Interdisciplinary Cyber Security Education

Randal Milch and Nasir Memon

New York University

NIST's National Initiative for Cybersecurity Education (NICE) is a crucial step toward remedying the Nation's undeniable shortage of "people with the knowledge, skills, and abilities to perform the tasks required for cybersecurity work." Such a workforce will include "technical and nontechnical roles that are staffed with knowledgeable and experienced people."

The NICE Cybersecurity Workforce Framework goes on to identify 7 workforce categories, which encompass 33 specialty areas and over 50 work roles. A review of the specialty areas and work roles shows that – in many crucial areas – an "integrated cybersecurity workforce" is not split between "technical and non-technical roles." Within the seemingly non-technical "Oversee and Govern" workforce category for instance, every work role in the Legal Advice and Advocacy, Strategic Planning and Policy and Executive Cyber Leadership Specialty Areas requires technical knowledge of "computer networking concepts and protocols, and network security methodologies." (K001). Similarly, every work role in the apparently technical "Securely Provision" workforce category, requires quintessentially non-technical knowledge of "laws, regulations, policies, and ethics as they relate to cybersecurity and privacy." (K003).

The question, then, is how to produce a workforce with these inter-disciplinary skills. Recent and laudable strides made to create more cybersecurity engineers at do not require a law and policy course for masters candidates on the technical track.[1] Similarly, Professor Chesney's recently published and excellent syllabus for his "Cybersecurity Foundations: Law, Policy, and Institutions" course has no technical component for law and policy students without technical training.[2]

We propose that a critical component to an interdisciplinary need is actual

interdisciplinary instruction. For two years, the authors have taught a seminar in which JD and LLM students at NYU Law School and MS and PhD students at NYU Tandon School are instructed together. The class's premise is that technology and policy are interdependent in cyberspace.

We posit that the key to intelligent application of the disparate regulatory and policy schemes with which we confront cyberinsecurity – and the basis for intelligent development of law and policy – is a thorough understanding of the technology that underlies the current and future security of the Internet. At the same time, the engineers who build products and solve problems can increase the range of policy choices if they appreciate the range of policy needs and legal/compliance requirements, including those that are inefficient or counter-intuitive from an engineering point of view.

Our seminar aims to bring the relevant technology and the current legal landscape together, for a richer understanding of each. The seminar seeks to impart the following key cybersecurity engineering concepts:

- Understand threat, vulnerability and risk;
- Basic concepts of security - confidentiality, integrity and availability, and the means for achieving these properties in a system;
- Basic concepts related to how the Internet works - packet switching, routing, DNS, etc.;
- Understand how anonymity can be provided while communicating on the Internet and why attribution of attacks is difficult;
- Problems related to identity and authentication.

And the following key cybersecurity law and policy concepts are taught:

- How rules are made with respect to cybersecurity and who makes the rules – legislators, regulators and private groups;
- The roles and responsibilities of the government and private parties in

protecting networks;

- What companies are obligated to do with respect to cybersecurity;
- Issues surrounding voluntary information-sharing (public/private and private/private);
- How regulation and private civil litigation are defining "reasonable" cybersecurity measures;
- Obligations to provide information to and cooperate with government (intelligence, law enforcement, data vs. metadata):
- Data privacy regulation (EU vs. US) and its impact on cybersecurity (e.g. insider threat monitoring).

Students are placed in interdisciplinary groups to tackle problems from both technical and legal/policy angles. Responses to the course have been favorable, and it is clear that both the engineering and the law students take away a new and valuable literacy with one another's chosen fields. It is also apparent that the difficulties in cross-training are not equal. It is easier to provide engineering students with instruction in law and policy than it is to provide law students will little or no technical background with meaningful technical instruction.[3]

Efforts at the graduate level, however, ignore the large cybersecurity workforce already in place. Steps must be taken to provide existing cybersecurity professionals without interdisciplinary training with a route to obtain the knowledge they need to excel in their role. Based on the success of the graduate-level seminar, NYU is seeking to meet this need through a new Executive MS in Cybersecurity Risk and Strategy offered jointly by NYU School of Law and NYU Tandon School of Engineering.[4] The one-year program is intended for experienced professionals from a range of backgrounds who seek to deepen their understanding of cybersecurity risk and strategy. This program will create managers with the integrated expertise needed to play a leadership role in the field.

The MS in Cybersecurity Risk and Strategy program is a 30-credit executive MS management degree incorporating both online courses and blended-learning modules. Over a 12-month period, participants attend three residential sessions consisting of five days per session. Between residential periods, students are expected to study 10-15 hours per week in online and blended-learning formats. Semesters are divided into three phases: online introduction, in-class residency, and online implementation.

In order to ensure a common foundation for students from widely disparate backgrounds, MS-CRS students must, before starting their credit-bearing courses, pass on-line "bridge" courses in U.S. Law and in the technical Foundations of Cybersecurity. Each semester includes a 3 credit, core engineering course (Information Security and Privacy, Network Security, and Information Systems Security Engineering and Management) and two law or policy courses (such as Information Privacy Law, Cybersecurity Governance and Regulation, Cyber Crime and Innovation Policy) bearing a total of 5 credits. Spanning all three semesters is a 6 credit, team-based "Integrative Cybersecurity Management" Capstone Project.

Author Bios

Randal Milch is the Co-Chair of the NYU Center for Cybersecurity, a Distinguished Fellow at the Center on Law and Security, and a Professor of Practice at NYU School of Law

Nasir Memon Nasir Memon is a professor in the Department of Computer Science and Engineering at NYU Tandon. His research interests include digital forensics, biometrics, data compression, network security and security and human behavior.

[1] On-line students in the Georgia Tech program who chose a "Policy specialization" would be hard-pressed to avoid at least one law or policy course.

[2] Importantly, Professor Chesney hopes to attract "grad students . . . in business, engineering, and computer science" to his course.

[3] Law students *with* a technical background, however, are perhaps the most adept at mastering the combined material.

[4] The authors serve as Faculty Co-Directors of this new Program.