loop as much as possible. The next area for focused, applied research should explore the most effective means to hunt within networks in real time. Research should move the industry closer to eliminating the detection gap instead of allowing threats to go undetected for months or even days. The AI capabilities should go hand in hand with research embedded within a hunt framework to automate the search, detection, and eviction of the adversary, while automating many of the processes that remain overly manual and time- and resource-intense. Given the talent shortage, AI technologies could help the ASEAN region leapfrog the rest of the world in building learning cybersecurity systems that evolve with additional data.

Tackling disinformation

Historically, when data was digitally stolen, the attacker kept it hidden. Today, this data is likely to be released along with a combination of valid and altered data to maximize the desired impact. Similarly, bots are often used to spread disinformation, especially on social media. R&D efforts to distinguish between content created by bots and humans could help tackle the rising use of disinformation, including using natural language processing aimed at the content itself or analytics on time frequency and other temporal patterns to expose bot-driven behavior. Because bots are a growing percentage of online traffic, any capability must also be able to separate disinformation from the streams of legitimate bot-driven advertising.

Security in the OT environment

The convergence of IT and OT has become a business imperative. The absence of standards or guidelines around IT and OT convergence remains a significant challenge, and the shortage of skilled professionals with an understanding of the nuances of industry-specific challenges amplifies the problem.

3.4.4 Anchor world-class capabilities to facilitate knowledge exchange and capability building

Attracting world-class companies with advanced capabilities has long been a strategy to facilitate knowledge exchange and develop the local industry. A pillar of Singapore's cybersecurity strategy is to use the country's status as an economic hub to attract world-class cybersecurity companies to base advanced operations, engineering, and R&D activities in Singapore. This increases access to cutting-edge cybersecurity capabilities and creates cybersecurity career pathways.

The Malaysia Digital Economy Corporation formalized a strategic partnership with the Protection Group International to help the country develop cybersecurity capabilities. The organization will share its expertise and set up a cybersecurity academy in Malaysia.

The region could benefit from establishing clusters for cybersecurity innovation. In other markets, these ecosystems are emerging in areas that provide the factors needed to sustain the development of the industry. Proximity to government cybersecurity functions creates a ready talent pool with access to job opportunities. Research centers and incubators and industry leadership in the form of national agencies, military cyber units, large companies, or chambers of commerce serve as catalysts for the growth of the local ecosystem. Establishing connections between military and government units and the corporate sector is an important way to attract and nurture talent. Global cybersecurity clusters such as Beersheba in Israel and Malvern in the United Kingdom exhibit similar features such as close links with government cybersecurity functions, strong leadership by the private sector, and the presence of training hubs (see sidebar: The United Kingdom's Malvern Cybersecurity Cluster on page 46).