REPORT

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

SALVE REGINA UNIVERSITY

One Leader at a Time: The Failure to Educate Future Leaders for an Age of Persistent Cyber Threat

Francesca Spidalieri

March 26, 2013

Internet-based technologies have proliferated to such an extent over the past few decades that they are now the predominant method through which we create, process, store, and share information. Nearly 80% of Americans are connected to the Internet today and there were 2.4 billion users worldwide as of June 2012.[1] The growth in this area has been such that, by 2015, the number of Internet hosts is expected to exceed the planet's human population.[2] The very openness that allowed the Internet to spread into almost every area of human activity, however, has also spawned vulnerabilities of staggering proportions—vulnerabilities that are already exploited by non-state and state actors alike, generating billions of dollars in criminal revenue. Stories about the U.S. critical infrastructure vulnerability to cyber attack, the threat it poses to its economy and the increase of cybercrime and economic cyber espionage now dominate the news on an almost daily basis. Cyber threats have the potential to undo all the huge economic, social and military advances that cyberspace has enabled, if not properly understood and mitigated. Ultimately, these threats can touch—if not harm—every institution in American society. The public and private sectors' increasing reliance on cyberspace and the growing scope and sophistication of cybercrimes have resulted in what President Obama called "one of the most serious economic and national security challenges we face," and what U.S. Cyber Command chief and director of the National Security Agency (NSA), Gen. Keith B. Alexander, has labeled as "the greatest transfer of wealth in history."[3]

The threat is widely recognized by experts and acknowledged by non-experts as well.[4] The needs of government and the private sector have driven academic and technical institutions to introduce new majors and courses in computer science, programming, and information assurance. Most of the cybersecurity related courses and certification programs offered, however, were created for professionals in the information technology (IT) field who want to develop a cybersecurity expertise. Many of these programs are therefore not introductory, and an existing IT skill set is usually required to be admitted.

Many of these courses, then, may not suit the needs of the modern world for several reasons. One is the narrow focus of these technical courses; IT experts are principally concerned with the technical solutions to these problems, but lack the expertise to develop policy to guide the direction that technical development should follow, and how to implement it in an institutional, legal, and economic context. Cyber defense requires not only IT experts with computer science, electric engineering, and software security skills, but also professionals with an understanding of political theory, institutional

Francesca Spidalieri is a fellow at the Pell Center for International Relations and Public Policy at Salve Regina University.

The author would like to thank Dr. Chris Demchak of the Naval War College for her insights and encouragement. Any faults in the report, however, remain the author's alone.

theory, behavioral psychology, military ethics, international law, international relations, and additional social sciences.[5] A second reason is the lack of this type of knowledge at the leadership level, and the fact that most institutions in our society are run by individuals who have virtually no background in cybersecurity. Most leaders in the public and private sectors earned degrees in fields other than computer network security, and few of them understand what 'cyberspace' is, how networks physically work, and what dangers lurk within each.[6] As a result, the pillars of our society—our universities, our hospitals, our local governments, our courts, and many of our businesses—are often led by individuals with an extremely limited exposure to cyber issues and the existential threats they pose to those institutions.

More troubling, the nature of cyber threats today is so pervasive, so strategic and so precise that we cannot expect new technologies alone to protect an organization's information and business, nor we can expect our IT departments to be the only ones in charge of preventing and containing these threats. Firewalls and encryptions alone are insufficient to counter cyber threats today and they will be insufficient to counter the cyber threats of tomorrow.[7] No matter how good a particular technology is, if it is not effectively adopted and implemented by executives, and correctly used by skilled employees who follow well-defined processes, vulnerabilities will surface that can be leveraged by both internal and external threat actors.[8] As Melissa Hathaway, former National Security Council Director for Cyberspace and primary author of Obama's 60-day Cyberspace Policy Review, explains:

> Every profession today has to have some basic understanding of the benefits of information communications and technology (ICT) adoption as well as the security risks that may be attended with them. If you are the CEO of a major corporation, you need to understand the contribution of ICT to the bottom line and how it affects your efficiency and productivity, but you also need to understand when the policies and programs in place are affecting your risks if you have a security breach. From a policy maker's perspective, it is basically the same thing. We are moving in adopting these technologies without regard to the security risks that may be attended with them.[9]

More than being a mere technical problem, achieving cybersecurity is a social, institutional, legal, and governance problem. In other words, it is an operational issue that requires the leaders of institutions to implement fundamental, overarching policies and strategies that can begin to mitigate cyber threats. Cybersecurity problems often start with ordinary digital technology users who have not received the proper training, or who do not take security seriously and sidestep basic security measures. Effective security has to synthesize organization-wide prevention and mitigation measures, and not rely on IT professionals working in a vacuum to "fix" a breach after the fact. Achieving cybersecurity thus requires managerial action and oversight throughout the entire organization, as much as rules and software solutions. Institutional leaders do not need to be trained as programmers, but they must have a deep understanding of the cyber-context in which they operate to harness the right tools, strategies, people, and training to respond to this dynamic and rapidly-developing array of threats.

Universities are key institutions in bridging from concept to methodology, tools, and implementation. They can play a key role in educating civilian and military workforces on the unique tenets of cyber, and optimizing their campus-wide resources to fuse knowledge, intellectual capacity, and practical skills.[10] Despite the pressing need to educate future leaders about information security, however, only a handful of American universities offer courses or degree programs that combine both cybersecurity policy and technology, and even fewer encourage collaboration among departments to optimize their efforts. In addition, professional military institutions studying national security and strategy have only recently begun to integrate cybersecurity issues into their curricula, despite more than a decade's worth of experience suggesting that networks and information technologies are both essential to operations and vulnerable to attack.[11] To help encourage the study of cyber threats to our national information infrastructure, the National Security Agency (NSA) and the Department of Homeland Security (DHS) have established criteria for the designation of qualified non-military universities or academic departments as Centers of Academic Excellence in Information Assurance Education (CAE/IAE), CAE IA Research (CAE/R), and lately as CAE Cyber Operations.[12] However, even most of these designated institutions' qualifying programs are deeply technical and center around *information assurance*—limited to the protection and management of information-related risks—and rarely pursue broader multi-disciplinary approaches that are commensurate with the complexity of cyberspace.[13]

This study surveys current efforts by graduate-level educational programs in the United States to prepare non-technical institutional leaders in government, academia, civil society and in the private sector for an era of persistent cyber threat. It focuses primarily on the top ten ranked graduate schools (a few other niche programs are also evaluated) in each of the major degree programs that traditionally develop leaders across society—Master of Business Administration (MBA), Master of Public Administration (MPA), Master of Public Policy (MPP), Master of International Relations (IR), Master of Laws (LLM), Criminal Justice, and Healthcare Management—to assess what level of exposure to cyber issues students already receive and to what extent they graduate with an adequate understanding of the cyber challenges facing their respective fields. Lastly, the report identifies which leading programs still need to include a cybersecurity component into their curricula. For each institution, the study indicates CAE/IAE and CAE/R designations—if awarded—and a Likert score (0 to 4) obtained from a set of variables and the use of a modified Likert approach to evaluate the opportunities offered to students in relation to the broader systematic need to educate future leaders about cyber threats in each discipline.[14]

This study is not a one-time only endeavor; it is simply the beginning of a larger effort to review and update the state of cybersecurity leadership development in America's higher education system. As schools come to recognize the importance of cybersecurity to their curricula—a recognition of its importance to the future of the human community—updates to this report will monitor, track and evaluate those developments. It is also our hope that this work catalyzes additional research into the development of best practices, specific curriculum recommendations and heightened awareness of the need to develop non-technical cyber leaders across society.

Methodology

This study summarizes our survey findings of current efforts by graduate-level educational programs in the United States to include information technology and cybersecurity education in their curricula. It seeks to identify best practices, review program effectiveness in promoting cybersecurity knowledge in non-technical fields of study, as well as recognize existing curriculum gaps in this area of interest. This report does not provide an in-depth analysis of specific courses or an extensive audit of particular programs; rather, it presents the critical need for each discipline analyzed to integrate an information technology and cybersecurity component into their core curricula and outlines the progresses, or lack thereof, made by each university in this directions so far. The survey is not confined to top ranked graduate programs alone. A number of schools that are at the vanguard of creating new cybersecurity concentrations and certification programs within different fields of study are also evaluated. These other schools provide a context for exploring how other institutions are positioning themselves in the field of non-technical cybersecurity education and for getting a glimpse of what future trends may look like.

The survey findings are based on data collected between August 2012 and March 2013 from each educational institution through a combination of interviews with academics and university staff, and information presented on the school's website. The results derive from the responses to four main curriculum questions and the use of a modified Likert approach to evaluate the level of exposure students receive to cybersecurity issues in each of these academic institutions and the opportunities offered to deepen their knowledge in this field. Interview respondents were asked whether their specific department offers: 1) a core course in information technology, with at least part of the course dedicated to cybersecurity; 2) elective courses in information technology and cybersecurity; 3) the possibility for their students to enroll in other elective courses in information technology and cybersecurity at other departments of the university; 4) occasional seminars or conferences in cybersecurity issues. The modified Likert scale used to derive a notional ranking of the academic institutions analyzed assigns a number (0 to 1) to each response as follow: Yes = 1; Not specifically, but… = 0.5; No = 0. The answers are then summed up and each school receives an overall score on a 0 to 4 scale, 4 being the highest score a school can receive. The specific responses are also discussed in more details in this report.

Whenever the interviewees did not provide an answer to all four questions, we made our own assessment based on the information available from that graduate program's website. The assumption behind this approach is that if a school offers a dedicated core course in IT and cybersecurity, all students in the program will most likely receive the broader education and practical knowledge needed to manage the information security needs of their sector. If the school, or the university at large, offers elective courses in IT and cybersecurity, students interested in the topic will have at least the opportunity to gain a basic understanding of the cyber-context and explore cybersecurity related issues. If cyber issues are covered as part of broader courses, students will at least be aware of the cybersecurity challenges and opportunities in that specific area of study. If the school offers occasional seminars or conferences on IT and cybersecurity, students will have some opportunities to be exposed to understanding cybersecurity issues and how they relate to their field of study. If none of these opportunities are provided, we assume that graduates of these programs do not gain a thorough understanding of the challenges, opportunities, and threats of the digital age beyond their own personal experience. Recognizing that the inclusion of cybersecurity technology and policy components may still be a work in progress for many universities, we hope that our findings will add value to other efforts to integrate cybersecurity education in non-technical disciplines and serve as useful tools for academic and professional institutions considering various approaches towards cybersecurity leadership development.

The graduate school rankings used—and thus the sequential order of the universities presented—in this report for the MBA, MPA, MPP, LLM, Criminal Justice and Health Care Administration programs are based on surveys from *U.S. News & World Report*.[15] *U.S. News* analyzed more than 1,200 graduate programs throughout the United States, covering an array of disciplines and programs. Their rankings are based upon data which *U.S. News* collects from each educational institution either from an annual survey or from the school's website. The results derive from a weighted average of different indicators, including peer assessment score, recruiter assessment score, job placement success and student selectivity. Although *U.S. News* rankings of best graduate schools is not the only ranking system available—this system has also sparked significant controversy surrounding their annual survey—it is still regarded as the most influential and widely used of all college rankings in the United States.

The IR program rankings are based on the Best International Relations Master's Programs list compiled by *Foreign Policy*.[16] The survey's authors are researchers with the Teaching, Research, and International Policy (TRIP) project at the College of William and Mary. International Relations faculty members from every four-year college and university in the United States participated in the survey.

MBA Graduate Programs

***"There are two types of companies in the United States,
those that have been hacked and those that don't yet know they've been hacked."[17]***

U.S. News Ranking	College/University	School of Business	City	State	Likert Scale Average Score	NSA Certification*
#1	Harvard University	Harvard University Business School	Cambridge	MA	2.5	N/A
#1	Stanford University	Stanford Graduate School of Business	Stanford	CA	2	N/A
#3	University of Pennsylvania	Wharton School of Business	Philadelphia	PA	2	N/A
#4	Massachusetts Institute of Technology	Sloan School of Management	Cambridge	MA	2.5	N/A
#4	University of Chicago	Booth School of Business	Chicago	IL	1	N/A
#4	Northwestern University	Kellogg School of Management	Evanston	IL	0.5	N/A
#7	University of California, Berkeley	Walter A. Haas School of Business	Berkeley	CA	1.5	N/A
#8	Columbia University	Columbia Business School	New York City	NY	1.5	N/A
#9	Dartmouth College	Amos Tuck School of Business Administration	Hanover	MA	2	N/A
#10	New York University	Stern School of Business	New York City	NY	1.5	N/A

** Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

Businesses around the world today tender services and products through the Internet to more than 2.5 billion people using secure protocols and electronic payments. From managing supply chains, to controlling the operations of banks, coordinating business transactions, and storing intellectual property, the Internet has opened global markets and revolutionized modern business practices. Yet, while providing new opportunities, reliance on the Web has also exposed new vulnerabilities. The cyber security firm Symantec estimated that U.S. businesses alone are losing upwards of $250 billion in intellectual property (IP) theft every year. A recently released Poneman Institute study reported that cybercrime now costs U.S. companies an average of $8.9 million a year, with an average of 24 days needed to spot and resolve a cyber attack.[18] The Poneman study showed that the highest cost of cybercrime estimated for one company was $46 million and that malicious attacks can take more than 50 days on average to contain. Cleanup costs, including lawsuits, amounts to millions of dollars a year, and then companies have to deal with the damage that a hack does to the integrity of their brand. In 2011, another study of 583 U.S. companies conducted by Poneman Research on behalf of Juniper Networks established that hackers had breached 90% of those organizations at least once in the past 12 months.[19]

"There are two types of companies: companies that have been breached and companies that don't know they've been breached," Shawn Henry, the F.B.I.'s top former cyber agent who recently joined the cybersecurity start-up CrowdStrike, said in an interview with *The New York Times.* "I've seen behind the curtain. I've been in all the briefings. I can't go into the particulars because it's classified, but the vast majority of companies have been breached," although such breaches rarely make headlines because companies fear what disclosure will mean for their stock price.[20]

These attacks are often driven by financially-motivated cyber criminals who use malware, Trojans, phishing and other automated attack tools.[21] Hackers have targeted companies of all sizes, and cyber attacks on small businesses as well as large financial institutions are expected to grow in both volume and complexity in 2013.[22] Nor does it matter what new technology a company may have acquired to protect their information and business, or how prepared their IT department may be. Experts at Booz Allen Hamilton indicate that the cyber attacks of 2013 will overwhelm a company's capacity to protect its networks if not accompanied by appropriate education of top executives and employees and fine-tuning processes to ensure, not only the proper use of technology, but that processes that require interfaces between organizations are well managed and executed flawlessly.[23]

Many of the top executives and employees in these institutions have likely pursued MBAs before obtaining leading positions in their organizations (and more than half of them got their degree before cybersecurity was even an issue). MBA programs encompass a wide variety of concentrations including but not limited to: accounting, consulting, finance, health care administration, manufacturing, technology, marketing, non-profits, public policy, human resources and real estate. None of the MBA programs analyzed in this survey offers courses that are exclusively dedicated to the technical, policy or operational aspects of cybersecurity. Many of these programs, however, have added case studies and elective courses that address the business challenges of information security and introduce elements of effective cybersecurity practices and policies. Further, many of these universities as a whole sponsor conferences and seminars on cybersecurity and, in some cases, they have also established centers for the advancement of cybersecurity research and development.

Harvard University – Harvard Business School (HBS) Cambridge, MA
(U.S. News Rank #1) NSA Cert: N/A

The Harvard Business Review has published case studies and articles on cyber espionage, cyber war, cyber terrorism and cybersecurity since the early 2000s. Nonetheless, the MBA program at HBS offers only one core course in "Technology and Operations Management" which touches upon information technology and operation strategies, but does not address cybersecurity questions and dilemmas in the business sector. At most, MBA students can choose from a limited number of elective courses focusing on the use of information communications technology (ICT) to promote business, navigate strategic interactions with competing platforms, and manage technology-intensive businesses. These courses, including "Strategy and Technology," "Understanding Technology Businesses," "The Online Economy" and "Competing with Social Networks," do not seem to provide a sufficient understanding of the security challenges that may be attended from the adoption of these technologies. Despite the lack of cybersecurity dedicated courses, for nearly twenty years HBS has held an annual cyberposium, the largest MBA technology conference in the world. The conference facilitates an interactive network of current and future business leaders to engage in discussion about technology and its impact on business and society. Finally, HBS offers the opportunity for students to cross-register for up to two courses at other academic departments and other selected graduate programs (including MIT and the Fletcher School) that may offer IT and cybersecurity courses. In brief, Harvard MBA students can gain a deep understanding of ICT in the business sector, but have limited exposure to the specific cybersecurity issues necessary to manage the information security needs of various business organizations.

Stanford University - Graduate School of Business Stanford, CA
(U.S. News Rank #1) NSA Cert: N/A

The Stanford MBA program offers several elective courses focusing on the evolution of information technology, economics of the Internet, network analysis, advantages and risks of new technology opportunities, and electronics, computing, networks and software applications used in a variety of business settings. However, only a few of these courses occasionally address information security, Internet policy, and intellectual property topics, dependent on student interests. Even though the MBA program does not include a thorough cybersecurity component, Stanford University has established a Cybersecurity Center that offers a number of elective cybersecurity related courses and seminars open to all Stanford students.[24] Stanford University as a whole houses one of the top-ranked undergraduate and graduate computer security programs in the country, and is extremely well-connected with the tech industry in Silicon Valley, where MBA students can be exposed to the latest technologies, research and strategies in IT and cybersecurity. However, it remains surprising from the information gathered that the Stanford MBA program has not integrated more aspects of cybersecurity in its curriculum, and that only those students already predisposed to cybersecurity issues will further their education in this field.

University of Pennsylvania - Wharton School of Business Philadelphia, PA
(U.S. News Rank #3) NSA Cert: N/A

Although they do not include cybersecurity per se, the Wharton MBA program offers core courses in "Information Technology and Business Transformation" and "Advance topics in Information Strategy" for students concentrating in Information Strategy and Economics. All MBA students have the option to choose among the many elective courses in information technologies and systems, innovation management, and information strategy offered through the Operation and Information Management Department at the Wharton School. However, the only course that touches upon security issues in IT is "Information Systems for Managers." In addition to Wharton MBA courses, "students are also welcome to enroll in 4-6 classes offered at any of the 11 Graduate and Professional Schools at the University of Pennsylvania that may address cybersecurity issues, as long as the respective department or school allows" said MBA program coordinator Cindy Armour.[25] The courses available in computer and information technology, however, are highly technical and specialized, and require a pre-existing competency in statistics, computer language and information technology. Thus, MBA students at the Wharton School have the opportunity to pursue a strong information technology curriculum if they choose, but one that does not include a significant cybersecurity component.

Massachusetts Institute of Technology - Sloan School of Management Cambridge, MA
(U.S. News Rank #4) NSA Cert: N/A

MBA students at the Sloan School can personalize their curriculum after completing the first-semester core subjects (none of them addressing IT and cybersecurity), and choose from various MBA electives focusing on information technology, digital business and network security. Other courses in IT, cybersecurity and cyberpolitics are offered through other departments at MIT. As Tish Miller, Director of Academic Programs for MIT Professional Education, explains: "these courses are open to all MIT students, including MIT Sloan MBA graduates. Many of the classes are offered through the Computer Science Department," which includes "several courses that cover the topic of computer and network security." Finally, last year annual MIT Sloan CIO Symposium, where CIOs and other senior business executives from around the world gathered to explore how leading-edge academic research and innovative technologies can help address the practical challenges faced in today's changing economy, focused primarily on cybersecurity issues. Aside from the Sloan School's initiatives, MIT leads the efforts to advance and protect the capabilities of the nation's global defense networks, and is one of the biggest cybersecurity employers in the country. In principle, MIT could be at the forefront of cybersecurity research, education and policy by tapping into a number of advantages—among them its world-class research centers and strong bonds with businesses—that other programs in this survey do not have. The Sloan School MBA curriculum, however, has yet to incorporate a cybersecurity component sufficient to teach students how to prevent and mitigate cyber threats in the business sector.

University of Chicago - Booth School of Business Chicago, IL
(U.S. News Rank #4) NSA Cert: N/A
The Booth School of Business has yet to include an information technology and cybersecurity component in its MBA core and elective courses. Nonetheless, Booth student-organized conferences and occasional roundtables, such as the Booth School 2011 Business Forecast event, have addressed many of the cybersecurity threats facing the business sector. In 2012, the school hosted the Security Innovation Network (SINET) Summit, which focused on the advancement of cybersecurity innovation through public-private collaboration. Finally, the Booth School used to offer a three-day *Executive Program in Information Technology: Strategies and Solution* for senior executives and upper management, which provided them with the technical foundation, strategies and solutions to effectively plan, implement and sponsor information technology initiatives within their organizations. According to Program Manager Catherine Cabrera, however, the program has been currently discontinued due to conflicting commitments of the faculty director, but should be offered again in the future.[26]

Northwestern University - Kellogg School of Management Evanston, IL
(U.S. News Rank #4) NSA Cert: N/A
Although the MBA program at the Kellogg School does not offer any core courses in information technology or cybersecurity, a limited number of electives address topics in technology and innovation strategy, marketing in the networked economy, managing ICT adoption, and protecting intellectual property. The only course that includes particular IT privacy and security aspects is "Health Information Technology," designed for students who are specializing in Health Enterprise Management. As Academic Advisor Kalpana Waikar explained: "Students can also cross-register for classes offered by other Northwestern University schools," but evidence suggests that MBA students rarely do so because of the heavy caseload of their curriculum.[27]

University of California - Walter A. Haas School of Business Berkeley, CA
(U.S. News Rank #7) NSA Cert: N/A
The MBA program at the Haas School does not offer core courses in information technology and cybersecurity. Students, however, can choose from a variety of evolving IT electives and dual degree offerings—from within the Haas School and from the wider university—as well as design courses of their own in conjunction with faculty members, for example from the College of Engineering.[28]

Haas School IT electives include “Introduction to Management of Technology,” “Technology Strategy,” “The Future of IT,” and “Innovation and Entrepreneurship in Information Technology,” but these courses do not seem to address any specific cybersecurity related issues. Nonetheless, Berkeley-Haas takes advantage of its location in the Bay Area and Silicon Valley to invite local executives and technology experts to be guest lectures and visiting fellows, and to partner with them in research projects. Twitter Co-founder Biz Stone, for example, is currently serving as a Haas Executive Fellow. Other recent technology experts to speak at Haas have included Former Apple Chief Evangelist Guy Kawasaki, Pixar President and Co-founder Ed Catmull, and Cisco Chairman and CEO John Chambers.[29] In addition, student groups host special events, such as an annual Digital Media Conference, and organize career-oriented activities with local tech firms. In principle, Haas students interested in pursuing careers in the information technology industry can receive a comprehensive education in technology management and strategy, and benefit from the many hands-on opportunities offered by the local tech industry. However, it is not clear that students in this or any other MBA fields at UC Berkeley are exposed to specific cybersecurity issues in the business sector.

Columbia University - Columbia Business School New York, NY
(U.S. News Rank #8) NSA Cert: N/A

Columbia Business School does not currently offer any courses in information technology and cybersecurity, although it has in the past. The Richman Center for Business, Law, and Public Policy at Columbia University—a joint venture of Columbia’s Business and Law Schools—offers lectures on emerging policy issues at the nexus of law and markets, including cyber threats and cybersecurity. Moreover, students interested in business aspects of information technology can participate in the events and activities organized by the MBA student-run Technology Business Group (TBG). Last years’ events included a trip to Silicon Valley, participation in the Harvard Business School Cyberposium, and private dinners with tech executives and industry speakers. However, as TBG co-president Eric Metelka points out: “IT is definitely a gap that needs to be filled at Columbia Business School.”[30] In principle, students inclined to learn more about IT and network security can take a limited number of courses at the Computer Science Department; in practice, though, these courses are difficult to access due to their high degree of technicality and pre-existing competency requirements, leaving few opportunities for MBA students to explore cybersecurity related issues.

Dartmouth College - Amos Tuck School of Business Administration Hanover, NH
(U.S. News Rank #9) NSA Cert: CAE/R

There is no current course in the MBA curriculum at the Tuck School of Business that address cybersecurity specifically.[31] The Tuck School, however, houses the Center for Digital Strategies (CDS), which focuses on the challenges of businesses dependence on the Internet and ways in which the private sector can address these challenges.[32] “CDS brings together groups of CIOs in the Americas and Europe that meet throughout the year to discuss issues facing IT leaders [and management in the digital, networked economy],” explained CDS Program Manager Tim Paradis. “Security is a recurring theme at meetings of the Roundtable on Digital Strategies,” and CDS “conducts periodic seminars, conferences and workshops on cybersecurity issues—such as the Information Security Workshop,” he continued. Moreover, “CDS conducts research into information security through its affiliated faculty as well as post-doctoral researchers […] and serves as a sounding board and resource for issue around IT and information security for Tuck students and interested parties." A number of Center-affiliated MBA electives cover various aspects of digital business strategies, cyber risks of firms reliance on the information infrastructure, information security risks and privacy in healthcare, and elements of effective cybersecurity practices and policies. Finally, CDS organizes various events in collaboration with the Institute for Information Infrastructure Protection (I3P), a national consortium of leading academic institutions, national laboratories, and non-profit research organizations working to address cybersecurity challenges affecting the nation's critical infrastructures.[33] In principle, Dartmouth MBA students involved in CDS and I3P activities have the opportunity to be exposed to a great deal of cybersecurity issues and explore the many ways in which they affect business strategies in general. From the information collected, however, it is not clear if Tuck MBA students who are not affiliated with CDS receive any significant exposure to the challenges, opportunities, and threats of cyberspace in the business sector.

New York University - Leonard N. Stern School of Business New York, NY
(U.S. News Rank #10) NSA Cert: N/A
The NYU Stern prides itself for being a leader in addressing the ways information technology affects business development. "MBA students can graduate with an Information Systems (IS) specialization and choose from a variety of electives addressing Internet technologies, information systems, digital strategies, cyber laws, computer forensics, and network security," explains Sara Gorecki, Administrative Assistant for the Information, Operations, and Management Systems Department.[34] Professor Norman White confirms that: "a number of the MBA elective courses in information technology will cover a part of cybersecurity."[35] However, none of the core courses in the MBA curriculum focuses on IT or cybersecurity, and MBA students do not have the opportunity to cross-register for other IT courses at other NYU departments "unless they take a non-credit course." An exception to this, are those NYU Stern MBA candidates who choose to enter the field of cybersecurity and who receive the ASPIRE scholarship from the National Science Foundation. ASPIRE fellows are required to take a set of ASPIRE interdisciplinary gateway courses encompassing the technological (NYU-Poly)[36], business (NYU-Stern), cultural (NYU-Steinhardt), public policy and management (NYU-Wagner) and scientific (NYU Courant Institute) aspects of real world security and privacy problems. Upon graduation, recipients must work for two years at a federal agency. In sum, NYU Stern offers a broad cyber-related curriculum for MBA students who want to specialize in Information Systems, and provides them with few incentives to pursue cybersecurity careers upon graduation. It is unclear from the information provided, though, whether MBA students who do not specialize in IS receive any exposure to understanding cybersecurity issues in the business sector.

Other Programs of Note

A recent article in *U.S. News & World Reports* makes clear that other MBA programs are carving out their own niche business degrees in information security in response to industry demand.[37] **James Madison University**, for example, launched its Information Security MBA program in 2000 and its graduates receive NSA certification upon completion of their MBA. The program combines traditional business courses—such as accounting, finance, and marketing—with specialty courses such as information security, ethics and computer forensics to show students how protecting data fits into a business model. Other schools offering business degrees with a focus on cybersecurity include the **University of Dallas**, which offers a MBA Concentration in Cybersecurity, and the **Colorado Christian University**, which pairs in-person business courses with online information security classes from the University of Fairfax in Virginia. Students enrolled in the MBA program at **Ferris State University** in Michigan can opt to specialize in information security and networking management. **George Washington University** offers a World Executive MBA in cybersecurity, aimed at both public and private sector professionals who work in areas ranging from policy and contracting, to privacy and data security. The School of Business Administration at the **University of Dayton** has recently announced a new MBA concentration and certificate program in cybersecurity, which plans to prepare students for careers in cybersecurity management in government organizations and the private sector.

MPA and MPP Graduate Programs

"We use Facebook to schedule the protests, Twitter to coordinate, and YouTube to tell the world."[38]

U.S. News Ranking	College/University	School	City	State	Likert Scale Average Score	NSA Certification*
#1	Syracuse University	Maxwell School of Citizenship and Public Affairs	Syracuse	NY	3	E, R
#2	Indiana University	School of Public and Environmental Affairs	Bloomington	IN	1.5	E, R
#3	Harvard University	John F. Kennedy School of Government	Cambridge	MA	3	N/A
#4	University of Georgia	School of Public and International Affairs	Athens	GA	0.5	N/A
#5	Princeton University	Woodrow Wilson School	Princeton	NJ	1.5	R
#6	New York University	Robert F. Wagner Graduate School of Public Service	New York	NY	2	N/A
#6	University of Southern California	Sol Price School of Public Policy	Los Angeles	CA	2	R
#9	Carnegie Mellon University	Heinz School of Public Policy and Management	Pittsburgh	PA	3.5	E, R
#9	University of Kansas	School of Public Affairs and Administration	Lawrence	KS	1	E
#9	University of Washington	Daniel J. Evans School of Public Affairs	Seattle	WA	2	E, R

** Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

The Internet, together with the information communications technology (ICT) that underpins it, has become a critical national resource for governments and has allowed the public, private, and non-profit sectors to improve their efficiency and better serve constituents. It has also given a voice to the weak and disenfranchised against their authoritarian leaders, resulting in what *New York Times* columnist Nicholas Kristof labeled the "quintessential 21st-century conflict," in which "on one side are government thugs firing bullets…[and] on the other side are young protesters firing 'tweets.'"[39] Indeed, cyber activism has become a catalyst for protests—such as Occupy Wall

Street and the Arab Spring—and a tool for change. But with a rapidly growing user base globally, an increasing reliance on the Internet, and a great potential for disruption, digital tools are also exposing the public sector to a new set of cyber threats. Most recently, Internet activist group Anonymous extracted from U.S. Federal Reserve computers—and published—databases containing the credentials of 4,000 American bank executives. It also defaced various U.S. government websites as part of its Operation Last Resort, launched in January in response to the suicide of Internet activist Aaron Swartz. Internet hacking of government networks is nothing new, though. There have been 618 publicly disclosed cases of breaches of government and military networks since 2005, in which at least 147 million records were stolen, according to the Privacy Rights Clearinghouse Chronology of Data Breaches.[40] Cybersecurity and law enforcement experts say the publicly disclosed cases represent only a fraction of the actual number of successful hacks of corporate and government networks.[41]

As governments and public organizations grow increasingly dependent on information technology, cyber threats have the potential to touch—if not harm—every institution in American society. Richard Clarke, in his book *Cyber War*, warns us that a potential "broad-based cyber attack on a nation's infrastructure could keep the power grid off-line for weeks, pipelines unable to move oil and gas, trains sidelined, airline grounded, banks unable to dispense cash, distribution systems crippled, and hospital working at severely limited capacity."[42]

Today's cyber threats require government leaders to be equipped with, at minimum, a basic knowledge of the web, the physical structure of networks, its players, major risks, and emerging trends. No captain of a ship would say: *"I don't know anything about the ocean, but I hired somebody to drive the ship."* Likewise, public leaders whose physical institutions exist and operate in, through, and with the digital realm need to be able to make good policy and sound security decisions based on knowledge of cybersecurity risks and potential impacts. Thus, cybersecurity policy, law and technology ought to become an integral part of all those graduate programs—such as MPA and MPP—intended for public leaders.

At present, only few of the MPA and MPP programs analyzed have added a cybersecurity technology and policy component to their curricula. Many universities, however, have some type of cybersecurity research or education program at one of their research centers or other departments, indicating at least an interest in preparing their master's programs candidates to lead in a fundamentally different cyber age. These programs are still in their incipient stages and it may be too soon to assess if their graduates emerge with the necessary understanding of the technical, legal, policy and operational aspects of cybersecurity.
MPA Graduate Programs

Syracuse University - Maxwell School of Citizenship and Public Affairs Syracuse, NY
(U.S. News Rank #1) NSA Cert: CAE/IE, CAE/R
Although the MPA program at the Maxwell School does not require students to take any core courses in information technology or security, it does offer a number of electives that explore relevant topics in IT and cybersecurity, including: cyber threats to U.S. infrastructure, cyber attacks waged by nation states, cybersecurity policy implications for governments, management

in the information age, privacy concerns and policies, encryption, IT and national security, and the impact of information technology upon foreign affairs. Aside from a dedicated course in "Cybersecurity and Policy," however, the other courses only explore these issues peripherally. MPA students pursuing the Certificate of Advanced Study in Security Studies or in IT Management and Policy are encouraged to enroll in these courses and take advantage of the many other research opportunities, educational programs and events offered by the Maxwell School Institute for National Security and Counterterrorism (INSCT). INSCT features cybersecurity as one of its main research areas and organizes conferences, workshops and speaker series on various aspects of this topic. Their project seeks to analyze and influence specific policies, create an interdisciplinary dialogue among scholars and practitioners, and educate future leaders on emerging topics in cybersecurity. Finally, as MPA graduate Eric Noggle explains: "MPA students have a great deal of flexibility to enroll in other departments. For example, the iSchool offers a Certificate in Information Security Management [with coursework in information security technology, policy, risk management, and evaluation] and MPA students can take any of these courses if they wish, as long as they meet the prerequisites."[43] Importantly, Syracuse University as a whole is one of the few schools assessed that has been designated as a National Center of Academic Excellence in both Information Assurance Education and Research. In sum, Maxwell MPA students interested in information technology and security issues have many opportunities to be exposed to these topics, especially in relation to policy, law enforcement, and international affairs.

Indiana University - School of Public and Environmental Affairs Bloomington, IN
(U.S. News Rank #2) NSA Cert: CAE/IAE, CAE/R
Indiana University was one of the country's first schools of public administration to offer an Information Systems (IS) concentration in its MPA program. Although the school does not emphasize the security aspects of ICT, it does address the growing gap between the number of graduates with IT skills and the number of places where such individuals can make an impact. The school also focuses on the application of IT to complex problems in organizational and environmental affairs. Only students concentrating in IS are required to take the courses in "Public Management Information Systems" and "Database Management Systems." Elective courses addressing other information technology and security issues, including: programming, digital economy, security for networked systems, and economics of security technologies, are offered for all MPA students through other departments at Indiana University—such as the Department of Computer Science, the School of Informatics, the Kelley School of Business, and the School of Library and Information Science. Moreover, MPA students interested in information security can take advantage of further learning opportunities in applied cybersecurity technology and policy at the Indiana University Center for Applied Cybersecurity Research.[44] Indiana University has also been designated as a National Center of Academic Excellence in both Information Assurance Education and Research. Aside from the students focusing on IS, it is not obvious from the MPA program website whether or not their graduates receive even a basic education in cybersecurity issues and how they relate to public affairs.

Harvard University - Kennedy School of Government Cambridge, MA
(U.S. News Rank #3) NSA Cert: N/A

MPA students at the Harvard Kennedy School (HKS) can design their individual plan of study and include electives from the broad array of courses available at HKS or through cross-registration with other graduate schools at Harvard University, MIT or The Fletcher School. Although none of the MPA core courses focuses on IT or cybersecurity, HKS does offer electives in "International Cybersecurity: Public and Private Sector Challenges," "Technology, Security, and Conflict in the Cyber Age" and "The Future of Cybersecurity." Students may also participate in the many cybersecurity events sponsored by the HKS Belfer Center for Science and International Affairs. In conjunction with MIT, the HKS Belfer Center launched an interdisciplinary research program called *Exploration in Cyber International Relations*.[45] The program focuses on ways in which cybersecurity affects the scope and complexity of international relations, and is designed to generate theory, policy, and strategy for how to address these challenges. Among the center's most prominent experts working on this project are: Joseph Nye (former chairman of the National Intelligence Council), Richard Clark (author of *Cyber War: The Next Threat to National Security*), and Melissa Hathaway (former director for cyberspace at the National Security Council). As Ms. Hathaway pointed out: "although the project includes research assistants and seminars open to all HKS students, unfortunately there is still no core cybersecurity requirement for any of the programs at Harvard University."[46] Thus, from the information provided, it appears that while HKS MPA students are not exposed to cybersecurity issues in their core curriculum, those who are interested in this field have the opportunity to work alongside some of the most prominent thinkers and practitioners in cybersecurity and deepen their understanding of the issues.

University of Georgia - School of Public and International Affairs Athens, GA
(U.S. News Rank #4) NSA Cert: N/A

The University of Georgia's MPA program offers very little with regard to cybersecurity issues and how they impact decision-making in the public sector. Students interested in IT and cybersecurity related topics "can seek courses in other departments of the university—such as the Computer Science Department," explains MPA Program Director Andrew Whitford.[47] The school mainly focuses on cybersecurity issues during the National Cyber Security Awareness Month of October, offering educational programs and services to enhance faculty, staff, and student understanding of the challenges posed in the digital age. Beyond this, however, the school does not offer much related to IT and cybersecurity.

Princeton University - Woodrow Wilson School Princeton, NJ
(U.S. News Rank #5) NSA Cert: CAE/R

At present, the Woodrow Wilson School (WWS) MPA curriculum does not include any core courses dedicated to information technology or cybersecurity. Some of its elective courses—such as "Making Networks Work", "Defense Policy Analysis" and "Negotiating with Iran over its Nuclear Program"—touch upon IT and cybersecurity issues peripherally. As explained by WWS staff members, students interested in cybersecurity related topics may cross-register for up to two courses at other academic departments of Princeton University, although this is usually discouraged because of the heavy load of the MPA curriculum. The Woodrow Wilson School's Center for Information Technology Policy offers lecture series and other special events that investigate cybersecurity policy topics and other aspects of how digital technologies in general interact with policy, markets, and society.[48] Finally, Princeton University as a whole has been designated as a National Center of Academic Excellence in Information Assurance Research, paving the way for further inclusion of cybersecurity research and courses in its various programs. In addition to fellowships and grants opportunities through the DoD Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program, the Scholars in the Nation's Service Initiative (SINSI) program at Princeton offers scholarships to encourage MPA or MPP students to pursue careers in government—focusing on various areas including cyber-warfare. Aside from these opportunities, however, MPA students do not receive a significant exposure to cybersecurity issues. In principle, the many programs and scholarships delineated above could offer the MPA and MPP curricula many ways in which to integrate a more robust cybersecurity component in the future.

New York University - Robert F. Wagner Graduate School of Public Service New York, NY
(U.S. News Rank #6) NSA Cert: N/A
The Wagner School's MPA program does not include any core requirements in IT or cybersecurity. It does offer, though, an elective course in "Information Systems in Public and Nonprofit Organizations," which covers IT organizational, technical and managerial aspects in the public sector. MPA students that choose to pursue cybersecurity related careers in the U.S. government are eligible to apply for the NYU ASPIRE award from the National Science Foundation and can take a set of interdisciplinary gateway courses offered through various NYU departments.[49] Further, the Wagner School participates in the NYU Center for Interdisciplinary Studies in Security and Privacy (CRISSP), which explores multidisciplinary approaches to privacy and cybersecurity challenges.[50] The CRISSP center offers seminars, lectures and interdisciplinary courses taught by faculty from the various NYU schools, including NYU-Poly, NYU Wagner, NYU Stern, NYU Steinhardt, and the NYU Courant Institute. The CRISSP course listing includes: "Economics of Networks," "Trust, Risk and Deception in Cyberspace," "Information Privacy Law" and "Psychology and Internet Security". "MPA Students interested in IT and cybersecurity can always discuss the possibility to enroll in other courses [at other NYU schools] with their academic advisor, especially if in relations to the ASPIRE fellowship," explained Admission Officer Marissa Jones.[51] Overall, MPA students at Wagner generally do not receive an education in the core tenets of cybersecurity, but can pursue extracurricular courses and events in this field throughout other NYU schools if they wish.

University of Southern California - Sol Price School of Public Policy Los Angeles, CA
(U.S. News Rank #6) NSA Cert: CAE/R
The MPA program at the Price School does not include information technology and cybersecurity courses in its curriculum. In 2004, however, USC-Price and the USC Viterbi School of Engineering established a National Center for Risk and Economic Analysis of Terrorism Events (CREATE), which is funded by the U.S. Department of Homeland Security.[52] In addition to serving as an academic program for the study of the risks, costs and consequences of terrorism, the Center has recently started hosting a series of cyber seminars and sponsoring studies on cyber threats and cybersecurity technologies. USC as a whole has also been designated as a National Center of Academic Excellence in Information Assurance Research. As Sarah Esquivel, MPA Assistant Director of Admission, explains: "The relationship with CREATE is becoming stronger and

students are well aware of the opportunities offered by the Center in this field. Students are also able to cross-register at other departments of the University of Southern California for courses in computer security."[53] Although it is hard to assess the actual influence of CREATE's cyber related initiatives in exposing all MPA students to cybersecurity issues in the public sector, the Center offers ways in which to integrate a more robust cybersecurity component into the MPA curriculum.

Carnegie Mellon University - Heinz School of Public Policy and Management Pittsburgh, PA
(U.S. News Rank #9) NSA Cert: CAE/IAE, CAE/R

The Heinz School offers a wide range of innovative degree programs in public interest fields, and prides itself for its particular strengths in information and technology management and public policy analysis. Unlike many graduate schools, the Heinz College is not organized along academic departments, and offers a broader M.S. in Public Policy and Management (MSPPM), instead of a regular MPA. Faculty from its two schools–the School of Public Policy and Management and the School of Information Systems and Management–collaborate on instruction and research to provide graduates with a better understanding of current trends in information technology in organizations, markets and societies, no matter what their concentration will be. As Associate Dean Brenda Peyser explains: "MSPPM students are required to take a core course in database management and then choose from at least one or more courses in information technology."[54] Students specifically interested in cybersecurity have the opportunity to choose among a wide variety of electives in the Technology Policy field, and gain valuable exposure to information security, information warfare, information assurance policy, U.S. and European information security policy, management of technological innovation, and privacy policy law. Graduates can also choose among other cybersecurity related courses offered at the Carnegie Mellon Tepper School of Business, the University of Pittsburgh Graduate School of Public and International Affairs, and any of the Pittsburg Council on Higher Education (PCHE) institutions. Moreover, the Heinz School offers regular lectures on technology and policy issues, and has instituted a dedicated M.S. in Information Security Policy and Management (MSISPM), which is at the vanguard of the cybersecurity sector with recognized leadership in risk management, data privacy, threat control and information policy.[55] Finally, CMU as a whole has also been designated as a National Center of Academic Excellence in Information Assurance Education, paving the way for further inclusion of cybersecurity research and courses in its various programs.

University of Kansas - School of Public Affairs and Administration Lawrence, KS
(U.S. News Rank #9) NSA Cert: CAE/IAE

The University of Kansas MPA program does not offer any core courses in information technology or cybersecurity. It does, however, offer one elective course in "Management and Information Technology" that includes aspects of information policy, implementation and management of ICT in governmental organizations. Moreover, the school organizes occasional cybersecurity related seminars "typically one to two hours in length conducted by practitioners," as Administrative Director Ray Hummert explained.[56] Finally, the school participates in the annual Cyber Security Awareness Month by organizing events on campus during that month to increase cybersecurity awareness and promote safe computing. Aside from these activities, however, the school offers very limited opportunities for MPA students to explore cybersecurity issues further.

University of Washington - Daniel J. Evans School of Public Affairs Seattle, WA
(U.S. News Rank #9) NSA Cert: CAE/IAE, CAE/R

The Evans School MPA program does not include any core or elective courses specifically dedicated to information technology or cybersecurity. MPA students that specialize in Science & Technology Policy, however, can take a handful of electives that address cybersecurity issues peripherally and "more courses may be added in the future," explained Director of Academic Services Ellen Weinstein. Moreover, "students interested in this area can take courses through the UW Information School and even earn a UW certificate with this specialization. The UW Educational Outreach also offers an online certificate in Information Assurance and Cybersecurity. [The Evan School] offers also seminars and special events related to cybersecurity."[57] In addition, the Washington University Center for Information Assurance and Cybersecurity (CIAC), a Center for Academic Excellence in both Information Assurance Education and Research, actively collaborates with the Evans School, among other departments, to integrate IA education and research in their curriculum.[58] This center offers elective courses, online classes and training programs in information assurance, network security, incident forensics and cryptology. Most of their current activities and research projects are highly technical, but the Center aspires to become a leader in the Pacific Northwest for research and education in information infrastructure protection and cyber-security issues. From the information collected, the MPA curriculum does not currently include a significant cybersecurity component, but could very much benefit from a further collaboration with CIAC to include more cybersecurity aspects in its program.

MPP Graduate Programs

U.S. News Ranking	College/University	School	City	State	Likert Scale Average Score	NSA Certification*
#1	University of California, Berkeley	Richard and Rhonda Goldman School of Public Policy	Berkeley	CA	2	N/A
#2	Harvard University	John F. Kennedy School of Government	Cambridge	MA	3	N/A
#3	University of Michigan	Gerald R. Ford School of Public Policy	Ann Arbor	MI	2	N/A
#4	University of Chicago	Harris School of Public Policy Studies	Chicago	IL	1	N/A
#5	Princeton University	Woodrow Wilson School	Princeton	NJ	1.5	N/A
#6	Duke University	Sanford School of Public Policy	Durham	NC	1.5	N/A
#7	Carnegie Mellon University	Heinz School of Public Policy and Management	Pittsburgh	PA	3.5	E, R
#8	Syracuse University	Maxwell School of Citizenship and Public Affairs	Syracuse	NY	3	E, R
#9	Indiana University	School of Public and Environmental Affairs	Bloomington	IN	1.5	E, R
#10	University of Wisconsin	Robert M. La Follette School of Public Affairs	Madison	WI	1	N/A

** Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

In recent years, there has been a gradual convergence between MPA and MPP programs. Today, the course offerings of most MPA and MPP programs overlap to some degree, even if MPP programs still tend to place more emphasis on policy analysis, research and evaluation, while MPA programs usually provide more focused coursework in program implementation and public management.[59]

University of California - Goldman School of Public Policy Berkeley, CA
(U.S. News Rank #1) NSA Cert: N/A
Although not specifically dedicated to IT and cybersecurity, core courses in the MPP curriculum at the Goldman School "provide students with a strong foundation in quantitative and analytical methods so that they can analyze any type of policy area, including information technology and cybersecurity issues," explained Assistant Dean for Academic Affairs Martha Chavez.[60] Moreover, the MPP program "offers elective courses in information technology and cybersecurity, including Professor Jason Christopher's course in "Information Technology and Public Policy" [and] Professor Michael Nacht's course in "US National Security Policy," which includes discussion of some cybersecurity issues". In addition, MPP students "have the opportunity to take classes all throughout the UC Berkeley campus, including at the School of Information," Haas School of Business and Berkeley Law. Finally, the Goldman School and UC Berkeley Computer Science are currently collaborating with the University of California Institute on Global Conflict and Cooperation (IGCC) to develop an interdisciplinary graduate training program to prepare the next generation of university researchers to address critical challenges in cybersecurity for industry and government.[61] The program plans to bring together faculty in computer science, political science, international relations, economics, public policy, and law, together with industry and government experts, to train students to examine gaps in cyber defense and develop new approaches to thwart and defeat cybercrime and attacks. From the information provided, MPP students interested in cyber issues have the opportunity to receive at least a basic education on the policy aspects of information technology and security, and the Goldman School will likely expand such offerings.

Harvard University - Kennedy School of Government Cambridge, MA
(U.S. News Rank #2) NSA Cert: N/A
MPP students at HKS are encouraged to explore different policy areas that interest them and can take advantage of "all the courses and opportunities offered by the four graduate degree programs and thirteen research centers at HKS," says MPP Director Deborah Isaacson.[62] Although none of the MPP core courses focuses on cybersecurity, the International and Global Affairs (IGA) concentration, geared toward students seeking to join the ranks of international policy wonk, has incorporated readings and case studies on cybersecurity in many of its elective courses. In addition, MPP students interested in cybersecurity can include other electives from the broad array of courses available at Harvard University or through cross-registration with other graduate schools (MIT and The Fletcher School). Finally, the all-star faculty and senior advisors working on the *Exploration in Cyber International Relations* project at the HKS Belfer Center for Science and International Affairs offer an additional incentive for MPP students to delve into cybersecurity matters and participate in cyber-related events and research opportunities.

*See MBA and MPA sections of this report for more information on Harvard University cyber-security courses, and the Belfer Center activities and research opportunities.

University of Michigan - Gerald R. Ford School of Public Policy Ann Arbor, MI
(U.S. News Rank #3) NSA Cert: N/A
The Ford School MPP program does not include any core or elective courses focused on information technology or cybersecurity. Professor Robert Axelrod, however, dedicates a week of his "International Security Affairs" course to this subject. Moreover, "the University of Michigan is known for its low administrative barriers to cross registration among departments—such as the School of Information and the Computer Science Department—and all students can also pursue a Science, Technology and Public Policy Certificate while enrolled in their degree program at the university," explained Director of Communication Laura Lee.[63] This certificate is dedicated to learning how science and technology are influenced by politics and policy, and includes various electives in computer networks, IT, technology policy analysis, and information law. Finally, the Ford School has offered some public lectures on cyber issues more broadly. Thus, although no specific courses or seminars on cybersecurity have been added to the MPP curriculum, MPP students can take advantage of the many other opportunities offered through the University of Michigan to learn more about cyber issues in the public policy field.

University of Chicago - Harris School of Public Policy Studies Chicago, IL
(U.S. News Rank #4) NSA Cert: N/A
Although there are no core requirements in information technology or cybersecurity, the MPP program at the Harris School includes one elective course in "Science, Technology, and Policy," which provides students with an introduction to science policy and some cybersecurity issues. Moreover, the school has organized few "mini-courses in this subject taught by practitioners," explained Director of Admission Maggie De Carlo.[64] Other than these initiatives, however, cybersecurity issues are not mentioned in other school's course syllabi or lecture topics.

Princeton University - Wilson School of Public and International Affairs Princeton, NJ
(U.S. News Rank #5) NSA Cert: N/A
* See MPA section of this report.

Duke University - Sanford School of Public Policy Durham, NC
(U.S. News Rank #6) NSA Cert: N/A
The Sanford School "does not offer a core course or an elective course exclusively dedicated to cybersecurity at the graduate (or undergraduate) level," explained Director of Program Development Helene McAdams.[65] Professor Tom Taylor, however, teaches "a survey course on contemporary issues in national security, during which [he] devotes part of one class to cyber attacks."[66] "Similarly, other national security courses may touch on the topic, but they do not focus on it exclusively," continued Ms. McAdams. Moreover, MPP students can cross-register for other cybersecurity related courses at other departments of Duke University—such as the School of Engineering. Although, "there is no regular conference focused exclusively on cyber security [at the Sanford School], there is, for example, an annual national security law conference at the Duke Law School and in recent years there have been panels on cyber security," explained Professor David Schanzer.[67] From the information gathered, it is still surprising that the courses in the MPP National Security specialization—specifically designed to prepare future policymakers and practitioners to address U.S. national security challenges—do not address more of the cybersecurity concerns in the national security policy agenda and debate.

Carnegie Mellon University - Heinz School of Public Policy and Management Pittsburgh, PA
(U.S. News Rank #7) NSA Cert: CAE/IAE, CAE/R
* See MPA section of this report.

Syracuse University - Maxwell School of Citizenship and Public Affairs Syracuse, NY
(U.S. News Rank #8) NSA Cert: CAE/IAE, CAE/R
* See MPA section of this report.

Indiana University - School of Public and Environmental Affairs Bloomington, IN
(U.S. News Rank #9) NSA Cert: CAE/IAE, CAE/R
* See MPA section of this report.

University of Wisconsin - Robert M. La Follette School of Public Affairs Madison, WI
(U.S. News Rank #10) NSA Cert: N/A

Although, La Follette public affairs programs do not include any core or elective courses in information technology or cybersecurity, they allow students to cross-register among departments at the University of Wisconsin with the permission of their advisor. The only courses that address specific aspects of cybersecurity are offered through the School of Library and Information Studies and focus on international cyber law and policy. Aside from these electives and a series of activities sponsored during the Cyber Security Awareness Month of October, however, MPP students do not seem to have other opportunities to be exposed to cybersecurity issues in the public sector.

IR Graduate Programs

"Stuxnet […] achieved, with computer code, what until then could be accomplished only by bombing a country or sending in agents to plant explosives."[68]

Foreign Policy Magazine Ranking	College/University	School	City	State	Likert Scale Average Score	NSA Certification*
#1	Georgetown University	Edmund A. Walsh School of Foreign Service	Washington	DC	3.5	E
#2	Johns Hopkins University	Nitze School of Advanced International Studies	Washington	DC	2	E, R
#3	Harvard University	John F. Kennedy School of Government	Cambridge	MA	3	N/A
#4	Princeton University	Woodrow Wilson School	Princeton	NJ	1.5	R
#5	Tufts University	The Fletcher School of Law and Diplomacy	Medford	MA	2.5	N/A
#6	Columbia University	School of International and Public Affairs	New York	NY	2	N/A
#7	George Washington University	Elliott School of International Affairs	Washington	DC	2.5	E, R
#8	American University	School of International Service	Washington	DC	2.5	N/A
#10	University of Chicago	Committee on International Relations	Chicago	IL	0.5	N/A

** Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

In 2010, top software-security experts and top government officials were shocked by the discovery of a drone-like computer virus, radically different from and far more sophisticated than any seen until then. The self-replicating virus was making its way through thousands of computers around the world, searching for a specific target. *The New York Times* reported that the Stuxnet worm was probably developed by the United States and Israel to disrupt Iran's nuclear program.[69] While its exact source has not been confirmed, Stuxnet was a blueprint for a new way of attacking large scale societal infrastructure without direct personal involvement and represented "the new face of 21st century warfare: invisible, anonymous, and devastating."[70] As the Stuxnet case illustrates, cyberspace is changing the character of national power, the structure of the international system and the more traditional aspects of power and security in international relations theory. Cyber instruments are being used as offensive weapons and tools of national power. Moreover, while cybercriminals' goals are pretty straightforward—seek profit and (for most part) steal—state-sponsored attackers' objectives are widely different and concern sabotage and espionage, and even chaos and destruction.[71] The lessons from these broad, and different but interconnected cyber threats need to be learned and a common cybersecurity vocabulary and theory need to emerge in order to properly understand and prepare for the inevitable cyber component of 21st century international relations.

It is fundamental for International Relations (IR) Master's programs, then, to start integrating a cybersecurity component into their curricula. After all, these are programs designed to produce graduates who have the skills needed to take on leadership roles in the international arena, from heads of state and ambassadors to leaders in politics, non-profit research institutes, public interest and policy advocacy organizations, intelligence agencies, business and global institutions. There exists no group with a greater need for understanding cybersecurity issues, as these issues are by definition global in scope and encompass all the ambiguities and challenges of an arena already concerned with state and non-state actors, international organizations, and global governance.

Most of the IR programs below have included case studies and elective courses that address some of the technical, military, commercial, legal, or policy aspects of cybersecurity. In addition, many of these universities sponsor conferences and seminars on cybersecurity and, in some cases, have even established specific cyber projects for the advancement of cybersecurity policy, laws, and strategies.

Georgetown University - Edmund A. Walsh School of Foreign Service Washington DC
(*Foreign Policy* Rank #1) NSA Cert: CAE/IAE
Georgetown University offers a variety of master's programs within the IR field, including a Master of Science in Foreign Service and a Master of Arts in Security Studies. The Security Studies Program (SSP), which is the academic pillar of the Center for Security Studies at the School of Foreign Service, includes core and elective courses in fundamentals of cybersecurity, emerging technology and security issues, information warfare and cyber law. These courses are comprehensive, covering everything from what cyberspace is, and what role it plays in civilian life and military operations, to how information systems upon which cyberspace is built work, what security means in that realm, and what characteristics of such systems (e.g. vulnerabilities) permit others to violate security in this domain. Other elective courses at the School of Foreign Service analyze countermeasures, including authentication, encryption, auditing, monitoring, intrusion

detection and firewalls, and other aspects of cyberspace law, law enforcement, information warfare and the military, and intelligence in the information age. In addition, "SFS hosts a Yahoo! Fellow each year. The current one, Francesca Musiani, will teach a course in Information Technologies – Innovations & Society, which includes elements of science and technology studies, sociology of socio-technical controversies and contentious politics, sociology of media, international communication, and international law," explained Associate Dean Jennifer Windsor.[72] Moreover, the School of Foreign Service is involved in a cyber project sponsored by Georgetown University's Institute for Law, Science, and Global Security.[73] This project was created in 2009 in response to the demand for policy development in conjunction with legal analysis of cybersecurity measures. General Michael Hayden, former director of the National Security Agency, has joined the project as a senior advisor and will help the institute better integrate law, policy and technology to tackle the issue of cybersecurity. The institute organizes workshops, seminars and conferences that bring together policymakers, academics and key industry stakeholders from across the globe to explore ways to integrate cybersecurity in different disciplines. Georgetown University has also been designated as a National Center of Academic Excellence in Information Assurance Education. In sum, Georgetown IR students interested in information technology and cybersecurity issues have many opportunities to be exposed to these topics, especially in relation to national security, policy, law enforcement and international affairs.

Johns Hopkins University - Nitze School of Advanced International Studies Washington DC
(*Foreign Policy* Rank #2) NSA Cert: CAE/IAE, CAE/R
Although the SAIS curriculum does not have any core requirements in information technology or cybersecurity, it offers one elective course in "National and International Dimensions of Cybersecurity," which explores intra- and international aspects of cybersecurity from a theoretical and policy perspective. Other electives in the strategic studies concentration may also address these topics peripherally. Johns Hopkins as a whole houses one of the top-ranked graduate programs in information security and information assurance in the country, and allows IR students to cross-register for specific courses that may interest them. Despite the overall strength of its academic programs, however, SAIS has not yet fully-integrated cybersecurity issues into its curriculum, and it has not placed as much emphasis on the security aspects of cyber-threats as some other institutions.

Harvard University - John F. Kennedy School of Government Cambridge, MA
(*Foreign Policy* Rank #3) NSA Cert: N/A
*See MPA and MPP sections of this report.

Princeton University - Wilson School of Public and International Affairs Princeton, NJ
(*Foreign Policy* Rank #4) NSA Cert: CAE/R
* See MPA section of this report.

Tufts University - The Fletcher School of Law and Diplomacy Medford, MA
(*Foreign Policy* Rank #5) NSA Cert: N/A
The M.A. in Law and Diplomacy (MALD) at The Fletcher School is known for the flexibility of its curriculum that allows students to explore their particular area of interest and take advantage of multiple research opportunities. Although none of the Fletcher courses is exclusively dedicated to IT and cybersecurity, some of the faculty have started to integrate readings and case studies on

cyber issues to part of the coursework in each of the three major international affairs divisions—International Law and Organizations; Diplomacy, History, and Politics; and Economics and International Business. For example, Professor William Martel dedicates one to several weeks to cyber issues, including cyber attacks, cybercrime, cyber defense, and cyber strategy, in each of his policy, technology and international security courses.[74] Every year, at least one of the public policy course's final projects consists of an NSA simulation of a cyber crisis or cyber attack against the United States. Other Fletcher courses, including "Proliferation-Counterproliferation and Homeland Security Issues," "Crisis Management and Complex Emergencies," "International Intellectual Property Law and Policy" and even "The International Legal Order," now include aspects of cyber conflict, cyber crisis prevention and management, international laws in cyberspace, IP and technology law. Throughout these courses, students are encouraged to think analytically and critically about these issues and some of them are exploring cyber issues further in their final capstone projects. Moreover, a Cyber Policy Working Group of 10-15 MALD students, guided by Professor Martel, is currently working to create a *Code of Conduct for Cyberspace for States, Firms, and Individuals* in conjunction with MIT Lincoln Laboratory. This group is analyzing and researching prior and current activity in cyberspace so as to inform and direct behavior. In addition, The Fletcher School sponsors a series of roundtables and conferences on contemporary global issues, including cybersecurity, and organizes an annual crisis management exercise (SIMULEX), which allows participants to play roles as decision-makers on the international scene and experience the problems and processes of managing a crisis or resolving a conflict. Past SIMULEX scenarios have included staged cyber attacks and cyber crisis.[75] Finally, the Fletcher programs can be supplemented through joint partnerships with Harvard University and MIT, among others, which offer other courses and events on cybersecurity issues. Fletcher students, especially those focusing on International Security Studies, have various opportunities to be exposed to cybersecurity challenges in the international arena, and gain a broader perspective on cyber-related issues.

Columbia University - School of International and Public Affairs New York, NY
(*Foreign Policy* Rank #6) NSA Cert: N/A

The M.A. in International Affairs (MIA) at Columbia's School of International and Public Affairs (SIPA) encourages students to tailor their specific course of study to fit their academic and career interests. Although the school does not offer any core courses in information technology and cybersecurity, the International Security Policy (ISP) concentration includes a course in "Cybersecurity" that explores the evolution of cyberspace and its impact on national security, the commercial environment and individuals, and one in "Technology and National Security," which focuses on how military and intelligence related technological innovations are applied in the context of national security. "We are exploring the possibility of a cybersecurity focus within the ISP program for the future," explained ISP Coordinator Jessica Baen.[76] In addition, "ISP students can take any elective offered within the MIA/MPA program (and with some restrictions within the rest of the university–PoliSci, Law, etc.), so long as it doesn't conflict with their required courses." International and Public Affairs Professor Abraham Wagner added that "Columbia students can cross-register for the Cybersecurity" course and that "mostly law students do this."[77] Moreover, The Saltzman Institute for War and Peace Studies (SIWPS) offers regular events on topics related to security that are open to students and, as Ms. Baenis added, it is currently "working on a conference in cybersecurity with the Defense Advanced Research Projects Agency (DARPA) for this summer." SIPA's Defense and Security Student Organization (DSSO) has also hosted events about cybersecurity in the past. SIPA students, especially those focusing in ISP, have the opportunity to receive at least a basic education in cybersecurity and other technology aspects of national security.

George Washington University - Elliott School of International Affairs Washington DC
(*Foreign Policy* Rank #7) NSA Cert: CAE/IAE, CAE/R

The Elliott School of International Affairs offers a variety of MA degrees, but none of its IR fields of study have a strong IT or cybersecurity component at this time. The Center for International Science and Technology Policy at the Elliott School offers an elective course in "Cybersecurity" which provides students with an introduction to major debates over this issue, concentrating on the policy rather than the technical aspects. Professor Scott Pace has also pointed out how "other courses in International Science and Technology (S&T) Policy and S&T in National Security touch on information technology security and policy."[78] IR students interested in this field have also the opportunity to participate in other GW-affiliated events and choose additional classes from other schools within the university, which in some cases have already carved their own niche degrees in cybersecurity in response to industry demand.[79] George Washington University is now sponsoring a Cybersecurity Initiative to bring together all of their cybersecurity graduate education programs with the work of the GW's Cyber Center for National and Economic Security and the Cyber Security Policy and Research Institute in an integrated and interdisciplinary approach.[80] Further, GW has been designated as a National Center of Excellence in both Information Assurance Education and Research. GW seems to have a number of advantages that most of other programs in this survey do not. GW hosts prolific research centers and graduate programs that already promote technical research, national and economic examination, and policy analysis of problems that have a significant computer security and information assurance component; takes advantage of the relevant work and research opportunities in cybersecurity technology and policy offered by its central location in Washington, DC; and forges strong bonds with government and private organizations. All these aspects together could position GW at the forefront of cybersecurity research, education, and policy, but the Elliott School is not leading these efforts.

American University - School of International Service Washington DC
(*Foreign Policy* Rank #8) NSA Cert: N/A

The School of International Service (SIS) at American University offers a variety of degree programs and certificates within the IR field, some of which have started to integrate cybersecurity topics in their electives. For example, the International Communication program offers a course in "Cyber-Conflict in Global Perspective," and both the "Strategic Communication, Intelligence & National Security" and the "Theater of Terror: Modern Terrorism & Mass Media" courses address different aspects of cybersecurity. Students in other programs can choose from a few other special topics courses that, even if not exclusively dedicated to cybersecurity, touch upon information technology, cybercrime, cyber espionage and cyber warfare and examine the role of these issues in national and transnational security. Qualified graduates also have the opportunity to enroll in courses at any of the institutions in the Consortium of Universities of the Washington Metropolitan Area to complement their programs, particularly in specialized interest areas like cybersecurity. Lastly, like many of the universities analyzed, AU as a whole sponsors a series of activities during the

Cyber Security Awareness Month of October. In short, IR students, especially those focusing on International Communication, have the opportunity to explore cybersecurity issues in international affairs and national security, if personally interested in doing so.

University of Chicago - Committee on International Relations Chicago, IL
(*Foreign Policy* Rank #10) NSA Cert: N/A

The IR graduate program at the University of Chicago focuses on the more intellectual side of international affairs. The Committee on International Relations (CIR) at the University of Chicago is a predominantly "interdisciplinary program that takes advantage of coursework offered across the university's ten academic departments and professional schools," explained Student Affairs Administrator E.G. Enbar.[81] For example, students interested in cyber issues can take "a couple of courses that touch upon cyber intrusion and cyber warfare [and attend a few conferences on privacy issues in cyberspace] at the Law School." Because the structure of the international relations program at Chicago is driven by the priorities and offerings of other disparate departments, however, its ability to offer comprehensive education in cybersecurity issues is limited. "At present, none of the core coursework available to CIR students covers explicit cyber issues, but if faculty focus and student interest in cybersecurity issues motivates the offering of new courses, they would be included in the CIR course list," added CIR alumnus Steven Stashwick.[82]

LLM Graduate Programs

"If a cyber attack produces death, damage, destruction or high-level disruption that a traditional military attack would cause, then it would be a candidate for 'use of force' consideration."[83]

U.S. News Ranking	College/University	School	City	State	Likert Scale Average Score	NSA Certification*
#1	Yale University	Yale Law School	New Haven	CT	0.5	N/A
#2	Stanford University	Stanford Law School	Berkeley	CA	3	N/A
#3	Harvard University	Harvard Law School	Cambridge	MA	3	N/A
#4	Columbia University	Columbia Law School	New York	NY	2	N/A
#5	University of Chicago	The University of Chicago Law School	Chicago	IL	1.5	N/A
#6	New York University	New York University School of Law	New York	NY	1.5	N/A
#7	University of California, Berkeley	Berkeley Law	Berkeley	CA	2	N/A
#7	University of Pennsylvania	Penn Law School	Philadelphia	PA	2	N/A
#7	University of Virginia	University of Virginia School of Law	Charlottesville	VA	1	N/A
#10	University of Michigan	University of Michigan Law School	Ann Arbor	MI	1	N/A

** Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

In 2008, websites of the Republic of Georgia suffered numerous defacements and distributed denial-of-service (DDoS) attacks that shut down Internet access prior to the country's invasion by Russian forces. This represented the first instance of large-scale computer network attack occurring simultaneously with a conventional international armed conflict.[84] Targets included the websites of the President, Parliament, Foreign Affairs, Defense and Education ministries, domestic and foreign media, banks, and private Internet servers and blogs.

Although the identity of the originators of these cyber attacks remains uncertain, most of the operations were traceable to Russia. Proving the origin or motive of similar cyber attacks can be very difficult as attackers can route their intrusions through servers in other countries to make attribution difficult (for example, many of the attacks on Georgian targets were routed through American servers).[85] Attribution represents one of the main obstacles to legal restraints regarding cyber malfeasance, especially when cyber attacks originate outside the territory of the victim state. The enforcement, or lack thereof, of international laws on cybercrime constitutes another of the main challenges in international cybersecurity governance. Without effective international cybercrime laws, cyber attackers can escape prosecution by basing themselves in countries that do not punish or extradite for their offenses, and states can avoid taking responsibility for cybercrimes carried out abroad by cyber criminals and terrorist organizations within their borders.

Scholars and practitioners of international law are becoming increasingly sensitive to the challenges cyber warfare poses to norms, particularly international humanitarian law (IHL) or the law of armed conflict. As shown by the Georgian case, cyber operations have become embedded in modern warfare. Professor Michael Schmitt, director of the International Group of Experts tasked by NATO with crafting a *Manual on the International Law of Cyber Warfare*, eloquently explains that:

> The dilemma is that IHL was crafted during a period in which the cyber operations were but science fiction. However, today no modern military enters the battlespace without at least some reliance on computers and computer networks. […] And as demonstrated in the case of the Georgia-Russia conflict, civilian cyber assets are an especially attractive target set, not only for militaries, but also for individuals or groups intent on involvement in the conflict in question. IHL must respond to the challenges posed by this new technology.[86]

Attribution, cybercrime laws, and the application of international laws to conflicts in cyberspace are only some of the legal issues related to the use of the Internet that post-graduate degrees in law (LLM) will have to tackle to prepare future lawyers and academics to respond to the legal challenges posed by cyber threats. Most of the law schools analyzed have realized that lawyers preparing to practice in the 21st century will need to understand and address a host of new legal issues that derive from the emergence of information and communications technologies and global digital networks, and have started to integrate courses that explore specific problems in applying law to cyberspace in areas such as international law, intellectual property, online speech, anonymity, privacy, antitrust content, control, and the bounds of jurisdiction.

Yale University - Yale Law School New Haven, CT
(U.S. News Rank #1) NSA Cert: N/A

Yale Law School (YLS) offers a highly competitive LLM program designed for students committed to a career in teaching law. Although there is no course specifically dedicated to cybersecurity, the seminar on "International Law and Foreign Relations" has researched different topics in current legal debates, including the law of cyber-attack. As pointed out by Director of the YLS Center for Global Legal Challenges and International Law Professor Oona Hathaway, this seminar produced articles on cyber attacks, cybercrime and cyber warfare, and how these threats are regulated by existing bodies of law, including the law of war, international treaties and domestic criminal law.[87] Moreover, the "Internet Privacy" course explores how the Internet and other technologies are changing the privacy landscape, and how courts, legislatures, agencies, advocacy groups, and legal commentators are responding. From the information provided, however, YLS does not seem to offer LLM students other opportunities to explore cyber law related issues.

Stanford University - Stanford Law School Stanford, CA
(U.S. News Rank #2) NSA Cert: N/A

Stanford Law School (SLS) prides itself for its interdisciplinary education that encourages student to explore the many ways law intersects with other fields. Its LLM program in Law, Science & Technology (LST) provides academic and professional training in legal practice and interdisciplinary analysis related to developments in law and technology areas, including e-commerce, jurisdiction and dispute resolution in cyberspace, intellectual property regimes and contractual developments related to the global information economy.[88] Although there are no core requirements in information technology and cybersecurity, LLM students concentrating in LST can develop an individualized course of study and choose from a variety of cyber-related electives, such as "Cyberlaw: Difficult Problems," "Internet Business Law and Policy," "Internet Torts and Crimes," "Law and Virtual World," "Intellectual Property: Strategy for Technology Company," and "Communication Law: Internet and Telephony." LLM students also have the opportunity to participate in the hands-on experience of representing clients in cutting-edge issues of intellectual property and technology law, in the public interest. For example, in the project-oriented seminar "Cyberlaw/Fair Use Clinic", students work on a wide range of cyberlaw projects with lawyers from the Center for Internet and Society's Fair Use Project and with lawyers from the Electronic Frontier Foundation. Moreover, the LST program includes six related programs and centers each with its own more specific focus: the Center for E-Commerce, the Center for Internet and Society (CIS)[89], the Center for Law and the Biosciences, the Stanford Center for Computers and Law (CodeX), the Stanford IP Litigation Clearinghouse, and the Transatlantic Technology Law Forum. LLM students are also encouraged to attend other seminars and lectures on campus that are relevant to topics discussed during their required LST colloquium. From the information presented, Stanford LLM curriculum, especially for the LST Program, seems to have the most comprehensive cyber component of all the LLM programs analyzed in this survey and offers students the opportunity to delve into legal cybersecurity matters in a classroom setting and through experiential learning. In principle, SLS has a number of advantages that many of other programs in this survey do not—including renowned faculty experts proponent of experiential learning, prominent cybersecurity visiting scholars and scientists, alumni practicing on the cutting edge of technology law, a relevant study of science- and technology-driven law and policy, and a location in the heart of Silicon Valley.

Harvard University - Harvard Law School Cambridge, MA
(U.S. News Rank #3) NSA Cert: N/A
The Harvard University LLM program encourages students to design their own course of study within set parameters and even pursue a limited number of credits at other Harvard schools, the Fletcher School and MIT. LLM students particularly interested in the intersection of law, technology and cybersecurity, can choose from a variety of electives in the intellectual property, cyberlaw and technology areas of study, such as "Communication and Internet Law and Policy," "Controlling Cyberspace," "Cybercrime," "Cyberlaw and Intellectual Property," "Practical Lawyering in Cyberspace," and "Ideas for a Better Internet." Through these courses, LLM students are encouraged to think analytically about these issues and explore the complex challenges of effectively representing clients in a wide variety of disputes. For example, the "Practical Lawyering in Cyberspace" course uses a set of cyberlaw-related case studies drawn from recent legal controversies to address a broad range of experiences lawyers may encounter in the actual practice of law. The Harvard Berkman Center for Internet & Society, whose mission is to explore and understand cyberspace, share in its study, and help pioneer its development, is responsible for most of these course offerings.[90] The Center, in conjunction with other Harvard schools and MIT, supports the traditional Harvard Law School curriculum with various cyberspace-related courses, and sponsors gatherings that bring together members of their diverse network of participants to share ideas about what the Internet can become. The Center has recently developed a Cybersecurity Wiki, designed to be a set of evolving resources on cybersecurity for researchers, technologists, students, policy-makers, and others interested in cybersecurity issues more broadly.[91] LLM students also have the opportunity to participate in a "Cyberlaw Clinic" at the Berkman Center and enhance their preparation for high-tech practice by working on a variety of real-world litigation, client counseling, advocacy, legislation, and transactional/licensing projects and cases regarding cutting-edge issues of the Internet, new technology and intellectual property. In brief, Harvard LLM students interested in this field have the opportunity to effectively explore the legal challenges and opportunities of cyberspace while pursuing their LLM degree.

Columbia University - Columbia Law School New York, NY
(U.S. News Rank #4) NSA Cert: N/A
Columbia offers a general LLM degree that gives students much freedom to select their courses from the Law School's curriculum. Although there is no core course in information technology and cybersecurity, LLM students interested in this area can enroll in the "Computer, Privacy and the Law" course, which includes aspects of intellectual property, encryption and communications privacy in relation to law enforcement and government intelligence gathering; or cross-register for the "Cybersecurity" course at SIPA. Other law courses of interest include: "Law in the Internet Society," "Internet and Computer Crimes," and "Life, Liberty and Liability in the Digital Millenium." However, all the law courses are primarily focused on the legal challenges and opportunities of cyberspace and very little attention seems to be given to technology or policy aspects of cybersecurity. Moreover, the Columbia Law School Roger Hertog Program on Law and National Security tries to expose law students to real-world challenges and dilemmas facing government officials, and has hosted lectures on cybersecurity and supported the scholarship of national security experts focusing on the domestic and international legal aspects of cyber-warfare and cyber-terrorism. The Richman Center for Business, Law, and Public Policy at Columbia

University—a joint venture of Columbia's Business and Law Schools—offers lectures on emerging policy issues at the nexus of law and markets, including cyber threats and cybersecurity. Columbia LLM students interested in cybersecurity and cyberlaw have many opportunities to enhance their theoretical knowledge of this area of study, even if they do not receive the same level of exposure to its practical application in a legal forum as their Stanford and Harvard counterparts do.

University of Chicago - Chicago Law School Chicago, IL
(U.S. News Rank #5) NSA Cert: N/A
LLM students at the University of Chicago have the flexibility to create their own programs and choose courses and seminars that reflect their interest. However, the only courses that touch upon some of the legal, technological and policy aspects of cybersecurity are: "Computer Crime," "Electronic Commerce Law," "Counterintelligence and Covert Action" and "Developing Law Practice Skills through the Study of National Security Issues." The University of Chicago Law School has also hosted a few conferences on the legal and ethical issues of intellectual property, privacy and free speech in cyberspace. In brief, LLM students have limited opportunities to familiarize with cybersecurity issues and only if personally inclined to pursue this interest.

New York University - School of Law New York, NY
(U.S. News Rank #6) NSA Cert: N/A
NYU Law School offers nine different LLM degrees to meet students' personal and professional objectives. Although none of the specializations focuses on technology law or dispute resolution in cyberspace, students interested in these topics can choose from a limited number of courses, such as "Cyberlaw: Internet Points of Control," "Technological Impact on Contracts in the Digital World," "Key Readings in Information Law and Policy," and "Anonymity and Accountability on the Internet." Students may also pursue academic opportunities within the larger university by taking a limited number of cyber-related courses at NYU's other schools, or participating in the many events and lectures on privacy and cybersecurity challenges sponsored by the NYU Center for Interdisciplinary Studies in Security and Privacy (CRISSP). From the information available, however, it is not clear if LLM students at NYU Law School gain a significant education in cybersecurity matters and how they relate to the law, aside from what it is offered in the few relevant electives.

University of California - Berkeley Law Berkeley, CA
(U.S. News Rank #7) NSA Cert: N/A
Berkeley Law's LLM students can tailor their course of study to meet their individual needs and choose from among all the courses and seminars offered to JD students. Those who seek in-depth training in a particular area of law, such as Law and Technology, can also earn a Certificate of Specialization in this field. Berkeley Center for Law and Technology (BCLT) claims to offer the most comprehensive instructional program in law and technology and to take advantage of its location near Silicon Valley to reach out to Bay Area law firms and leading technology companies and forge a strong technology law community.[92] Although its main focus is on intellectual property, copyright and patent law, the Law and Technology course listing includes electives in "Cyberlaw," "Computer Law," "Information Privacy Law," and "Silicon Valley Antitrust." Moreover, the center has hosted a few lectures and seminars on cyberwar law, ethics and policy. Other BCLT

opportunities for students to develop their skills in this field include working with the Samuelson Law, Technology and Public Policy Clinic and the Berkeley Technology Law Journal, the first student-edited journal to focus on the intersection of law and technology. Although none of the courses focuses on cybersecurity policy or technology, LLM students interested in cyber issues have the opportunity to receive a strong education and training in cyberlaw and many other areas of constitutional, regulatory and business law that are affected by new technologies.

University of Pennsylvania - Penn Law School Philadelphia, PA
(U.S. News Rank #7) NSA Cert: N/A
Penn Law LLM students have to choose between a 'course track' and a 'thesis track' but can elect from a variety of law school classes to fit their interests. One of Penn Law's specialty areas is Intellectual Property and Technology Law, which includes courses such as "Computer Crime Law," "Cybercrime," "Privacy and Data Protection," and "Technology Policy." The University of Pennsylvania Law School has also hosted roundtables on Cyberwar and the Rule of Law, and the Changing Face of Warfare. Moreover, Penn Law Center for Technology, Innovation and Competition, which is dedicated to promoting research and discussion on technology policy among legislators, regulatory authorities, and scholars, has sponsored various conferences and workshop series on Internet policy, information privacy, and cloud computing.[93] From the information available, Penn Law LLM students interested in cyberlaw and cybersecurity have the opportunity to choose from a few specialized courses and attend related events offered throughout the year but like for most universities, only if personally inclined to do so.

University of Virginia - School of Law Charlottesville, VA
(U.S. News Rank #7) NSA Cert: N/A
University of Virginia LLM students can choose from a variety of courses and seminars in different fields of legal study to pursue their personal and professional objectives. Although it is not the primary focus of any of the courses offered at UVA School of Law, few faculty members conduct "research regarding the laws related to the Internet and telecommunications," explained Law School's chief administrative officer Stephen Parr. For example, the Criminal Justice and the Intellectual Property concentrations include a seminar in "Cybercrime" which touches upon cyber law, intellectual property and international legal issues. The course "Law of War: Contemporary Debates" covers some legal aspects of cyber weapons and other new technologies. UVA Law School has also hosted a few panels on cybercrime and efforts to combat cybercriminals. From the information collected, UVA Law School offers very limited opportunities for its LLM students to explore specific cybersecurity and cyberlaw issues at this time.

University of Michigan - Law School Ann Arbor, MI
(U.S. News Rank #10) NSA Cert: N/A
University of Michigan LLM students are free to select any of the courses and seminars offered to JD students to meet their personal interests. The Michigan Law School curriculum includes "several Internet related courses—such as "Law in Cyberspace" and "Computer Crimes"—although not one focusing specifically on cybersecurity," explained Professor Jessica Litman.[94] In addition, the "Intellectual Property Workshop" features presentations of works in progress by leading scholars on topics related to intellectual property, information policy and Internet regulation. The University

of Michigan Law School once offered a Microsoft Fellowship in Law, Economics, and Technology to support research in areas of Intellectual Property, Telecommunications, Internet and Cyberlaw and other areas related to information and technology. The post-doc fellowship, however, is no longer offered because Microsoft has chosen to only fund faculty-related research, according to former Law School Program Coordinator Alonzo LaGrone.[95] Consequently, LLM students have few incentives and opportunities to pursue the study of cybersecurity and cyberlaw, and only those who had a previous interest in this field will probably choose to do so.

Criminal Justice Graduate Programs

> ***"It's important that everybody understands that if you have a computer that is outward-facing—that is connected to the web—that your computer is at some point going to be under attack."[96]***

U.S. News Ranking	College/University	School	City	State	Likert Scale Average Score	NSA Certification*
#1	University of Maryland, College Park	College of Behavioral and Social Sciences	College Park	MA	2	R
#2	University at Albany-SUNY	School of Criminal Justice	Albany	NY	1.5	N/A
#3	University of Cincinnati	School of Criminal Justice	Cincinnati	OH	0	N/A
#4	University of Missouri	Department of Criminology and Criminal Justice	Saint Louis	MO	0	N/A
#5	Pennsylvania State University	Department of Sociology & Crime, Law and Justice	University Park	PA	0	E, R
#7	Rutgers- State University of New Jersey	Rutgers School of Criminal Justice	Newark	NJ	0	E, R
#5	University of California, Irvine	School of Social Ecology	Irvine	CA	1	R
#7	Florida State University	College of Criminology and Criminal Justice	Tallahassee	FL	1	E, R
#7	Michigan State University	School of Criminal Justice	East Lansing	MI	1	N/A
#10	CUNY-John Jay College	John Jay College of Criminal Justice	New York	NY	2.5	N/A

* *Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

Advances in information and communication technologies have created a host of crimes that did not previously exist. Cyberspace offers fertile ground for a variety of crimes, including distributed-denial of service (DDoS) attacks, phishing, digital piracy, cyber-stalking, cyber-bullying, cyber-terrorism, cyber-pornography, Internet fraud, and identity theft. These attacks affect governments, corporations, and private citizens alike with widespread and often debilitating damage.

According to one estimate, cybercriminals create nearly 60,000 fake websites per week—often mimicking the homepages of companies like eBay, Visa, Amazon, PayPal, and Bank of America—in an effort to steal information from others.[97] Victims of identity theft often become aware of the attack well after it occurred, and undoing the damage from the attack can take months. An even bigger concern, however, stems from cyber-criminals who steal data and intellectual property from corporations. There are millions of consumer records stolen annually and the content of that data can be staggering. While the costs of cyber-crime are hard to measure, it is generally believed to cost billions of dollars in losses each year.[98] The scope and enormity of cyber threats—not just to individuals and private corporations but also to the country's heavily networked critical infrastructure—was spelled out during FBI Director Robert Mueller's testimony to a Senate homeland security panel last September. "Computer intrusions and network attacks are the greatest cyber threat to our national security," Mueller said.[99]

The rise of Internet criminality has led to the growth of cyber criminology as a distinct discipline within the broader criminology framework. Criminology programs traditionally combine the principles of sociology, law, psychology, and public administration so that students understand the criminal justice system and can work to prevent crime. There is an urgent need for these programs to include analysis of the ethical, legal, cultural, and technical issues posed by cyber threats. The law enforcement and criminal justice personnel of the 21st-century will need training in cybersecurity—including the study of cyber threat analysis, cybercrime laws, cybercrime investigations, etc.—in order to prevent, mitigate and respond to the threat posed by cyber criminals.

Few of the criminal justice programs analyzed below have added a cyber criminology component to their curricula. Other universities, however, are starting to offer on-campus and online certificates and master's degrees in cybersecurity within their criminal justice programs. These developments underscore the importance of understanding cybercrimes so that the next generation of network security analysts, information assurance specialists, consultants, cybersecurity investigators, and other professionals can protect our nation's infrastructure.

University of Maryland - College of Behavioral and Social Sciences College Park, MD
(U.S. News Rank #1) NSA Cert: CAE/R
The Department of Criminology and Criminal Justice at the University of Maryland (UMD) does not currently offer any graduate level course in cybercrime or cyber forensics. Assistant Professor of Criminology and Criminal Justice David Maimon, however, applies criminological concepts and research methods to his own work on computer hacking, system trespassing, and computer networks vulnerabilities to cyber attacks. Professor Maimon is designing a graduate level course that will have "students work with network data and apply criminological, psychological and sociological theories and constructs in the study of computer focused crimes."[100] He emphasizes that "criminological insights in the study of cybercrime are important, since they may support the development of concrete security policies that consider not only the technical element of cybercrime but also the human component."[101] In addition to Professor Maimon's work, the Department offers graduate students the opportunity to take advantage of the multiple research opportunities, events, and graduate level cybersecurity courses offered by the Maryland Cybersecurity Center (MC2). MC2's unique approach is to bring together experts from both the computer science and engineering departments and other non-technical fields—such as economics and social sciences—to offer more comprehensive cybersecurity education opportunities and interdisciplinary solutions.[102] More broadly, UMD has been designated as a National Center of Academic Excellence in Information Assurance Research and recently launched the country's first Honors undergraduate program in cybersecurity. In principle, UMD's proximity to the nation's

capital and close interactions with key federal agencies, its efforts to facilitate the growth of the cybersecurity profession, and MC2's comprehensive approach to cybersecurity education, research and technology development make this university an ideal place to educate future leaders. From the information collected it remains surprising, though, that the Department of Criminology and Criminal Justice has yet to take advantage of the many resources UMD offers to integrate a stronger cybersecurity component in its graduate criminology curriculum.

University at Albany–SUNY - School of Criminal Justice Albany, NY
(U.S. News Rank #2) NSA Cert: N/A
The School of Criminal Justice at the University at Albany-SUNY offers a M.A. in Criminal Justice with a concentration in information technology, which focuses on the collection, protection, storage, manipulation, interpretation and communication of data. Only graduate students who choose this concentration have to take a core course in "Fundamentals of IT" and then focus on other IT-related courses instead of an equivalent number of electives in other fields. All Criminal Justice students, however, can choose among elective courses dedicated to information systems and technology, information security, and the policy, legal and ethical implications of the use of information technology in criminal justice. It is not clear from the information provided if the School of Criminal Justice sponsors any additional seminars or conferences on cybercrime, or if graduates are able to cross-register at other departments of the University at Albany to seek more courses on cyber-related issues. Nonetheless, Criminal Justice students at SUNY-Albany, especially those focusing in IT, seem to have the opportunity to receive at least a basic education on the technical, security and policy aspects of cyber criminology during their graduate studies.

University of Cincinnati - School of Criminal Justice Cincinnati, OH
(U.S. News Rank #3) NSA Cert: N/A
The M.S. in Criminal Justice at the University of Cincinnati does not offer any courses or seminars on cybersecurity or cyber criminology. They have, however, incorporated some aspects of these topics at the undergraduate level and likely will expand such offerings. Academic Director Jean Gary confirmed that "similar course work is going to be developed into graduate level work."[103]

The **University of Missouri–St. Louis** (U.S. News Rank #4), **Pennsylvania State University–University Park** (U.S. News Rank #5), and **Rutgers-State University of New Jersey–Newark** (U.S. News Rank #5) have yet to include an information technology and cyber criminology component to their criminal justice and criminology graduate curricula. At most, the schools have computer science or engineering departments that offer bachelor degrees and courses in network security, cryptography, programming and digital forensics.

University of California - School of Social Ecology Irvine, CA
(U.S. News Rank #5) NSA Cert: CAE/R
The Department of Criminology, Law and Society at the University of California School of Social Ecology offers an online Masters of Advanced Study (MAS) in Criminology, Law and Society, which is designed for experienced legal and criminal justice professionals. Although it is not part of any of the core requirements, electives in "Cybercrimes, Investigation, Forensics, and Prosecution," "Science and Law," and "White-Collar Crime" cover different aspects of computer crimes and

intellectual property in the digital era. Because of the structure of the online program, students can only take courses offered for the criminology master degree. With the exception of the courses listed above, students do not seem to have other opportunities to explore cybersecurity issues related to criminal justice.

Florida State University - College of Criminology and Criminal Justice Tallahassee, FL
(U.S. News Rank #7) NSA Cert: CAE/IAE, CAE/R
The College of Criminology and Criminal Justice (CCJ) at Florida State University does not currently offer any courses in cybercrime, network security or other aspects of cyber criminology. CCJ Director of the Graduate Program Professor Carter Hay, however, has pointed out that: "CCJ in conjunction with the Computer Science Department at FSU, offers an M.S. in Computer Criminology. For this degree, students take a number of traditional criminology courses from CCJ on criminological theory, criminal justice, and so on. From the Computer Science Department, students take a number of network security courses (along with related prerequisites)."[104] Participation in this program may be limited given that it is highly technical and requires a pre-existing competency in computer programming.

Michigan State University - School of Criminal Justice East Lansing, MI
(U.S. News Rank #7) NSA Cert: N/A
The School of Criminal Justice at Michigan State University (MSU) offers both an online and on-campus master's degree in Criminal Justice (CJ) and seven graduate certificate programs in various areas of criminology. It is also currently developing a new certification in information security. At the moment, graduate students interested in cybersecurity can combine their coursework in criminal justice with other academic areas—such as computer science. In addition, "CJ students can take as undergrads a course in 'Cybercrime and Cybersecurity' and one in 'Topics in Cybersecurity'. [The School is] also developing an elective that will be offered in Fall 2013 for the first time for masters and Ph.D. students focusing on cybercrime and security research," explained Professor Tom Holt.[105] Finally, the School does not "have a colloquium series [in cyber issues] yet, but [hopes] to establish one in the next year." From the information provided, CJ students seem to have the opportunity to achieve at least a basic understanding of cyber-crime and network security, and the school's offerings will be augmented soon.

City University of New York - John Jay College of Criminal Justice New York, NY
(U.S. News Rank #10) NSA Cert: N/A
The John Jay College of Criminal Justice at the CUNY offers nine Masters' programs, including a M.S. in Digital Forensics and Cybersecurity, and two certificate programs in Computer Science for Digital Forensics and in Applied Digital Forensic Science. While the M.A. in Criminal Justice offers an elective in "Cybercriminology," the M.S. in Digital Forensics and Cybersecurity provides students with a balance of practice and theory in computer science, law, and criminal justice. Both core and elective courses include aspects of cyber criminology, network security, and security of information and technology. The instructional staff includes academic researchers who analyze the latest computer security threats as well as cyber investigators from law enforcement agencies and private security firms. This program aims at producing professionals qualified as cybersecurity analysts and investigators, information assurance specialists and consultants, and

so forth. Moreover, John Jay College, in collaboration with NYU-Polytechnic University, offers also a fellowship program for students pursuing the M.S. in Digital Forensics and Cybersecurity, which includes a full tuition waiver, stipend and research opportunities with faculty at John Jay and NYU-Poly. Moreover, students and faculty interested in cybersecurity can pursue their individual research projects and participate in the various events sponsored by the Center of Cybercrime Studies.[106] The Center focuses on developing and disseminating the knowledge and tools needed to understand, detect and deter computer related criminal activity. From the information available, John Jay College seem to offer one of the most comprehensive cyber-related curriculum of all the criminal justice programs analyzed, and provides students with incentives to pursue research opportunities and careers at the forefront of cybersecurity.

Other Programs of Note

In addition to the schools above, there are other schools carving out their own niche criminal justice degrees in cybersecurity in response to the needs of homeland security, law enforcement and criminal justice in the 21st century. **Salve Regina University**, for example, is pioneering a new cybersecurity and intelligence concentration for its M.S. in Administration of Justice and Homeland Security.[107] The program combines traditional criminal justice courses with specialty courses, such as information technology, high-tech crimes, cyber threat analysis, cyber threat management, cyber intelligence and cyber methodology. The program focuses on innovative leadership and the conceptual aspects of what steps need to be taken so that managers can lead and interact in a technological environment and bridge the gap between management and technicians. Other schools offering criminal justice degrees with a focus on cybersecurity include **South University**, which offers an online M.S. in Criminal Justice with a concentration in Cybercrime, and **Boston University**, which offers an online Master of Criminal Justice with a heavy focus on cybercrime, digital security and fraud detection. Students enrolled in the Master of Professional Studies in Security & Safety Leadership at **George Washington University** can also opt to specialize in cybersecurity.

Healthcare Management Graduate Programs

"I have never seen an industry with more gaping security holes. If our financial industry regarded security the way the healthcare sector does, I would stuff my cash in a mattress under my bed."[108]

U.S. News Ranking	College/University	School	City	State	Likert Scale Average Score	NSA Certification*
#1	University of Michigan	School of Public Health	Ann Arbor	MI	2	N/A
#2	University of Minnesota	School of Public Health	Minneapolis	MN	1.5	E
#3	University of North Carolina, Chapel Hill	Gillings School of Global Public Health	Chapel Hill	NC	0.5	N/A
#4	University of Pennsylvania	Wharton School of Business	Philadelphia	PA	1	N/A
#5	University of Alabama at Birmingham	School of Health Professionals	Birmingham	AL	2	R
#5	Virgina Commonwealth University	School of Allied Health Professionals	Richmond	VA	1.5	N/A
#7	Northwestern University	Kellogg School of Management	Evanston	IL	1	N/A
#8	University of Washington	School of Public Health	Seattle	WA	1	E, R
#9	Rush University	College of Health Sciences	Chicago	IL	2	N/A
#9	Saint Louis University	College for Public Health and Social Justice	Saint Louis	MO	1	N/A

** Indicates university NSA designation as a Center of Academic Excellence in Information Assurance Education (E) and/or Research (R).*

Safeguarding patient information in the digital age may be just as challenging as trying to control ballooning U.S. healthcare costs in general. Questions about the cybersecurity of medical systems have intensified as hospitals embrace wireless devices and electronic health records (EHR), mandated by the Congress in 2009.

As a new report from *The Washington Post* describes, while the U.S. healthcare industry might have some of the country's most sensitive personal information, failure to use rudimentary safeguards like disk encryption and password protection shows that it also has "the least regard, understanding and respect for IT security."[109] In the two years since the Department of Health and Human Services mandated public disclosure of any exposure of data involving 500 or more patients, breaches affecting more than 10 million individuals have been reported. Recent cases of information security breaches in the healthcare industry—from stolen laptops with unencrypted data, to hacked hospital servers and medical records linked to the Internet, to unaware employees handling sensitive information without the tools to protect it—have led to the exploitation of patient information to steal identities, finances, drugs, supplies and healthcare itself.[110] As Avi Rubin, computer scientist and technical director of the Information Security Institute at Johns Hopkins University, explains: "the routine failure to fix known software flaws in aging technology and a culture in which physicians, nurses and other healthcare workers sidestep basic security measures, such as passwords, in favor of convenience" are making those healthcare professionals "a pipeline for attackers into the sensitive networks." While hospitals might not provide the same attractive target for hackers as financial institutions, the array and rapid increase of personal information stolen from patients' records is forcing healthcare professionals to be equipped with, at minimum, a basic knowledge of health information systems and technology, a better understanding of how data is transmitted, stored and processed, and training on how to protect it.

Healthcare is the largest industry in the United States and the second largest employer, and healthcare management programs across the country encompass a wide variety of concentrations. Graduates can pursue an array of careers within the field, including executive-level administrators for healthcare delivery organizations, insurance company executives, public health workers, healthcare consultants, policy analysts, healthcare financial analysts, lobbyists, and policy advocates. Cybersecurity education can no longer be an option for any of these healthcare professions. However, only few of the healthcare management programs analyzed in this report have started to integrate courses that explore specific problems in IT security and privacy in healthcare organizations.

University of Michigan - School of Public Health Ann Arbor, MI
(U.S. News Rank #1) NSA Cert: N/A
The Department of Health Management and Policy at the University of Michigan offers a variety of master degrees related to healthcare and public health services, including a newly added program dedicated to health informatics. Although none of these programs comprises a course specifically dedicated to cybersecurity issues in healthcare management, Associate Professor K. Zheng explained that members of the faculty "cover cybersecurity related issues as components of various course offerings, including a required course on health IT for those who are not enrolled in the health informatics program."[111] Other courses that cover aspects of health information technology applications and management, database security, privacy, policy and security issues are: "Health Informatics," "Database Systems and Internet Applications in Health Care" and "Critical Policy Issues in Health IT." Finally, the Michigan Health Information Network (MiHIN) held its Healthcare Cybersecurity Workshop at the University of Michigan this past summer.[112] From the information provided, healthcare graduate students at the University of Michigan have the opportunity to receive at least a basics education in health information technology and familiarize with some of the most important IT security aspects.

University of Minnesota - School of Public Health Minneapolis, MN
(U.S. News Rank #2) NSA Cert: CAE/IAE
The Master of Healthcare Administration (MHA) curriculum at the University of Minnesota School of Public Health includes only a core course in "Information Technology in Healthcare," which provides an in depth analysis of the theory and conceptual base for healthcare information technology, the use of current and developing health IT applications, and current issues in healthcare IT—such as how the Internet is changing healthcare delivery and affecting privacy and security concerns.[113] Students interested in information technology and cyber-related issues can cross-register for a limited number of electives at the Carlson School of Management or at the College of Science and Engineering. Finally, last year the University of Minnesota Technological Leadership Institute (TLI) joined the DHS' national cybersecurity awareness campaign—Stop. Think.Connect.™—and hosted a weeklong series of events on cyber awareness, cyber careers, and digital critical infrastructure protection. Aside from these sporadic events, however, MHA students do not have other opportunities to explore cybersecurity related issues.

University of North Carolina - Gillings School of Global Public Health Chapel Hill, NC
(U.S. News Rank #3) NSA Cert: N/A
The Department of Health Policy and Management at the University of North Carolina (UNC) offers a Residential and an Executive master's program in Healthcare Administration (MHA). The set MHA curriculum includes only a couple of courses that touch upon information systems and technology in healthcare, but do not address specific security or information privacy issues related to the applications of information technology in healthcare.

University of Pennsylvania - Wharton School of Business Philadelphia, PA
(U.S. News Rank #4) NSA Cert: N/A
The Healthcare Management Department at the University of Pennsylvania Wharton School offers an MBA Program in Healthcare Management. The only elective course in this program that introduces students to the role that health information technologies (HIT) play in improving the performance of healthcare delivery, financing and innovation, is "E-Health: Business Models and Impact." Healthcare Management students interested in IT issues can also choose from a few other elective courses in information technologies and systems, innovation management, and information strategy offered through the Operation and Information Management Department at the Wharton School, as pointed out by MBA Advisor June Kinney.[114] None of these courses, however, touch upon specific cybersecurity concerns in the healthcare sector. From the information available, Healthcare Management students at the Wharton School have the opportunity to explore health information technology topics if they choose, but those offerings do not include cybersecurity components.

University of Alabama - School of Health Professions Birmingham, AL
(U.S. News Rank #5) NSA Cert: CAE/R
Graduate students at the University of Alabama School of Health Professions can enroll in an M.S. in Health Administration (MSHA) alone or in one of its coordinated degree options—M.S. in Health Administration/M.S. in Health Informatics or M.S. in Health Administration/MBA. "All MSHA students are required to take a course in Information Systems and Management Science, which addresses some security issues in healthcare," according to Assistant Director Sara Patterson.[115] However, only the M.S. in Health Informatics curriculum integrates the domains of information and communication technology with the leadership and management principles of healthcare delivery, and is specifically designed for graduates that aspire to senior and executive level positions in the healthcare IT industry. This program is the only one to include courses in "Health Information Systems," "Security and Privacy in Healthcare," and "Strategic Planning and Contracting for Health Information Systems." From the information provided, graduates of the M.S. in Health Informatics program are generally better equipped with the knowledge necessary to efficiently manage the flow of information throughout a healthcare organization, navigate cyberspace more safely, and make sound decisions when implementing and using technology in a healthcare setting.

Virginia Commonwealth University - School of Allied Health Professions Richmond, VA
(U.S. News Rank #5) NSA Cert: N/A
The VCU School of Allied Health Professions offers an 'industry specific' MBA program in Health Administration (MHA) and a professional distance-learning M.S. in Health Administration (MSHA). Both programs include a core course in "Information Systems for Healthcare Management," which provides a basic understanding of foundational principles and practical strategies in healthcare information systems, including technology standards and security issues, according to Director of the Graduate Programs in Health Administration Dr. Dolores Clement.[116] Moreover, "students interested in IT and cyber-issues can take one elective at other schools that offer courses" in this area. The Schools of Business and Engineering, for example, offer a joint Master degree in Computer and Information Security, which includes courses in "Ethical, Social and Legal Issues in Computer and Information Systems Security," "Computer and Information Systems Security," "Network and Operating Systems Security," and "Database and Application Security." Given the fact that MHA students can only pick one elective, though, it is doubtful that they will be able to gain a comprehensive understanding of cybersecurity issues in the healthcare industry.

Northwestern University - Kellogg School of Management Evanston, IL
(U.S. News Rank #7) NSA Cert: N/A
The Kellogg School of Management offers a Health Enterprise Management (HEMA) major among its MBA options. The only elective in this program that includes IT privacy and security topics is "Health Information Technology." In principle, HEMA students interested in IT and cyber-related issues can cross-register at other departments of Northwestern University, "but in practice none do," explained Professor David Dravone.[117] From the information provided, HEMA students have limited opportunities to be exposed to cybersecurity issues in the healthcare industry.

University of Washington - School of Public Health Seattle, WA
(U.S. News Rank #8) NSA Cert: CAE/IAE, CAE/R
The Master of Health Administration (MHA) at the University of Washington is focused on leadership development and innovation. However, the only core course in this program that exposes students to the understanding of informatics and its healthcare applications, while also discussing successes stories and failures in implementing information technology, is "Informatics in Healthcare Management." Aside from this class, graduates do not seem to gain any further exposure to cybersecurity issues in the healthcare industry.

Rush University - College of Health Sciences Chicago, IL
(U.S. News Rank #9) NSA Cert: N/A
Rush University's Health Systems Management Department offers an M.S. in Health Systems Management (HSM), which links practitioner-focused coursework with real-world management experience at the Rush University Medical Center. Students study a comprehensive health management curriculum, which comprises quantitative and analytical techniques, strategic planning, finance and human resources management as well as information systems and health information management. All courses in this program are required and they include: "Health Informatics" and "Health Care Information Systems," which address security and privacy risks of

electronic patient data, and management and protection of information assets. As Professor Diane Howard explained, "the HSM curriculum is core course heavy so there is no time for students to take additional IT coursework." Moreover, candidates for this program are encouraged to have a prior knowledge of economics and computer science to strengthen their application. From the information provided, Rush University HSM graduates seem to receive at least a basic education on healthcare information systems, as well as on IT security, privacy risks, and data protection.

Saint Louis University - College for Public Health and Social Justice St. Louis, MO
(U.S. News Rank #9) NSA Cert: N/A
St. Louis University (SLU) offers a Master of Health Administration (MHA) in a traditional-based format and in a hybrid format—Executive MHA—to fit the needs of working professionals. The traditional MHA degree requires the completion of a set core curriculum, which includes one course in "Health Information Systems" dedicated to healthcare information systems and technology. The program also offers "an elective that is offered occasionally on health information technology privacy and security," explained MHA Program Director Dr. Ana Maria Lomperis.[118] In addition, "the Department of Health Informatics and Information Management in the SLU College for Health Science offers a Master in Health Informatics," added Dr. Lomperis. From the information provided, however, it is not clear if MHA students gain any exposure to specific cybersecurity issues in the healthcare industry.

Conclusion and Future Directions

"It is not enough for the information technology workforce to understand the importance of cybersecurity; leaders at all levels of government and industry need to be able to make business and investment decisions based on knowledge of risks and potential impacts."[119]

As the MacAfee research team pointed out in their *2012 Threats Report*, "the areas of cybercrime, hacktivism, and cyber warfare are in a continual state of evolution and, in certain cases, revolution. Governments, enterprises, and consumers face a wide range of digital threats from these forces."[120] Institutions of all sizes and across all sectors are vulnerable to the cyber threat, and leaders from all disciplines must be prepared for an era of persistent cyber challenges regardless of whether they are computer engineers or not. Addressing current and future cybersecurity challenges requires a new cadre of cyber-strategic leaders.

Universities must be an incubator of these non-technical cyber leaders, bridging theory and doctrine with methodology, tools, and implementation, and optimizing their campus wide-resources to devise comprehensive curricula that include technical, policy, sociology, and legal components of the study of cyber threats. Cyber-strategic leadership is not to the same as, nor does it replace, the specific technical skills required to develop and administer the cyber environment. Rather it is the set of knowledge, skills, and attributes essential to future generations of leaders whose physical institutions nevertheless exist and operate in, through, and with the digital realm. These individuals need not have specific training in engineering or programming, but they must be equipped with a deep understanding of the cyber context in which they operate to harness the right tools, strategies, people, and training to respond to a dynamic and rapidly-developing array of threats.

This survey has highlighted the increased interest of some preeminent American universities and a few other niche programs across the country to develop new content for cybersecurity education across various disciplines and prepare graduates to lead in a fundamentally different cyber age. It has also illustrated, however, that there remains a strong imbalance between the evident need to educate future leaders about the complexities of cyberspace and the marginal role that cybersecurity education still plays in most graduate programs. Even the science or engineering departments that have received CAE/IAE and/or CAE/R designations do not necessarily collaborate to a visible degree with their university policy or law schools, for example, to expand the cybersecurity education opportunities for their graduates and utilize their joint knowledge. In fact, of the 70 programs at 44 universities analyzed, only 5 programs at 3 universities have both a CAE designation and academic programs with an overall Likert score of at least 3 out of 4.

Thus, the efforts underway in academic institutions across the country to institutionalize cybersecurity education must be expanded and incorporated into all major graduate and professional leadership development programs in the country, while also encouraging stronger intra-university collaboration. Additional steps should include integrating best practices, core curriculum tenets, and minimum standards to create a holistic plan to address the cybersecurity issues confronting every sector in American society. The integration of these core elements will require developing a comprehensive framework for the technical, operational, policy, and legal aspects that are critical to any effective cybersecurity program. Input and support from experts—academics, researchers, industry professionals, and government officials—who have championed the development of cybersecurity leadership and cybersecurity programs will be critical.

America's future security hinges on its ability to prepare leaders for the challenges of the digital age. Efforts to use cyberspace for malicious purposes have matured in scope and sophistication over the past two decades; this threat will only intensify as criminals continue to embrace its low cost of entry and states operationalize cyber instruments as offensive weapons and tools of national power. Meeting this challenge in both the public and private sector will require careful planning and consideration. Placing more emphasis on the development of traditional graduate programs and specialized cybersecurity programs that prepare individuals for the complexities of cyberspace is imperative, and the time is ripe for universities to help America's next leaders meet those challenges.

References

1. Internet World Stats, *World Internet Usage and Population Statistic* (30 June 2012), http://www.internetworldstats.com/stats.htm.

2. Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, (New York: The Penguin Press, 2011), 15.

3. Gen. Keith B. Alexander, "Cybersecurity and American power: Addressing new threats to America's economy and military," *American Enterprise Institute,* (9 July 2012), http://www.aei.org/events/2012/07/09/cybersecurity-and-ameri-

can-power/.

4. For more on the extensive research and consultations with individuals in government, the military, the private sector and non-profit organizations about cyber threats, see Kristin M. Lord and Travis Sharp, "America's Cyber Future: Security and Prosperity in the Information Age," vol. I, Center for a New American Security (June 2011).

5. Jan Kallberg and Bhavani Thuraisingham, "Cyber Operations: Bridging from Concept to Cyber Superiority," *Joint Forces Quarterly 68,* no.1 (January 2013), 53-58.

6. Chris C. Demchak, "Hacking the Next War," *The American Interest*, vol.8, no.1 (September/October 2012).

7. Chris C. Demchak, "Resilience, Disruption, and a "Cyber Westphalia": Options for National Security in a Cybered Conflict World," in Nicholas Burns and Jonathon Price, eds, *Securing Cyberspace: A New Domain for National Security*, (Washington, DC: The Aspen Institute, 2012), 59-94.

8. Greg MacSweeney, "10 Financial Services Cyber Security Trends for 2013," *Wall Street & Technology* (5 December 2012), http://www.wallstreetandtech.com/data-security/10-financial-services-cybersecurity-tre/240143809.

9. Author's interview with Melissa Hathaway, President of Hathaway Global Strategies LLC (9 November 2012).

10. Kallberg and Thuraisingham, "Cyber Operations."

11. Rhode Island Academic Collaboration on Cybersecurity Technology and Policy (13 September 2011), http://www.cs.brown.edu/people/jes/cyberpolicy.html.

12. The National Security Agency (NSA) sets up the criteria for the designation of universities or academic departments as Center of Academic Excellence in Information Assurance Education (CAE/IAE) and CAE IA Research (CAE/R). The designation is valid for five academic years. Students attending designated schools are eligible to apply for scholarships and grants through the Department of Defense (DoD) Information Assurance Scholarship Program (IASP) and the Federal Cyber Service Scholarship for Service Program. The list of CAE institutions can be found at http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml.

13. Information assurance is part of cyber defense—but it is not cyber defense. More specifically, IA practitioners seek to protect and defend information and information systems by ensuring availability, integrity, authentication, confidentiality, and non-repudiation.

14. The Likert scale is commonly used in survey research. This approach is usually used to measure respondents' attitudes by asking the extent to which they agree or disagree with a particular question or statement.

15. "2013 Best Graduate Schools Rankings," *U.S. News & World Report.* For more statistical information on more than 1,200 graduate programs nationwide, see: www.usnews.com/grad.

16. "The Best International Relations Master's Programs," *Foreign Policy* (Jan/Feb 2012), http://www.foreignpolicy.com/articles/2012/01/03/top_ten_international_relations_masters_programs.

17. Nicole Perlroth, "Nissan Is Latest Company to Get Hacked," *The New York Times* (24 April 2012).

18. Eric Shaw and Harley Stock, "Behavioral Risk of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall," Symantec Corp. (December 2011), http://www.symantec.com/about/news/release/article.jsp?prid=20111207_01; Ponemon Institute, "2012 Cost of Cybercrime Study" (October 2012), http://www.ponemon.org/library/2012-cost-of-cyber-crime-study.

19. Ponemon Institute, "Perceptions About Network Security: Survey of IT & IT Security Practitioners in the U.S." (June 2011), http://www.juniper.net/us/en/local/pdf/additional-resources/ponemon-perceptions-network-security.pdf.

20. Nicole Perlroth, "Study May Offer Insight Into Coca-Cola Breach," *The New York Times* (30 November 2012).

21. Moriah Sargent, "Cybercrime 2012: Malware attacks prominent in retail, financial industries," *Search Security* (13 December 2012), http://searchsecurity.techtarget.com/news/2240174500/Cybercrime-2012-Malware-attacks-prominent-in-retail-financial-industries.

22. Booz Allen Hamilton, "Top 10 Financial Services Cyber Risk Trends for 2013" (November 2012), http://www.boozallen.com/media-center/press-releases/48399320/cyber-top-ten-2013-press-release.

23. Ibid.

24. For more on the Stanford Cybersecurity Center, see: http://cybersecurity.stanford.edu/.

25. Author's interview with Cindy Armour, MBA program coordinator at the University of Pennsylvania Wharton

School of Business (31 January 2013).

[26] Author's interview with Catherine Cabrera, Program Manager at the University of Chicago Booth School of Business (22 November 2012).

[27] Author's interview with Kalpana Waikar, MBA Academic Advisor at Northwestern University Kellogg School of Management (30 January 2013).

[28] Author's interview with University of California Haas School of Business Admission Office (30 January 2013).

[29] For more information on technology management opportunities at the University of California Haas School of Business, see: http://mba.haas.berkeley.edu/academics/areas-of-emphasis.html.

[30] Author's interview with Eric Metelka, co-president of the student-run Technology Business Group at Columbia Business School, (14 February 2013).

[31] Author's interview with Phil Charbonneau, Program Coordinator at Darmouth College Tuck School of Business (14 February 2013).

[32] For more on the Center for Digital Strategies at Dartmouth, see: http://digitalstrategies.tuck.dartmouth.edu/.

[33] The Institute for Information Infrastructure was founded in 2002 at Dartmouth College, and brings together researchers, government officials, and industry representatives to address cybersecurity challenges affecting the nation's critical infrastructures. For more on I3P, see: http://www.thei3p.org/.

[34] Author's interview with Sara Gorecki, Administrative Assistant for the Information, Operations, and Management Systems Department at New York University Stern School of Business (30 January 2013).

[35] Author's interview with Professor Norman White, Deputy Chair at the NYU Department of Information Operations and Management Science (28 February 2013).

[36] The Polytechnic Institute of New York University (NYU-Poly) was one of the earliest schools to introduce a cyber security program. Designated as both a Center of Academic Excellence in Information Assurance Education and a Center of Academic Excellence in Research, the school operates a National Science Foundation-funded Information Systems and Internet Security (ISIS) laboratory to conducts cyber security research.

[37] Kelsey Sheehy, "Information Security M.B.A.'s Teach Business Side of Cybersecurity," *U.S. News & World Reports* (February 21, 2012), http://www.usnews.com/education/best-graduate-schools/top-business-schools/articles/2012/02/21/information-security-mbas-teach-business-side-of-cybersecurity.

[38] Anonymous Cairo activist, quoted in Nadine Kassem Chebib & Rabia Minatullah Sohail, "The Reasons Social Media Contributed to the 2011 Egyptian Revolution," *International Journal of Business Research and Management* 3 (2011).

[39] Nicholas D. Kristof, "Tear Down This Cyberwall!" *The New York Times* (17 June 2009) http://www.nytimes.com/2009/06/18/opinion/18kristof.html.

[40] Privacy Rights Clearinghouse, "Chronology of Data Breaches, Government and Military, 2005-2013," http://www.privacyrights.org/data-breach/new.

[41] Byron Acohido, "S.C. data breach just latest in hacker onslaught," *USA Today* (26 October 2012), http://www.usatoday.com/story/tech/2012/10/26/south-carolina-data-breach-36-million-ssns-stolen/1661541/.

[42] Richard A. Clarke and Robert K. Knake, *Cyber War: The Next Threat to National Security and What to Do About It*, (New York: Harper Collins Publishers, 2010), 242-243.

[43] Author's interview with MPA student Eric Noogle, Syracuse University Maxwell School (8 February 2013).

[44] For more on the Center for Applied Cybersecurity Research at Indiana University, see: http://cacr.iu.edu/.

[45] For more on the Belfer Center research program "Exploration in Cyber International Relations," see: http://belfercenter.hks.harvard.edu/project/67/explorations_in_cyber_international_relations.html?page_id=312.

[46] Author's interview with Melissa Hathaway, President of Hathaway Global Strategies LLC (9 November 2012).

[47] Author's interview with Andrew Whitford, MPA Program Director at the University of Georgia (2 February 2013).

[48] For more on the Center for Information Technology Policy at Princeton University, see: https://citp.princeton.edu/.

[49] ASPIRE is a National Science Foundation scholarship to train the next generation of cybersecurity experts within the family of NYU schools. Recipients are required to take a set of ASPIRE interdisciplinary gateway courses encom-

passing the technological (NYU-Poly), business (NYU-Stern), cultural (NYU-Steinhardt), public policy and management (NYU-Wagner) and scientific (NYU Courant Institute) aspects of real world security and privacy problems, and will then have to work for two years at a federal agency upon graduation.

50. For more on the Center for Interdisciplinary Studies in Security and Privacy (CRISSP), see: http://crissp.poly.edu/.

51. Author's interview with Melissa Jones, Admission Officer at the New York University Wagner School of Public Service (1 February 2013).

52. For more on the Center for Risk and Economic Analysis of Terrorism Events (CREATE), see: http://create.usc.edu/.

53. Author's interview with Sarah Esquivel, Assistant Director of Recruitment and Admission at the University of Southern California Sol Price School of Public Policy (1 February 2013).

54. Author's interview with Brenda Peyser, Associate Dean at the Carnegie Mellon University Heinz School of Public Policy and Management (1 February 2013).

55. For more on the Master of Science in Information Security Policy and Management (MSISPM) at Heinz College, see: http://www.heinz.cmu.edu/school-of-information-systems-and-management/information-security-policy-management-msispm/index.aspx.

56. Author's interview with Ray Hummert, Administrative Director of the University of Kansas School of Public Affairs and Administration (4 February 2013).

57. Author's interview with Ellen Weinstein, Director of Academic Services at the University of Washington Evans School of Public Affairs (5 February 2013).

58. For more on the Center for Information Assurance and Cybersecurity (CIAC), see: http://blogs.uw.edu/ciacsec/.

59. GlobalMPA.net, which was created by the U.S.-based National Association of Schools of Public Affairs and Administration (NASPAA) to promote MPA/MPP education internationally, surveys programs in the United States. For more, see: http://www.globalmpa.net/section/degrees_details/mpa_mpp_degrees.

60. Author's interview with Martha Chavez, Assistant Dean for Academic Affairs at the University of California Goldman School of Public Policy (25 February 2013).

61. For more on the Institute on Global Conflict and Cooperation's Cyber Security Graduate Training Program, see: http://igcc.ucsd.edu/research/technology-and-security/international-cooperation-on-cybersecurity/.

62. Author's interview with Deborah Isaacson, MPP Director at Harvard Kennedy School (14 February 2013).

63. Author's interview with Laura K. Lee, Director of Communication and Outreach at the University of Michigan Ford School of Public Policy (1 February 2013).

64. Author's interview with Maggie DeCarlo, Director of Admission at the University of Chicago Harris School of Public Policy Studies (4 February 2013).

65. Author's interview with Helene McAdams, Director of Student Services and Program Development at Duke University Sanford School of Public Policy (5 February 2013).

66. Author's interview with Professor Tom Taylor at Duke University Sanford School of Public Policy (5 February 2013).

67. Author's interview with Associate Professor David Schanzer at Duke University Sanford School of Public Policy (13 February 2013).

68. David E. Sanger, "Obama Order Sped Up Wave of Cyberattacks Against Iran," *The New York Times* (1 June 2012), http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html.

69. Ibid.

70. Michael J. Gross, "A Declaration of Cyber-War," *Vanity Fair* (April 2011).

71. Sun Bing et al., "MacAfee Threats Report: Third Quarter 2012," McAfee Labs (November 2012).

72. Author's interview with Jennifer Windsor, Associate Dean for Programs and Studies at Georgetown University Walsh School of Foreign Service (5 February 2013).

73. For more on the Georgetown Institute for Law, Science, and Global Security's Cyber Project, see: http://lsgs.georgetown.edu/programs/CyberProject/.

74. Author's interview with Associate Professor William C. Martel, The Fletcher School (22 February 2013).

75. For more on The Fletcher School SIMULEX 2008, see http://fletcher.tufts.edu/News-and-Media/2008/10/28/Simulex-2008.

76. Author's interview with Jessica Baen, Coordinator for the International Security Policy Concentration and International Conflict at the Columbia University School of International and Public Affairs (8 February 2013).

77. Author's interview with Saltzman Institute for War and Peace Studies' Senior Scholar Abraham Wagner (5 February 2013).

78. For more information on the courses offered by the Center for International Science and Technology Policy at the Elliott School of International Affairs, see: http://www.gwu.edu/~cistp/academics/courses.cfm.

79. For example, the College of Professional Studies and the GW Center for Excellence in Public Leadership offer a Master of Professional Studies in Security and Safety Leadership, with the option to specialize in Strategic Cybersecurity Enforcement. GW School of Business offers a World Executive MBA in Cybersecurity. The School of Engineering and Applied Science offers a new M.S. in Cybersecurity in Computer Science. The Graduate School of Education and Human Development and the Law School are both working on creating a specialization in cybersecurity for their respective degrees.

80. For more on the George Washington University Cybersecurity Initiative, see: http://research.gwu.edu/cybersecurity.

81. Author's interview with E.G. Enbar, Student Affairs Administrator at The Chicago University (5 February 2013).

82. Author's interview with Steven Stashwick, CIR alumnus at the University of Chicago (20 February 2013).

83. Siobhan Gorman and Julian E. Barnes, "Cyber Combat: Act of War," *The Wall Street Journal* (30 May 2011).

84. Paulo Shakarian, "The 2008 Russian Cyber Campaign Against Georgia," *Military Review* (November-December 2011), 63-69.

85. Robert E. Kahn et al., "America's Cyber Future: Security and Prosperity in the Information Age," Center for a New American Security, (June 2011), http://www.cnas.org/cyber.

86. Michael N. Schmitt, "Cyber Operations and the Jus in Bello: Key Issues," *Naval War College International Law Studies* (2 March, 2011), http://ssrn.com/abstract=1801176.

87. Author's interview with Professor Oona Hathaway, Director of the Yale Law School Center for Global Legal Challenges (19 November 2012).

88. For more information on the Stanford University LLM program in Law, Science & Technology (LSP), see: http://www.law.stanford.edu/degrees/advanced-degrees-for-international-students/llm-in-law-science-technology.

89. For more on the Center for Internet and Society at Stanford Law School, see: http://cyberlaw.stanford.edu/.

90. For more on the Harvard University Berkman Center for Internet & Society, see: http://cyber.law.harvard.edu/.

91. For more on the Berkman Center Cybersecurity Wiki project, see: http://cyber.law.harvard.edu/cybersecurity/Main_Page.

92. For more on Berkeley Center for Law and Technology (BCLT), see: http://www.law.berkeley.edu/5065.htm.

93. For more on the Penn Law Center for Technology, Innovation and Competition, see: https://www.law.upenn.edu/institutes/ctic/.

94. Author's interview with Professor Jessica Litman at the University of Michigan Law School (28 November 2013).

95. Author's interview with Mr. Alonzo LaGrone, former Law School Program Coordinator at the University of Michigan-Ann Harbor (19 November 2012).

96. "Cyber Division Focusing on Hackers and Intrusions," The Federal Bureau (FBI) (26 October 2012), see: http://www.fbi.gov/news/stories/2012/october/cyber-division-focusing-on-hackers-and-intrusions/cyber-division-focusing-on-hackers-and-intrusions.

97. "Cybercriminals Creating 57,000 Fake Websites every week," *Security Week* (9 September 2010), http://www.securityweek.com/cybercriminals-creating-57000-fake-web-sites-every-week.

98. Joseph S. Nye, Jr., "Cyber Power," Belfer Center for Science and International Affairs, Harvard Kennedy School (May 2010).

99. "Cyber Division Focusing on Hackers and Intrusions," FBI.

100. Author's interview with David Maimon, Assistant Professor of Criminology and Criminal Justice at the University of Maryland-College Park (28 November 2012).

101. Maryland Cybersecurity Center, "Researchers Explore How Cyber-Attackers Think Like Regular Crooks," *News Story* (29 November 2011), http://www.cyber.umd.edu/news/news_story.php?id=6141.

102. For more information on the postgraduate opportunities offered by the Maryland Cybersecurity Center, see: http://www.cyber.umd.edu/education/grad.

103. Author's interview with Jean Gary, Academic Director at the University of Cincinnati School of Criminal Justice (26 November 2013).

104. Author's interview with Professor Carter Hay, Director of the Graduate Program at Florida University College of Criminology and Criminal Justice (28 November 2013). For more information on Florida State University's M.S. in Computer Criminology, see: http://www.cs.fsu.edu/current/grad/cc_ms.php.

105. Author's interview with Professor Rom Holt at the Michigan State University School of Criminal Justice (14 February 2013).

106. For more on the John Jay College of Criminal Justice Center of Cybercrime Studies, see: http://johnjayresearch.org/ccs/.

107. For more on the Salve Regina University's M.S. in Administration of Justice and Homeland Security, see: http://www.salve.edu/academics/graduateStudies/programs/gad/masters.

108. Robert O'Harrow Jr., "Health-care sector vulnerable to hackers, researchers say," *The Washington Post* (25 December 2012), http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_print.html.

109. Ibid.

110. Eric Johnson, "Health-Care Industry: Heal Thyself," *Wall Street Journal* (26 September 2011).

111. Author's interview with Zheng Kai, Associate Professor of Health Informatics at the University of Michigan School of Public Health (29 November 2012).

112. For more on the Michigan Health Information Network (MiHIN) Workshop on Healthcare Cybersecurity, see: http://mphi-web.ungerboeck.com/Documents/MIHINEXv2.pdf.

113. Author's interview with Professor Steve Parente at the University of Minnesota Carlson School of Management (7 February 2013).

114. Author's interview with June Kinney, MBA Advisor at the University of Pennsylvania Wharton School of Business (7 February 2013).

115. Author's interview with Sara Patterson Assistant Director at the University of Alabama School of Health Professions (7 February 2013).

116. Author's interview with Dr. Dolores Clement**,** Director of the Graduate Programs in Health Administration at the Virginia Commonwealth University (7 February 2013).

117. Author's interview with Professor David Dravone at Northwestern University Kellogg School of Management (7 February 2013).

118. Author's interview with Professor Ana Maria Lomperis, Director of the St. Louis University Master of Health Administration Program (5 March 2013).

119. Executive Office of the President of the U.S., *Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure* (2009), http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

120. Sun Bing et al., "MacAfee Threats Report: Third Quarter 2012," McAfee Labs.

www.salve.edu/pellcenter

About the Pell Center

The Pell Center for International Relations and Public Policy at Salve Regina University is a multi-disciplinary research center focused at the intersection of politics, policies, and ideas. Dedicated to honoring Senator Pell's legacy, the Center promotes American engagement in the world, effective government at home, and civic participation by all Americans.

PELL CENTER
for INTERNATIONAL RELATIONS
and PUBLIC POLICY

SALVE REGINA UNIVERSITY