Proposal Participants

- Steven Block, Academic Dean, The Fletcher School
- Ming Chow, Senior Lecturer, Computer Science
- Kathleen Fisher, Professor, Computer Science
- Soha Hassoun, Professor, Computer Science (Chair)
- Michele Malvesti, Professor of the Practice, The Fletcher School
- Jeff Taliaferro, Associate Professor, Political Science

Executive Summary of Proposal

We request the creation of a Bridge Professorship to strengthen expertise at Tufts in Cyber Security and Policy and to provide leadership for the creation of a variety of degree programs in Cyber Security and Policy. Cyber Security and Policy is an emerging cross-disciplinary field that impacts many aspects of our increasingly technology-dependent society. Tufts can make global contributions to this nascent field by leveraging our existing strengths in Diplomacy, International Relations, Political Science, Computer Science, and Active Citizenship. The relatively modest additional investment of a Bridge Professorship can lead to substantial gains for the university in reputation, revenue, and societal impact by providing the impetus for new revenue-generating degree programs and by opening up collaboration and funding opportunities with the Commonwealth of Massachusetts, the federal government, and industry.

"America's economic prosperity, national security, and our individual liberties depend on our commitment to securing cyberspace and maintaining an open, interoperable, secure, and reliable Internet. Our critical infrastructure continues to be at risk from threats in cyberspace, and our economy is harmed by the theft of our intellectual property. Although the threats are serious and they constantly evolve, I believe that if we address them effectively, we can ensure that the Internet remains an engine for economic growth and a platform for the free exchange of ideas." --President Obama [1]

Proposal for a Joint Cyber Security and Policy Program at Tufts University

Overview

To become a recognized world-leader in Cyber Security and Policy, Tufts needs to make key investments now before other institutions claim the role. A Cyber Security and Policy Bridge Professorship linking the School of Engineering, the School of Arts & Sciences, and the Fletcher School is a critical first step towards leveraging Tufts' existing strengths in this critical area. Such a Bridge Professor would possess experience and expertise in both technology and policy aspects of Cyber Security and would be able to work across multiple Departments at the University. We also envision the Bridge Professor to work in tandem with the proposed Tufts Center for Data-Empowered Research as data science and machine learning are proving to be indispensable manipulating and analyzing network data. The initial goals of the Bridge Professorship are to attract students, faculty and staff to the study of Cyber Security and Policy, connect and engage with federal and state government, local industry, and special interest groups. The ultimate goals of the position are to attract funding, to spearhead the creation of a master's and/or certificate program in Cyber Security and Policy, and to explore the creation of a joint center of study. Currently, the Deans of the Tufts School of Engineering and the Fletcher School of Law and Diplomacy have each agreed to fund 1/3 of a Bridge Professorship. Consequently, we are seeking the remaining 1/3 of the position from Tufts. In conjunction with creating a Bridge Professorship in Cyber Security and Policy, we recommend that Tufts create a new certificate program in Cyber Security and Policy as a first step towards serving a larger student population in this area.

Why Cyber Security and Policy at Tufts?

The proposed Cyber Security and Policy initiative draws on and ties together resources from across Tufts, reflecting the spirit of the Bridge Professorship program. A Bridge Professorship in Cyber Security and Policy realizes goals outlined in the strategic plans of the participating schools. The Fletcher School's 2015 strategic plan "To the Know the World" identifies Cyber Security and Cyber Warfare as potential growth areas for faculty research and teaching. The strategic plan promises: "The School will enhance and streamline the curriculum while maintaining its traditional areas of excellence; offerings in cyber/digital and biology/health will focus on the international and governance dimensions of these issues; Fletcher should seek to leverage its relationships with partners including the Gordon Institute for entrepreneurship; and the School of Arts and Sciences for cyber/digital, and non-academic partners, including think tanks and foundations" [4]. Cyber Security has been a major part of past EPIIC Symposiums sponsored by the Tufts Institute for Global Leadership.

Cyber Security and Policy also realizes goals in the strategic plans of both the School of Engineering and the School of Arts & Sciences [20][21]. One of the overarching goals in the School of Engineering's plan is "interdisciplinary education and research in strategic areas." Cyber Security is an integral part of engineering for human health, sustainability, and human factors. Cyber Security is also a critical part of "educating engineers committed to the innovative and ethical application of science and technology in addressing the most pressing societal needs." Long term, an investment in a joint Cyber Security and

Policy program would lead to "an investment in graduate education that enhances the education of all students in Arts and Sciences."

Cyber Security and Policy as an Interdisciplinary Challenge

Society has become heavily reliant upon computers and networked computer systems. The ubiquitous use of technology has produced significant improvements to the quality of life, but it has also led to a society acutely vulnerable to cyber criminals and to cyber warfare. As a result, Cyber Security has become a critical national and foreign policy issue [1].

Addressing the threats posed to society by poor Cyber Security requires expertise spanning many fields, including Computer Science, Economics, International Relations, Law, Political Science, and Psychology because the challenges are not only technical but also political. For example, what doctrines and policies should be followed to reduce the risks to society from Cyber Warfare? The military doctrines developed during the Cold War for managing nuclear weapons do not apply because cyber weapons are fundamentally different from nuclear weapons. For example, with nuclear weapons, the origins of any attack are obvious to everyone. In contrast, identifying the perpetrators of a cyber attack is technically difficult and often relies on non-technical information. Defending against and/or attributing a cyber are complicated tasks that can take a long time. For example, it took weeks for the U.S. to publicly blame North Korea for the Sony attack. It took months for the U.S. to formally charge Chinese Military Hackers with cyber espionage [16][17]. Even after a cyber attack, there are many questions that do not have simple answers: Whose job is it to defend against cyber attacks? How should the National Security Agency/US Cyber Command, the Department of Homeland Security (DHS) and other agencies in the US Intelligence Community partner with state and local law enforcement to combat cyber-espionage and cyber crime? How can defensive measures be implemented given that much of the critical infrastructure for the Internet is divided between the private and the public sector? Answering these questions requires knowledge in a number of areas including strategic studies, international law, and computer networking.

Electronic voting is another example. Countries including Estonia, France, and Switzerland-Geneva currently uses electronic voting for elections. The idea of electronic voting is appealing as it supports greater suffrage. However, there are significant challenges related to electronic voting including trust in Internet voting, secrecy and freedom in voting, and accessibility. Given how easily hackers can break into almost any computer system today and given the importance of elections to world power, how can we ensure the integrity of the results [22]? Cryptography, national, and international law are critical to this topic.

Both of these examples require expertise in both technology and policy to solve, highlighting the cross-disciplinary nature of Cyber Security.

Cyber Security and Policy Opportunities on a National Level

Because of the importance of this field, many funding agencies are making substantial sums available for research in Cyber Security and Policy. In October 2015, the National Science Foundation invested $74.5 million to support interdisciplinary cybersecurity research; investment included 257 new projects involving researchers in 37 states [11]. In November 2015, the Hewlett Foundation awarded the Woodrow Wilson International Center for Scholars $400,000 for support of the new Congressional Cybersecurity Lab "that builds congressional capacity on cybersecurity in a nonpartisan manner. The lab aims to close the knowledge gap with a dedicated educational program for Capitol Hill, introducing cyber fundamentals to a non-expert policymaking audience" [12]. Since 2006, Master's Degree enrollment in "new specialized programs in the core professional fields" including in cyber security have grown significantly with multidisciplinary Master's degrees growing 113.1% from 2002-2012 [13][19].

The demand for expertise in cyber security is substantial and growing rapidly. In September 2010, the Pittsburgh Tribune-Review ran a story on "Universities Push To Graduate Cybersecurity Experts As Demand Grows." Nearly six years later, Forbes ran a story "One Million Cybersecurity Job Openings In 2016."

Today, many policy makers have only a poor understanding of technology, which leads to poor decisions at the national level. An example are recent discussions in Congress to "review encryption --specifically how technology helps terrorists avoid surveillance" [3]. As a University with expertise in this area, we have an obligation to produce more informed policy makers.

Cyber Security and Policy Opportunities with the Commonwealth of Massachusetts

The Massachusetts Secretary of Housing and Economic Development has identified expansion of the State's Cyber Security industry as a high priority. The state already has a rich variety of institutions and companies vested in Cyber Security including Veracode, Cigital, Bit9, MITRE, Rapid7, Akamai, Draper Lab, Confer, Sqrrl, MIT Lincoln Laboratory, Mass General, and Dana Farber [5]. Tufts already has a relationship with many of the institutions and companies as evident by past guest lectures, career fair presence, and industry collaborations. Boston is also home to a plethora of security events and conferences including SecureWorld Boston, SOURCE Boston, BSides Boston, and the IEEE International Symposium on Technologies for Homeland Security coming in May 2016. A number of security-related think tanks and groups meet often including OWASP and I Am The Cavalry.

Our peer institutions have done very well in the past five years securing funding and new opportunities. Northeastern University, a National Center of Academic Excellence, received a $4.5M award to train future cybersecurity workforce in 2012 [6]. WPI was awarded $4.4 Million to Help Bolster the Nation's Cybersecurity Workforce in January 2015 [7]. Boston College recently inaugurated the MS in Cybersecurity Policy and Governance [8]. As recently as January 2016, a $15M gift was given to the Belfer Center of the Kennedy School of Government at Harvard to Launch Cyber Security Project [9]. UMass Amherst also received a $4.2 Million to train next national cybersecurity workforce [10].

At the Massachusetts Innovation Partnerships Network (IPN) meeting on December 9, 2015, there was an emphasis on building innovation centers and building talent strategy into research partnerships. The points made: both companies and universities place a strong focus on using partnerships to develop

talent, universities want students to learn from real world data, companies benefit from an up-close look at potential new employees. These points are especially true in cross-functional areas like Cyber Security where the competition is fierce. We anticipate being able to leverage such partnerships to build a strong Cyber Security and Policy program at Tufts.

Existing Resources

While there is tremendous interest in Cyber Security and Policy at Tufts, we currently lack the critical mass of human capital necessary to be viewed as leaders in this area. Currently, Ming Chow of the Department of Computer Science is actively engaged with the security community and offers the course "Introduction to Computer Security" in the fall semester. The late William Martel at the Fletcher School offered a seminar on Cyber Policy. He was also principal investigator in a joint Fletcher School-MIT Lincoln Laboratory studies on formulating codes of conduct for space and cyber. Michele Malvesti was recently hired as Professor of the Practice in The Fletcher School's International Security Studies Program. She is teaching the course "Foundations of International Cyber Security" this semester. Since the spring 2014 semester, Jeff Taliaferro of the Political Science Department has offered a course on "Intelligence and U.S. National Security." A Cyber Security and Cyber Warfare course has been proposed by Ming Chow and Jeff Taliaferro, submitted to the Tufts Innovates grant program. The Fletcher School's Institute for Business in the Global Context is currently doing research measuring cyber vulnerabilities and working with companies on cyber economic risk.

Risks

There is a risk that the proposed Bridge Professorship in Cyber Security and Policy does not bring the anticipated return on investment. Tufts can minimize the risk by hiring a superstar who has a proven track record of accomplishments and who has strong connections in academia, industry, and government. Tufts could further mitigate the financial risk by recruiting a foundation or corporation to endow the position. Given the nature of the position and the quality of the people who might fill it, we believe finding such outside support is feasible.

Certificate Program in Cyber Security and Policy

The timing to create a new certificate program in Cyber Security and Policy is excellent as evidenced by:

1. The University-wide email on January 26, 2016: "The Graduate School of Arts and Sciences is pursuing the creation of a number of new academic programs across a variety of areas as part of its strategic plan. These consist of new certificates programs and new master's programs"
2. The growing demand for professionals in Cyber Security as evident by the opportunities on the national level [2], and
3. Local institutions receiving federal funding to train next national cybersecurity workforce [6][7][10].

A new certificate program in Cyber Security and Policy will have a number of immediate benefits, namely:

1. Providing visibility for Tufts as an institution focusing on Cyber Security and Policy
2. Generating revenue
3. Attracting future funding and hiring opportunities
4. Serving as a springboard for the creation of a new Master's program in Cyber Security and Policy that will span multiple departments and schools.

We can craft a certificate program in Cyber Security and Policy with courses currently being offered at Tufts (see Appendix A). A graduate certificate program can be counted towards Master's credit, creating a transition path for part-time students to gain a Master's.

While a certificate program in Cyber Security and Policy could be created immediately, it would be unwise to do so without the additional resources reflected in the hiring of a Bridge Professor because of the severe resource constraints in Computer Science and the existing modest levels of expertise in Cyber Security and Policy currently available at Tufts. A Bridge Professor will bring expertise and depth to this program. The interest in such a program is evident: in the past three offerings of COMP 116: Introduction to Computer Security, there have been at least two working students who have afterwards pursued a graduate degree or certificate program in the topic.

Return on Investment (ROI)

The return on investment on investing in Cyber Security and Policy is potentially stellar. The immediate return on investment by having a Bridge Professorship would be to demonstrate that Tufts is committed to working on Cyber Security and Policy. If the Bridge Professorship encourages student involvement and active citizenship in Cyber Security and Policy, develops intellectual bridges between students and faculty, and brings in new opportunities to the University, it would already be an excellent investment. The stellar return on investment would be the creation of a new Master's program in Cyber Security and Policy that spans multiple Departments or a creation of a new joint center on International Cyber Security and Policy. This return on investment will be beneficial to society, and would bring global recognition and leadership in the field.

In Summary

It is in Tufts' DNA to make a significant impact on and lead in global affairs. Cyber Security and Policy has become an issue of critical importance to national security and the problems are getting worse. Solving these problems requires deep contributions from both technical and policy experts, and requires training many more individuals fluent in both. Because of its growing importance, the timing of this opportunity could not be better as evident by the growing interest in Cyber Security and Policy among students and different departments at Tufts, the strong presence of Cyber Security and Policy here in Massachusetts, and the vast amount of jobs and funding opportunities. At the very least, an investment in a Bridge Professorship will be a win for the University: it will add a needed resource across a number of different departments, it will add visibility for Tufts, it will add expertise, and it will start fulfilling the action items in Fletcher's and in the University's strategic plans. Tufts will be better even with a small investment. The sky is the limit on how far that investment can take Tufts.

Roadmap

Milestone	Timeline	Rewards	Risks and Effort Required
Bridge Professorship in Cyber Security and Policy	Immediately	Attracts new students, faculty, and staff at Tufts to the study of Cyber Security; connect and engage with federal and state government, local industries, and special interest groups; attract funding and opportunities related to Cyber Security to Tufts; immediately strengthen the certificate program in Cyber Security and Policy; leading a new graduate program in Cyber Security	Position does not pan out; will take time to recruit and sign on; requires an investment from Tufts or from a donation (e.g., endowed professorship)
Certificate Program in Cyber Security and Policy	Immediately	Provides visibility for Tufts as an institution focusing on Cyber Security; generates revenue; attracts future funding and hiring opportunities; serves as a springboard to a creation of a new Master's program in Cyber Security and Policy that spans multiple Departments; an inaugural class of 10 - 15 students would be deemed a success.	Program implemented under current conditions will be very weak given severe resource constraints in Computer Science and limited expertise in Cyber Security and Policy; inaugural class could be smaller than 10 students given competition in the Boston area; advertisement of new program required (e.g., MBTA ads)
MS in Cyber Security and Policy	2 - 3 years	Gives greater visibility and credibility to Tufts on Cyber Security and Policy	One bridge professor may not be enough to provide a strong MS program in Cyber Security --may need to hire new faculty members and adjuncts
Joint Center on International Cyber Security and Policy	3 - 5 years	Demonstrates global leadership on Cyber Security and Policy	New facility, staff, funding, and infrastructure (e.g., computing) required

Appendix A: Proposed Graduate Certificate Program in Cyber Security and Policy

The five required courses:

1. COMP 116: Introduction to Computer Security
2. DHP P249: Foundations of International Cyber Security
3. COMP 150: Cryptography
4. PS 187: Intelligence and National Security
5. PS / CS (Spring 2017, proposed Tufts Innovates Grant): Cyber Security and Cyber Warfare

The certificate program shall require two electives:

- DHP P242: Proliferation-Counterproliferation and Homeland Security Issues
- DHP P245: Crisis Management and Complex Emergencies
- DHP P247: Civil-Military Relations
- EM 54: Engineering Leadership
- COMP 111: Operating Systems
- COMP 112: Networks

Appendix B: People in Cyber Security and Policy

- Steve Bellovin, Professor of Computer Science at Columbia University, co-director of Columbia's Cybersecurity and Privacy Center, recently appointed technology scholar for the Privacy and Civil Liberties Oversight Board (PCLOB)
- Ed Felten, Professor of Computer Science and Public Affairs at the Princeton University, now Deputy U.S. Chief Technology Officer
- Jennifer Granick, Director of Civil Liberties for the Center for Internet and Society at Stanford Law School
- Susan Landau, Professor of Social Science and Policy Studies at Worcester Polytechnic Institute
- Herb Lin, Senior Research Scholar for Cyber Policy and Security at the Hoover Institute at Stanford University
- Andrea Matwyshyn, Professor of Law and Computer Science at Northeastern University

Acknowledgements

Many thanks to the following people for their help and guidance in writing this proposal:

- Karen Panetta, Professor and Associate Dean for Graduate Education at Tufts University
- Kevin Powers, Program Director of the Boston College MS in Cybersecurity Policy and Governance
- Diane Souvaine, Vice Provost for Research, Tufts University

In Memoriam

In memory of the late William Martel, Associate Professor of International Security Studies at The Fletcher School. His work in Cyber Security and Policy and his spirit made this venture possible.

References

[1] https://www.whitehouse.gov/issues/foreign-policy/cybersecurity

[2] http://www.forbes.com/sites/stevemorgan/2016/01/02/one-million-cybersecurity-job-openings-in-2016/#4cfd851f7d27

[3] http://money.cnn.com/2015/12/08/technology/encryption-congress-commission/index.html

[4] https://sites.tufts.edu/fletcherstrategicplan/files/2015/02/StrategicPlan_design_FINAL1.pdf

[5] http://www.bizjournals.com/boston/blog/techflash/2015/05/here-are-the-35-companies-that-have-put.html

[6] https://www.northeastern.edu/news/2012/08/northeastern-receives-4-5m-award-to-train-future-cybersecurity-workforce/

[7] https://www.wpi.edu/news/20145/fislercyber.html

[8] https://www.bc.edu/schools/advstudies/graduate/MScybersecurity.html

[9] http://belfercenter.ksg.harvard.edu/publication/26185/extraordinary_gift_to_harvard_kennedy_schools_belfer_center_to_launch_cyber_security_project.html

[10] https://www.umass.edu/newsoffice/article/umass-amherst-receives-42-million-train

[11] https://www.nsf.gov/news/news_summ.jsp?cntn_id=136481

[12] http://hewlett.org/grants/24226/woodrow-wilson-international-center-scholars

[13] https://www.eab.com/research-and-insights/academic-affairs-forum/expert-insights/2015/two-types-of-masters-programs-growing-fastest

[14] https://www.schneier.com/blog/archives/2015/03/attack_attribut_1.html

[15] https://www.justsecurity.org/24950/cyber-conflict-dods-law-war-manual/

[16] https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html

[17] https://www.fbi.gov/news/news_blog/five-chinese-military-hackers-charged-with-cyber-espionage-against-u.s

[18] http://www.parliament.uk/documents/speaker/digital-democracy/IFESIVreport.pdf

[19] http://www.vox.com/2014/5/20/5734816/masters-degrees-are-as-common-now-as-bachelors-degrees-were-in-the-60s

[20] http://engineering.tufts.edu/docs/soe_strategicPlanningFramework.pdf

[21] http://as.tufts.edu/documents/strategicPlan.pdf

[22] https://jhalderm.com/pub/papers/ivoting-ccs14.pdf