Cybersecurity automation and security

Susan G. Campbell and Petra Bradley, University of Maryland

The roles of future cyber professionals

The future of cybersecurity will be automated. Like less skilled personnel in other industries, less skilled cyber personnel are already being replaced by automated systems. Deep learning systems and other forms of artificial intelligence are being used for intrusion detection and network monitoring tasks. Straightforward tasks in other domains, such as secure programming, can be implemented using complicated but deterministic rules. Unlike humans, automated systems do not suffer negative effects from extended vigilance and do not accidentally omit procedural steps to create security holes. The current shortage of qualified cyber personnel should increase motivation to develop automated systems to fill holes in organizations' security postures that would otherwise have been filled by people.

Personnel who understand cybersecurity will still be required, because human decision-makers are needed to specify and build these systems, operate them, audit their operation, check them for security flaws, and provide them with training data. Cyber jobs of the future will encompass these areas rather than more routine actions, and people who are engaged in cyber work must also anticipate human and organizational behavior to mitigate human-generated security concerns. The roles of personnel in cyber will not necessarily change from the roles listed in the National Initiative for Cybersecurity Education (NICE) Cyber Security Workforce framework, but the way people do those jobs will change.

Future cyber education topics to support those roles

Security personnel will be required regardless of the level of automation that is achieved, but those personnel might focus their efforts on supervising automated processes and making decisions, rather than performing routine monitoring or defense.

Understanding human and organizational behavior

Future cyber personnel will need to understand which problems can be solved using technological means and which problems are due to the fact that organizations are made up of humans whose main priority is not generally security. Curricula need to increase cybersecurity

students' understanding of humans and sociotechnical systems (made up of people and technology), not just the technology.

Designing and evaluating automation

Other fields, as well as cyber, are building automated systems to accomplish tasks that do not need to be performed by humans to be successful. For example, goods that were once assembled by humans are now often assembled by machines, with human supervisors who ensure that the machines are working properly and who are equipped to trouble-shoot the systems when necessary. Cyber systems should gather best practices from other fields. Students who are planning to build systems should learn information security and networking concepts along with the appropriate kinds of automation (rule-based, machine learning based, or hybrid).

In addition to being able to build automated systems, organizations need personnel who are capable of evaluating whether automated systems are working properly and who can troubleshoot problems when necessary (or, at minimum, identify problems correctly so they can request the right kind of assistance). Generally, this requires understanding the systems and how they are meant to interact when they are working properly.

Operating systems and providing training data

Automated systems can reduce the number of personnel in certain roles within cyber, but any organization should have some way of evaluating whether their systems are working appropriately. This can be ascertained by inspection and monitoring of processes, or by challenging the system (e.g., conducting a "red team" exercise). In machine learning based systems, training data that are appropriately labeled and tagged can greatly accelerate the process of building and evaluating effective systems.

Operators may not need the skills to design automation, but they should be able to execute human-machine teaming tasks and identify malfunctions. Students who are planning to operate systems should have an understanding of the underlying mechanisms, but do not necessarily need to be able to build systems.

Securing the security software

The people who are most skilled at building automated systems may not be those who best understand security. Therefore, cybersecurity curricula should include a track for “pure” security, which would include evaluating automated systems as well as advancing the science of security.

Future-proofing cyber education

The realm of cyber is ever-evolving, and the types of threats to cybersecurity are likewise a changing landscape. Constant change presents a unique challenge; unlike topic areas in which our understanding of the basic truths has been constant for decades (or much longer), cybersecurity risks can change over a very short period. Deliberate human actions like denial and deception also co-evolve with defensive actions. One way to prevent curricula from “going stale” is to focus on basic understanding of human motivation and behavior. Although the actions and mitigations occur in a technological context, they are carried out by human actors whose actions can only be observed by their digital fingerprints. Understanding how people might exploit capabilities of new technology will help cybersecurity professionals to anticipate and understand the behavior they see on the systems they protect.

Author bios

Susan G. Campbell is an Assistant Research Scientist at the University of Maryland Center for Advanced Study of Language (CASL) and a Lecturer at the University of Maryland College of Information Studies (iSchool). Her current research focuses on determining and measuring the cognitive abilities required for different tasks within the cyber workforce. In addition to teaching a human-centered cyber course, she works on curriculum development for cyber across programs within the iSchool.

Petra Bradley (not attending) is an Associate Research Scientist at the University of Maryland Center for Advanced Study of Language (CASL). She is a cognitive psychologist interested in human learning and memory, decision making, and human-machine teaming. Her current projects focus on human trust of recommender systems and detecting insider threat. She has worked extensively with language and intelligence analysts to determine how they use information systems and what types of automated assistance can best benefit them in their work.