# CSTEC Cybersecurity Education and Training Status and Plan

---

## 1. Introduction

The Cyber Security Training and Exercise Center (CSTEC) has been established as a national hub to strengthen practical cybersecurity response capabilities, foster skilled professionals through education and training, raise public awareness on security, and contribute to international cooperation. This report summarizes the current status of CSTEC's education and training programs, key achievements, and future development plans based on the provided presentation materials.

---

## 2. General Overview of CSTEC

CSTEC was founded under the National Security Research Institute (NSR) to address the increasing need for advanced cybersecurity education and hands-on training. Its establishment was in line with major incidents that highlighted the vulnerability of national infrastructure, such as large-scale DDoS attacks and financial system disruptions.

Key milestones include:

- Establishment of the National Cybersecurity Education Center.
- Launch of the Cybersecurity Training Center.
- Planned opening of the K-Cyber Training Institute (scheduled for 2028).

---

## 3. Education and Training Programs

CSTEC delivers a structured set of programs covering **policy, prevention, detection, and investigation**, aligned with national cybersecurity requirements:

1. **Policy** – Training on establishing and managing security policies, including infrastructure protection strategies (4 courses).
2. **Prevention** – Training on secure IT system design, development, and risk assessment (3 courses).
3. **Detection** – Training on monitoring, detecting, and responding to cyber threats (5 courses).
4. **Investigation** – Training on evidence collection, incident analysis, and forensic investigation (4 courses).

This framework ensures a comprehensive coverage of the cybersecurity lifecycle, from policy design to post-incident investigation.

---

## 4. Major Training Activities

- **Cyber Crisis Response Exercises**: Simulation-based exercises replicating real-world incidents to enhance institutional resilience.
- **iCDX (Integrated Cyber Defense Exercise)**: Advanced exercises combining multiple scenarios for joint defense.
- **Cyber Attack and Defense Competitions (CCE)**: Competitive events aimed at sharpening technical defense skills.
- **Practical Training with Security Tools**: Focused on malware response, forensic analysis, and system recovery.

These activities are designed to build both individual skills and institutional readiness against evolving cyber threats.

---

## 5. Performance and Achievements (as of 2024)

CSTEC has produced measurable outcomes in the following areas:

- Development of specialized training programs tailored to government, military, and private sector needs.
- Enhanced real-time cyber incident response capabilities through simulation platforms.
- Increased public awareness and improved professional competence in cybersecurity.
- Strengthened cooperation with academia and international organizations.

---

## 6. Sustainable Education and Training Ecosystem

CSTEC has implemented a **cyclical model (Plan–Do–See)** involving:

- **CISOs**: Policy development and strategic management.
- **Managers**: Team supervision and training implementation.
- **Practitioners**: Execution of security operations and technology application.

This ecosystem promotes continuous improvement by integrating feedback, enhancing awareness, and fostering collaboration between policy, training, and technology domains.

---

## 7. Future Development – K-Cyber Training Institute

CSTEC plans to evolve into the **K-Cyber Training Institute** by 2028, expanding its scope to serve as a national and international center of excellence.

- **Construction Start**: May 2025.
- **Completion**: First half of 2028.

- **Goals**: To build a sustainable infrastructure for cybersecurity education, develop globally recognized programs, and establish Korea as a leader in international cybersecurity training and cooperation.

---

## 8. Conclusion

CSTEC plays a critical role in Korea’s national cybersecurity strategy by combining education, training, real-world exercises, and international collaboration. Its transition to the K-Cyber Training Institute will mark a significant step in ensuring long-term resilience against cyber threats while fostering a new generation of cybersecurity professionals.