Cyber Security Assignment

Find an article related to cyber security. You can use an article with any topics related to cyber security. Write an analysis of the article. Please answer **all of the following questions**.

Title: The role of national cybersecurity strategies on the improvement of cybersecurity education

- **What happened?**

  The research evaluates how top nations within the world implement cybersecurity education and training initiatives through their national cybersecurity strategic plans (NCSPs). The research evaluates the existing gaps between strategic objectives and educational content before presenting a GQO + Strategies framework to connect cybersecurity education with national strategic targets.

- **Who was involved?**

  The authors include Saleh AlDaajeh, Heba Saleous, Saed Alrabaee, Ezedin Barka, Frank Breitinger, and Kim-Kwang Raymond Choo. The authors analyze how different national governments (U.S., U.K., UAE, EU, China) and educational institutions work to establish cybersecurity curricula.

- **Where did this occur?**

  The research investigates academic and public policy domains through a worldwide comparative analysis. The authors selected NCSP examples from North America, Europe, Asia, and the Middle East for their study. The authors use the UAE University Master's in Information Security program as their case study to demonstrate the design application.

• **How did this happen? (lapse in security, mistake, etc.)**

The distance between strategic targets and educational systems emerges because of delayed curriculum updates, inconsistent relationships between official requirements and academic programs, and insufficient connections between learning objectives and teaching materials. The authors identify that numerous NCSPs include education as a priority but fail to establish specific learning outcomes for curricula.

• **What were the consequences/impacts? (individuals, legal, ethical, social, society, environment)**

1. The production of sufficient qualified cybersecurity professionals faces challenges because of workforce shortages and skills gaps that exist across numerous countries.
2. The absence of strong education systems creates a strategic weakness which puts critical infrastructure at risk while threatening national cyber sovereignty.
3. Students from underfunded educational institutions and geographic areas face limited access to the developing cybersecurity job market.
4. National strategy becomes ineffective because education systems fail to meet strategic goals, which keeps strategic objectives from becoming reality.
5. Educational institutions face three main challenges in their efforts to update curricula because they lack sufficient capacity, their faculty members need modern training, and they face limited resources.

• **What was done to address or prevent this from happening again?**

The authors suggest that curriculum design should incorporate the

GQO + Strategies framework by creating a sequence from Goals to Questions to Outcomes to Strategies, which support strategic objectives.
The authors apply the NICE framework to establish cybersecurity workforce competencies while linking educational results to national strategic objectives.
The authors show how this approach works through their example of the Information Security program at UAE University.

- **What are your suggestions to prevent this from happening again?**

National strategy updates should trigger scheduled reviews of the curriculum.
The education system should partner with private organizations to develop curricula which match current industrial requirements.
The organization should provide funding for faculty members to receive training about modern cyber threats, educational tools, and teaching methods.
The educational system should implement modular and stackable credential programs to achieve fast adaptation.
The organization should establish regional excellence centers to enhance the educational standards of institutions which lack sufficient resources.

- **Do you think this could happen again and why?**

Yes. Academic systems face challenges to keep up with the rapid pace of strategic plan development. The combination of bureaucratic resistance, funding limitations, faculty opposition, accreditation delays, and poor coordination between departments creates a high probability of repeated failures unless institutions establish formal synchronization systems.

• **What are the potential impacts including intended and unintended of cybersecurity on individuals, society, or the environment?**

Positive: The workforce will become more prepared, and national resilience will strengthen while cybercrime decreases, technological progress advances, and economic performance improves.

Negative: The focus on tactical skills creates two major issues which result in weak foundational theory education and unstable program structures. Some educational institutions dedicate excessive resources to cybersecurity education, which causes them to neglect their other academic programs. The ability of elite institutions to adapt to change will create new social inequalities between students. The expansion of laboratory facilities, server farms, and cloud infrastructure systems leads to increased energy consumption, while cybersecurity defense systems require powerful computing systems.

You can use any format you choose including sentence format, paragraph format, bullet points, lists, graphs, PowerPoint presentations, or any other format you wish.

Be as detailed as possible.

Upload the assignment to Canvas by Sunday September 28 at 11:59 pm.