Comments on the NICE Cybersecurity Workforce Framework, NIST Special Publication 800-181

1. Although the current version of the framework describes software programming as an integral component of the KSA and Tasks, it would be beneficial to include the impact of artificial intelligence and robotic software on the software tools designed for cybersecurity. The current version mentions one instance of machine learning (K0238). The learning algorithms at the core of AI tools are not often vetted for biases and thresholds, and the training data set might not represent a broader population. When such tools are used to develop cybersecurity defense mechanisms, the implications are significant ranging from misattribution of malicious or undesired activities to false alarms and prolonged legal challenges.

2. The issue of ethics is mentioned briefly in one instance (K003). Current cybersecurity training models (bootcamps, colleges, universities, MOOCs, executive education) develop cybersecurity curriculum that is focused on mostly on tools in forensics, penetration testing, cryptography, strategy, legal/compliance issues and operations. I think that there is a significant gap in the development of skills for cyberpsychology analysis. This includes the ethics of data collection, analysis, tool development and attacker profiling. The NICE framework would be a great place to begin the discussion on training/curriculum development that focuses on cyberpsychology and ethics challenges. Such curriculum might already be in place in armed forces and intelligence community curricula, and it might be worthwhile investigating how those skills would augment the capabilities of a broader population.

--
Renita Murimi, PhD, CISSP
Associate Professor of Cybersecurity
Satish and Yasmin Gupta College of Business
University of Dallas