, a security zealot who regularly falls into the stereotypical "security vs. business" mindset is of little value to an organization.

Understanding the ingredients for true risk management—recognizing good data from bad data, developing frameworks to measure progress, etc.

Influence organizational change—cyber security is a dynamic field and one's posture must change often, including large scale organizational changes.

Inter-company and public/private partnerships—more and more partnerships are the future of cyber security. executives must understand how to structure these agreements, how to influence legal agreements that will affect their ability to conduct business.

Intelligence community and specific customer environments.

The ability to manage in a virtual environment with geographically dispersed personnel. High-level project and program management skills. Experience or education in quality management and assurance dealing with information technology and systems requirements. Experience and/or knowledge in conducting quality audits.

Understanding of the cyberspace conops and the mission of their prospective organization and how they will use cyberspace.

All of the above with accents placed on enterprise engineering, coaching/teaching fundamentals, team building, project management.

Writing and speaking skills.

## 6. Please share any resources (including universities/colleges) and approaches currently used to train the cyber workforce.

Policy knowledge without practical experience is dangerous—you need a mix of both

We maintain an extensive set of internal training resources on IA and cyber topics as well as sponsoring professional certifications and undergrad/graduate degrees in Maryland and elsewhere.

Our business follows an intelligence-driven approach to computer network defense. As such we leverage a great deal of established military doctrine and intelligence analysis material, frameworks, and concepts to train our analysts. We're developing our own internal training program. Of all certifications, SANS are superior and well valued. We encourage our analysts to pursue higher education. A great deal of training occurs on the job

Internally developed and managed cyber certification program.

A very realistic approach is the use of distance education programs (undergraduate and graduate) with majors in Information Security. Also, creating concentrations, certificate programs, etc. to the degree program. Building alliances and degree bridge programs with vocational schools and community colleges that offer Associate's in Information/Cyber Security programs.

Cyber security consultations, product vendors, and special security training offerings from within the company.

Master's cohorts with NYU Poly, Capella and GWU. SANS courses and DOD 8570 certification providers.

## 7. Company representing.

CACI

Cisco

CSC

Lockheed Martin

ManTech International Corporation

NSA

Northrop Grumman

SAIC

Representing self and professional experience as a human resource professional in the high technology industry.

# Appendix D »

## FEDERAL PROGRAMS RELATED TO SCHOLARSHIPS AND DEBT FORGIVENESS FOR CYBER CAREERS

There are a number of sources of federal financial aid that serve as incentives for individuals to enter and persist in fields related to cyber security. These programs vary in funding levels and eligibility requirements. For the 11 programs listed below, the most current and accurate information is available on the hyperlinks.



### I. Loan Forgiveness for Public-Sector Workers

*studentaid.ed.gov/PORTALSWebApp/students/english/PSF.jsp*

- People who work full-time in:
  - Government (local, state, and federal)
  - Emergency management (police officers, firefighters, emergency medical technicians)
  - Military service
  - Public health
  - Public education
  - A nonprofit

### II. Loan Forgiveness for Workers in Areas of National Need

*studentaid.ed.gov/PORTALSWebApp/students/english/PSF.jsp*

- People who work full-time in:
  - Foreign language specialties
  - STEM fields
  - Allied health
  - School-related support (administrators, counselors, etc.)
  - Medical specialties
  - Child welfare

### III. Department of Defense Science, Math and Research for Transformation (SMART) Scholarships

*smart.asee.org/*

- Undergraduate students who are:
  - 18 years of age
  - U.S. citizens
  - Pursuing a bachelor's degree in a STEM field
  - In good standing at their school
  - Willing to accept employment at the DOD following graduation

- Graduate students who are:
  - U.S. citizens
  - Pursuing graduate degrees in a STEM field
  - Have a cumulative 3.0 undergraduate GPA
  - Willing to accept employment at the DOD following coursework completion

### IV. Barry Goldwater Scholarships

*www.act.org/goldwater/*

- Students who are in the top quarter of their class, have a GPA of 3.0 and are:
  - Undergraduate students in their junior or senior year
  - Community college students in their second year

- Students who intend to enter employment in STEM-related research

### V. Department of Defense Information Assurance Scholarship Program

*cio-nii.defense.gov/sites/iasp2/*

- U.S. citizens who can obtain a security clearance

- Undergraduate students:
  - Must attend a National Center of Academic Excellence (CAE) selected by the National Security Agency (NSA) and Department of Homeland Security (DHS)
  - Must have a 3.2 cumulative GPA
  - Must be in their junior or senior year and pursuing a degree with a concentration in information assurance

- Graduate students
  - Must have a 3.5 cumulative GPA
  - Must be pursuing a course of study with a strong information assurance component

### VI. National Science Foundation Federal Cyber Service: Scholarships for Service

*www.sfs.opm.gov/*

- U.S. citizens
  - Undergraduates who are in their junior or senior year
  - Master's students pursuing a two-year degree
  - Ph.D. students in their final two years of coursework

### VII. National Security Agency Stokes Educational Scholarship Program

*www.nsa.gov/careers/opportunities_4_u/students/stokes.shtml*

- U.S. citizens

- High school seniors who:
  - Are eligible for a security clearance
  - Plan to major in computer science or computer or electrical engineering
  - Have a minimum cumulative 3.0 GPA
  - Have a minimum SAT of 1100 (1600 under the new SAT)

- College sophomores who:
  - Are eligible for a security clearance
  - Are majoring in Persian or Farsi
  - Preferably, have a freshman year GPA of at least 3.0

### VIII. Central Intelligence Agency Undergraduate Scholarship Program

*www.cia.gov/careers/student-opportunities/undergraduate-scholarship-program.html*

- U.S. citizens

- High school seniors or college freshmen or sophomores with:
  - A minimum SAT of 1000 (1,500 under the new SAT)
  - A minimum cumulative 3.0 GPA
  - Demonstrated financial need

- Family income of $70,000 a year or less

### IX. Department of Energy Computational Science Graduate Fellowships

*www.krellinst.org/csgf/*

- U.S. citizens or legal resident aliens
  - Who plan to pursue full-time doctoral studies in computational science

- Certain students may apply
  - Undergraduates in their third or final year of college
  - Graduate students enrolled in a two-year master's program

### X. National Security David L. Boren Foreign Language Scholarship

*www.borenawards.org/*

- U.S. citizens attending any American institution of higher education
  - Undergraduates planning to participate in study abroad
  - Graduate students committed to study and research of areas that are critical to U.S. interests (Latin America, the Middle East, etc.)

### Xi. Harry S. Truman Public Service Scholarship

*www.truman.gov/home*

- U.S. citizens

- Undergraduates in their junior year at a four-year college or university