PRO CYBER NEWS

Academics and Experts See Esport Potential for Cybersecurity

Millions of fans world-wide watch professional videogame players compete in tournaments of “Halo” and “Call of Duty.” In the future, some experts say, this audience could be watching cybersecurity teams compete to hack one another’s systems.

By James Rundle

Millions of fans world-wide watch professional videogame players compete in tournaments of “Halo” and “Call of Duty.” In the future, some experts say, this audience could be watching cybersecurity teams compete to hack one another’s systems.Experts are becoming increasingly convinced that cybersecurity competitions could be an ideal area for esport development. Such a format could drive youth interest and participation in the industry, at a time when a shortage of skilled recruits is reaching critical levels, they say.

“We have a shortage of talent and a shortage of diversity in the cybersecurity field, and I think, if we turn this into a sport, we could really address both of those issues,” said Daniel Manson, a professor at California State Polytechnic University, Pomona. Mr. Manson serves as commissioner of the National Cyber League, a cybersecurity competition for high school and college students held across the U.S.

League, a cybersecurity competition for high school and college students held across the U.S.

There are around three million cybersecurity vacancies globally, according to ISC2, a trade association for cybersecurity professionals. Training skilled workers can take years, meaning such shortages are likely to continue.

Broadening the appeal of the cybersecurity industry into the esports market, which has a global audience of around 453.8 million, according to research firm Newzoo International BV, could be crucial to solving this issue.

"It's a natural overlap with the massive growth we see in esports and the growth of cybersecurity itself. It's two super-hot spaces that naturally go together," said Jason Kaehler, a videogame designer at Asylum Labs Inc. He is involved in research exploring how cybersecurity contests could become esports.

One recent cyber esport competition pitted collegiate teams against each other at the HyperX Esports Arena in Las Vegas's Luxor Hotel & Casino. The tournament, known as Wicked6, had six teams compete, capture-the-flag style, on Aug. 8. The live event raised money for the Women's Society of Cyberjutsu, a mentoring program for women in cybersecurity. Microsoft Corp. and Uber Technologies Inc. were among the key sponsors.

During capture-the-flag contests, teams who complete defensive and offensive objectives win flags. Goals can range from deploying patches on their own systems in time to thwart attacks, to taking parts of an opponent's system offline.

Creating a formal structure around these games, like the National Cyber League does, is a crucial step on the road to becoming an esport, Mr. Manson said. From attracting around 1,000 participants during its first season in 2012, the league had over 5,000 students take part in the spring season this year.

About 6,000 are expected to take part in the fall season, Oct. 14 to Dec. 14, covering all 50 states, he said.

Contestants play in easy, medium and hard brackets according to performance in previous seasons. As with professional sports, participants are given scouting reports that highlight their performance over the

course of a season.

The data for the scorecards is collected and processed by a platform provided by Cyber Skyline Inc., a company co-founded by former league players Franz Payer and Toby Lin.

"A lot of [student] players have been able to leverage the experience as their replacement for on-the-job experience," said Mr. Payer. "It gives them something that they can talk about during the interview process."

The format, statistics and competitive nature of the events lend themselves well to an esports setting, and the league proves that cybersecurity competition can flourish in an organized environment, but there is a major problem: They're just not very fun to watch. While pop culture often depicts cyberattacks at lightning speeds, the reality is that cyber contests, like malicious hacking, often involve hours of poring over code, sitting in front of a computer screen. Some cyber gaming events run over several days.

That type of activity doesn't lend itself well to audience engagement, said Mr. Kaehler. Along with Phillip Porras and Rukman Senanayake from the research institute SRI International, Mr. Kaehler recently published a paper describing how a cyber capture-the-flag event could be rendered in a format suitable for esports.

In a video accompanying the paper, teams are represented by robots, and their networks as cities. Certain types of hacks, like denial-of-service attacks and attempts to corrupt patches, are represented by visuals, including missile attacks on the cities. Explosions signify successful hacks and a narrator gives context to the action.

Cybersecurity experts might complain about oversimplification, Mr. Kaehler said, but visual engagement is key to attracting players in esports. Striking a balance is key to reaching a broad audience.

"The gatekeepers would need to see the value, and see that we're treating the domain respectfully. While it may not be for the hard-core, it's great for everybody else," he said.

Write to James Rundle at james.rundle@wsj.com