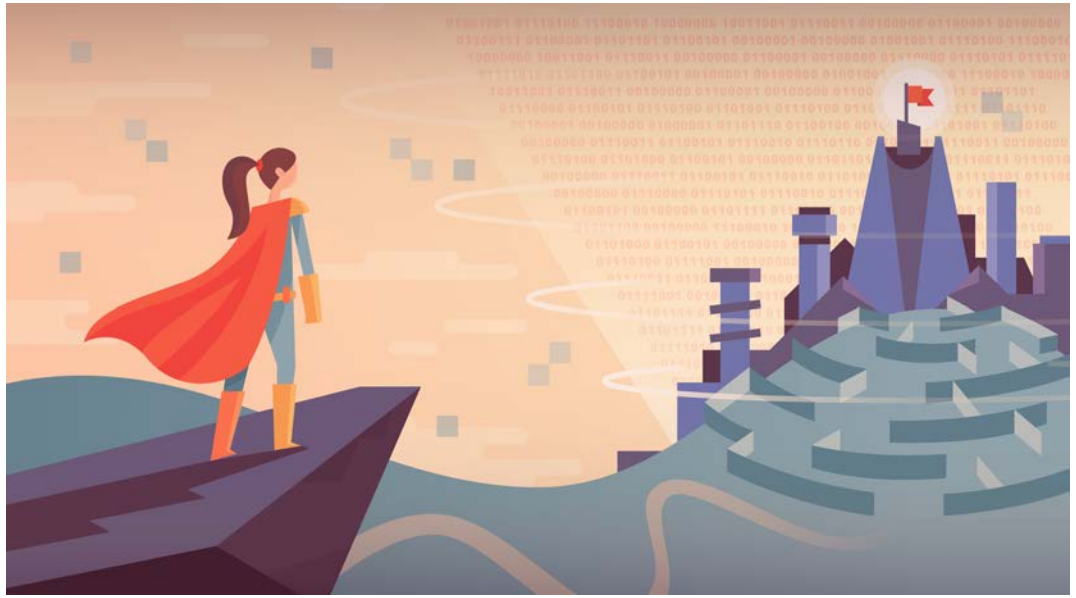
National Cyber League Update for CISSE 2020



NCL: A community where cybersecurity is a passion

NCL: a 501(c)3 non-profit organization enabling students to develop, measure and demonstrate their technical cybersecurity skills so they can bridge the gap from curriculum to career. NCL's virtual training ground is powered by Cyber Skyline.

POWERED BY CYBER SKYLINE

In 2019...

10,000
players annually

550+ academic institutions
participating annually

8,548
college players

375
4-year colleges

193
2-year colleges

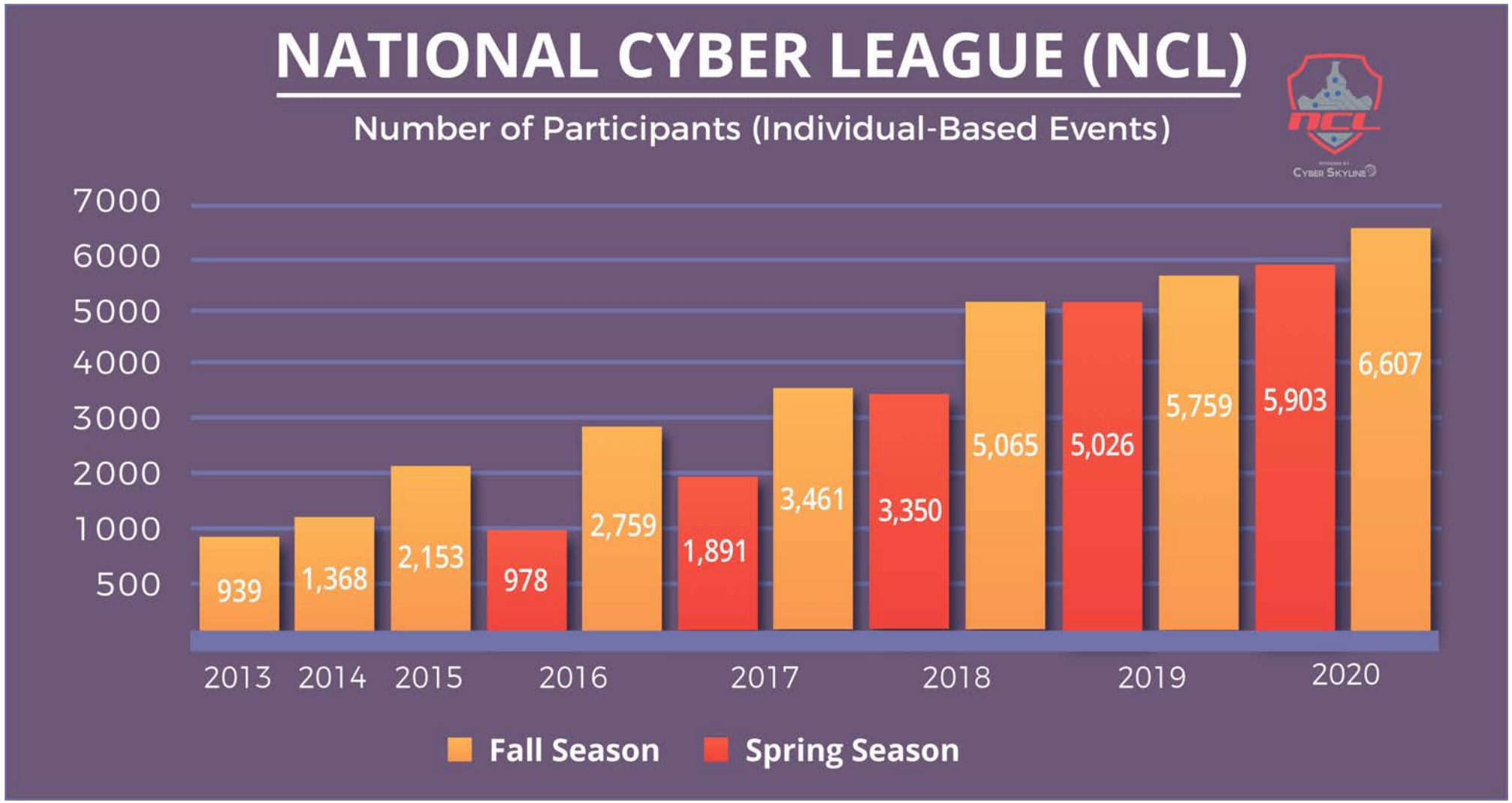
1,163
high school players

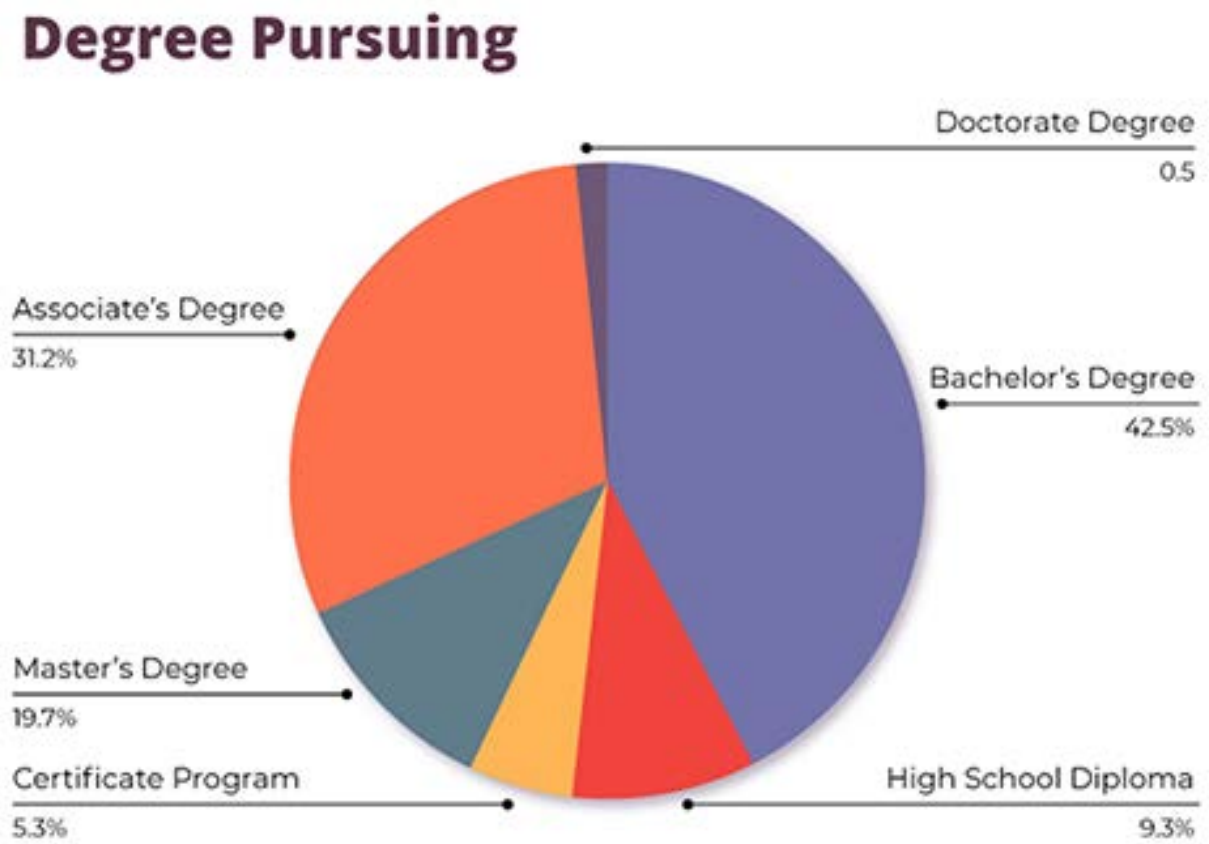
61%
of CAE schools
participate in NCL

63 out of 98
2-year CAE
colleges participate

94 out of 152
CAE-CD (Cyber Defense
Colleges) participate

11 out of 25
CAE-R (Research
Colleges) participate

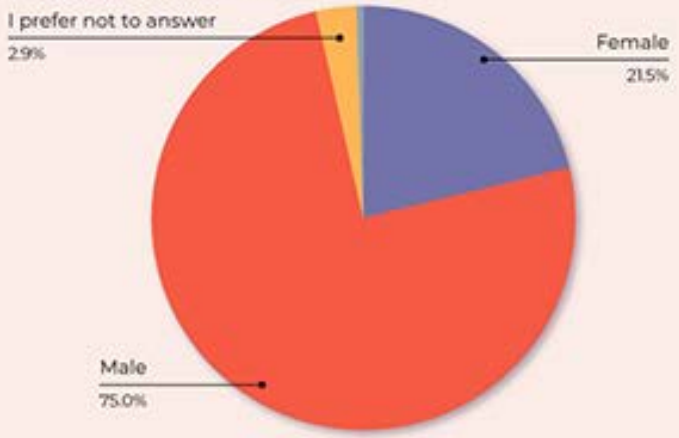

NATIONAL CYBER LEAGUE (NCL)
Number of Participants (Individual-Based Events)
7000
6000
5000
4000
3000
2000
1000
500
939
1,368
2,153
978
2,759
1,891
3,461
3,350
5,065
5,026
5,759
5,903
6,607
2013
2014
2015
2016
2017
2018
2019
2020
Fall Season
Spring Season


Degree Pursuing
Doctorate Degree
0.5
Associate's Degree
31.2%
Bachelor's Degree
42.5%
Master's Degree
19.7%
Certificate Program
5.3%
High School Diploma
9.3%

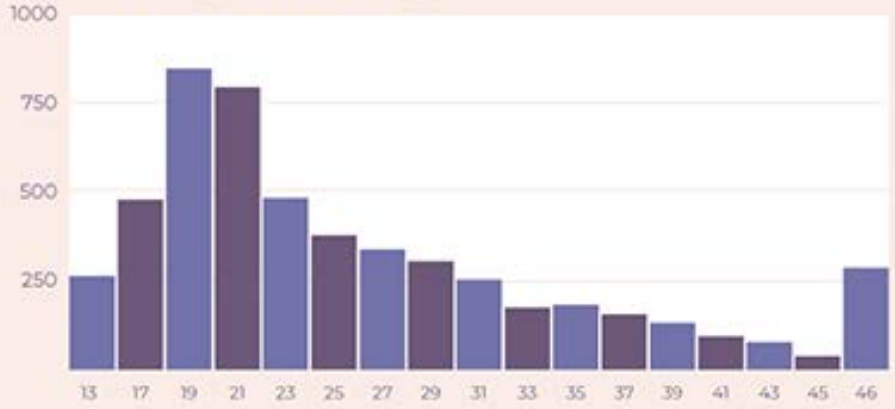
POWERED BY CYBER SKYLINE

NCL Encourages Diversity

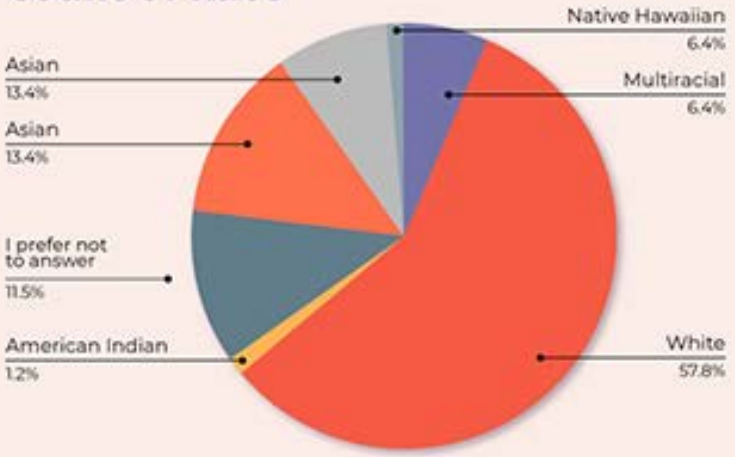
Count of Gender



Histogram of Age



Count of Race



And at CISSE 2021- a celebration of progress!

Exploring a National Cybersecurity Exercise for Universities

In cybersecurity competitions, participants either create new or protect preconfigured information systems and then defend these systems against attack in a real-world setting. Institutions should consider important structural and resource-related issues before establishing such a competition.

Lance J. Hoffman and Tim Rosenberg
George Washington University

Ronald Dodge and Daniel Ragsdale
US Military Academy, West Point

Critical infrastructures increasingly rely on information systems and on the Internet to provide connectivity between systems. Maintaining and protecting these systems requires an education in information warfare that doesn't merely theorize and describe such concepts. A hands-on, active learning experience lets students apply theoretical concepts in a physical environment.[1] Craig Kaucher and John Saunders found that even for management-oriented graduate courses in information assurance, such an experience enhances the students' understanding of theoretical concepts.[2] Cybersecurity exercises aim to provide this experience in a challenging and competitive environment. Many educational institutions use and implement these exercises as part of their computer science curriculum, and some are organizing competitions with commercial partners as capstone exercises, ad hoc hack-a-thons, and scenario-driven, multiday, defense-only competitions.

several others conducting a combination of cyberreconnaissance, network and system defense, and cyberattacks. The model for each event varies, presenting scenarios that are significantly different in execution yet very similar in effect. The exercises can serve to both introduce concepts and measure understanding of computer security and information assurance. The Cyber Security Exercise Workshop highlighted four examples of such exercises: defensive cyberexercises; small, internal, and continuous capture-the-flag competitions; national capture-the-flag competitions; and integrated, semester-long exercises.

All of the cybersecurity exercises described in this article give students a laboratory in which to experiment, just as in other fields of science. They also fulfill the same role as capstone projects in traditional engineering programs—that is, they let students synthesize and integrate knowledge acquired through course work and other learning experiences into a project

nationalcyberleague.org