# Cybersecurity Education Breakout Report

**Leads:** Michel Cukier (University of Maryland), Melissa Dark (Dark Enterprises, Inc.), and Fan Wu (Tuskegee University)

**Scribes:** Sarah Elder (NC State) and Hossain Shahriar (Kennesaw State University)

This breakout session addresses two of the most important issues today and next ten years in cybersecurity education. These issues need to be deliberated because they have consequences for you, your students, your institutions, and the nation.

**Workforce composition**: More people, more diverse, and more qualified? How can such workforce composition be achieved? What is happening and what needs to be created for such a workforce?

**Teaching content**: What should we be teaching to what students? What will become obsolete? Which material is the most important to be taught?

After a brief introduction from M. Dark, F. Wu and M. Cukier, both sessions consisted of open discussions regarding the two announced topics. The audience was also asked what, from their viewpoint, the main topics were. Finally, the audience was asked what recommendations should be made to NSF. The following paragraphs cover these items.

Topic #1: What is Cybersecurity?
Cybersecurity is not its own discipline, yet, and may never be. Multi/interdisciplinary aspects of cybersecurity make it hard to institutionalize and expand cybersecurity as a sustainable field of study in colleges and universities. These institutional barriers are thwarting workforce development. This trend appears to be repeating itself as cybersecurity moves into K-12. K-12 cybersecurity has an additional confusion about what it is. Cybersecurity is often taught as cybersafety in K-12.

Topic #2: What is the Cybersecurity Workforce?
There is a mismatch - what should be taught is sometimes unclear for academia and for employers? The field is evolving rapidly. The interdisciplinary aspect of cybersecurity is challenging. There are many different curricula. Teachers do not know what students' background knowledge & experience will be.

Topic #3: Availability of Shared Infrastructure and Resources
We could use more investment in common resources (labs, teaching resources, hardware). “Availability and Sustainability of Infrastructure” is important to consider. Especially at small, teaching universities, hardware & software may be unaffordable. Sharing of other resources (e.g., curriculum) and best practices can enable growth of cybersecurity education.

Topic#4: Broadening Participation in Computing (BPC)
Broadening Participation in Computing (BPC) projects appear to be fragmented and an afterthought. While RFPs ask for a BPC project, there might be some mismatch between the BPC plan and the proposed research. Investment in what works - sharing, and scaling should be prioritized. NSF has developed a website on BPC (https://www.nsf.gov/cise/bpc/). In addition, the BPCnet site (https://www.nsf.gov/cise/bpc/) includes the list of approved BPC plans.

Proposition: NSF Workshop on Cybersecurity Education
Over the **last** 10 years of SaTC, much has been done to foster cybersecurity research as evidenced by the PI meeting and the 13 breakout sessions on cybersecurity research. Cybersecurity education is **perceived as less important and sometimes decoupled from traditional research** in SaTC as evidenced by one breakout session, fewer funded projects, and funding limits. However, workforce and cybersecurity education challenges are mounting and there is much expertise and potential in the SaTC community to define and address them. The main outcome of the session is a recommendation for NSF to fund a workshop **(annual or bi-annual)** on cybersecurity education:

- Identify (common) content to teach (evolves rapidly);
- Exploring how resources can be shared;
- Characterize cybersecurity workforce.