# Resources to Meet Cybersecurity Education Demands

**By**

**Balakrishnan Dasarathy, PhD**
**Professor and Program Chair, University of Maryland University College, Adelphi, MD**
**Email: Balakrishnan.Dasarathy@UMUC.edu**

The mission of the University of Maryland University College (UMUC) is to improve the lives of adult learners by operating as Maryland's open university, serving working adults, military service-members, their families, and veterans across the United States, and around the world. UMUC serves over 80,000 students worldwide and is one of the largest distance-learning institutions in the world. We have eight different cybersecurity and related degree programs at the undergraduate and graduate levels with specializations in software security, network security, cybersecurity technology, policy and management, digital forensics and information assurance, and about 11,000 students are currently enrolled in these programs. To increase access to quality higher education in cybersecurity at affordable cost (at UMUC and elsewhere), it is imperative that we develop several resources nationally. Nationally-developed resources not only amortize the cost over several institutions, they also prescribe and enforce certain minimum standards. The resources we need fall into the following categories (The need for many of these resources exists in other disciplines as well, but the need is more acute in our field.):

- (Hands-on) Laboratory exercises
- Environments for laboratory exercises
- Content
- Assessment materials

**Laboratory Exercises**: This is one area, as a field, we have made a good bit of progress. I am particularly aware of three programs funded by NSF, all of high quality. SEED at the University of Syracuse is a comprehensive one with laboratory exercises in network, web, software, system and mobile security, and cryptography. The Cyber4All exercises at Towson University focus on secure coding. The third one, a recent one, from the Florida Center for Cybersecurity includes exercises on incident response, penetration testing and malware analysis. All these three projects do have content support, but the content is tied to their laboratory exercises. UMUC will be using several of these laboratory exercises in a new program on Cyber Operations. To meet our cyber

workforce needs, it is imperative that NSF and other agencies continue to support this type of laboratory development work and transitioning the output to institutions nationwide.

**Environments for Laboratory Exercises**: Many universities need a laboratory environment with 24x7 support. Currently, in spite of advances in cloud computing and virtualization technologies, having a reliable computing environment for student teaching, and sandbox for research and experimentation cannot be taken for granted. Emulab and environments based on Emulab such as the DeterLab are better at supporting experimental research than instructional exercises by a large number of students. Several states (see, for example, Virginia Cyber Range, Baltimore Cyber Range) now offer cyber ranges for their citizens to practice their cybersecurity skills, but they are in preliminary stages of development. Students, in general, require a lot of hand-holding and assistance with trouble-shooting. Students in digital forensics also require access to a local, physical laboratory, as certain segments of computer science, telecommunication & networking students experimenting new concepts in operating systems, virtualization and cloud computing.

**Content**: I believe this is next frontier in higher education. As we know, textbooks are expensive and often students need to buy more than one textbook for a course. Fields like ours are also changing rapidly, and as such, textbooks become outdated within a few years after their release. An online version of a textbook is generally cheaper and supports revisions more easily than the corresponding hardcopy of the textbook. However, online textbooks, controlled by DRM software, have many restrictions such as short time of usage (often till the end of a specific semester), limited amount of printing, and restrictions on the number of devices; moreover, they are hosted on proprietary platforms. UMUC has had successful experience going "bookless" since 2015/2016, as noted in the one of the 2018 College Jeopardy Championship tournament episodes! With the assistance of subject matter experts, I have experience in developing content for seven courses in information assurance/cybersecurity over a two year period in areas that include network security, intrusion detection, digital forensics, cryptography, cyberlaw and privacy, and software assurance. My fear is that no single institution will able to keep up with content development and updating all on its own. Apart from the government supplied resources, specifically from NIST, there are very few "open resources." For a resource to be truly open, it should meet these 5 R's: (1) retain (make and own a copy of the resource), (2) reuse (use the

resource in many places), (3) revise (adapt/modify), (4) remix (combine the resource with other resources), and (5) redistribute (share the resource). With truly open educational resources that are self-contained, an instructor can easily tailor the content for a session or an entire course. Our community and sponsors should be encouraging high quality content development for degree programs at various levels. The National CyberWatch Center' Digital Press and EBooks, funded by NSF, is a good start here. The center also develops laboratory exercises and curricula, but the focus of the center currently is on community colleges and associate degree programs. MOOCs are a good development here as well, but, by and large, the content from MOOC courses have Intellectual Property restrictions. Moreover, content from a MOOC course might be tied to a specific platform and may not be easily portable and tailorable.

There are two competing requirements faced by higher education in content development today. One is the use of multimedia for enhanced learning experience. The other is in meeting the requirements of the Rehabilitation Act (1973) and Americans with Disabilities Act (1990, amended 2008). The key concept behind these acts is equal opportunity. A resolution agreement with the US Department of Education establishes that students with disabilities must be: "able to obtain the information as fully, equally, and independently as a person without a disability." At the minimum, in the short run, UMUC is committed to providing meaningful text alternatives for any non-text content. Technologies are available today (see, for instance, Office 365: Accessible by design) to create content that can be accessed without barriers as well for creating content by those who are challenged in some ways. Expanding access is not only the right thing but also the smart thing to do in meeting our cyber workforce needs!

**Assessment Materials**: To produce cybersecurity knowledge workers rapidly, our cybersecurity programs need to be more "open." We should not be demanding credentials (e.g., B.S. in Computer Science with 3.0 GPA); we should only be requiring that specific competencies be met. We need tailorable tests/assessments for verifying competencies. A good model to follow here is that of CYBRScore. The CYBRScore Skills Assessment is mapped to the NIST-NICE framework and employs hands-on scenarios to test competencies for a specific work role. For example, their Cyber Defense Analyst assessment consists of assessments for competencies in protocol analysis, intrusion detection, incident handling, and vulnerability analysis. This CYBRScore assessment technology is, however, proprietary. We need open solutions!