Impact of AI on Cyber and Physical Security Convergence

TechRounder PDF Edition

Live article: https://www.techrounder.com/security/impact-of-ai-on-cyber-and-physical-security-convergence/

By Vipin PG | Published January 26, 2023 | Updated March 8, 2026 | Format: Analysis | 4 min read

In brief

Improvements in artificial intelligence technology continue to prove essential to the modern world, with many of our society's integral functions benefiting greatly from newly developed AI processes. 91.

Improvements in artificial intelligence technology continue to prove essential to the modern world, with many of our society's integral functions benefiting greatly from newly developed AI processes. 91.5% of leading businesses now invest in AI on an ongoing basis, allowing for the automation of complex functions and streamlining workflows to make more efficient use of all available resources.

One such instance in which integrated AI technology continues to prove beneficial to daily operations is in developing commercial security systems, with specially designed AI automation helping security teams improve incident response times and better protect properties.

Since Artificial Intelligence is a powerful tool with unmatched potential, there are already numerous cases of the application of AI in cybersecurity. AI enhances network security, detects advanced malware, and improves cloud and IoT security. Empowering cybersecurity strategy by integrating deep tech can protect the business from data breaches, and its consequences.

Modern AI programs can assist security professionals in analyzing large data pools much more efficiently than previously, which can help bridge the gap between traditional physical and cyber security processes. But what is the wider impact of AI on cyber and physical security convergence?

Automated testing and system notifications

A major benefit of using AI within commercial security systems is the ability to leverage intelligent learning capabilities to develop automated responses. In addition, modern AI systems can discern patterns found in data over time, which can be used to understand security concerns better.

By instructing an AI program to evaluate the common uses of cyber and physical security systems, networks can be developed to alert security teams whenever an anomaly is recorded. This removes the need for human operators to monitor every aspect of a wider security system and allows security teams to allocate resources more efficiently toward critical security issues.

This concept can also be utilized to save time and resources diverted to other ongoing security procedures, for instance, the testing of physical and cyber security systems. By programming an AI tool to perform regular checks of all operational security features, the system can use learned behaviors to highlight and alert staff to suspected issues while ignoring irrelevant stimuli.

Integrated video and access control

One aspect of commercial and residential security in which AI integrations have proven to improve existing protocols is video security and access control integration. With an estimated 58% of US citizens currently working in a hybrid role, the need for security teams to reliably monitor building access outside of traditional operating hours is only set to increase.

Security teams can develop automated responses designed to validate and accommodate visitors by leveraging AI technology alongside existing video and access control systems. Guests need only interact with an on-site reader to initiate a programmed voice response configured to guide staff, delivery couriers, vendors, and other individuals through any required access validation processes.

Further integrations can also be developed to send alerts to security staff in direct response to predetermined stimuli; for example, if an intruder attempts to force open an access point or motion is detected in a particular area, security staff can be remotely notified in real-time via their smartphones.

Remote management of cloud-based tools

Implementing cloud-based security tools can help teams better manage and navigate physical and cyber security systems, but hosting all of a site's security features within a cloud-based network will require a sophisticated management system to detect and prevent hacking attempts.

Integrating an AI management feature is ideal for this use case, as modern AI technology can learn how the system is commonly used to actively monitor all installed security functions and adjust its operation in direct response to any detected anomalies.

This means essential security features such as school door locks, firewalls, and on-site CCTV cameras can be easily viewed and operated by remote security teams, safe in the knowledge that any suspicious or potentially criminal activity will be detected and responded to automatically by AI tools.

Bridging the gap between cyber and physical security

As the convergence of traditional physical security features and cybersecurity processes through the implementation of cloud security and remote-management functions continues to be adopted heavily by businesses, schools, and other organizations, exploitable gaps between the two can begin to form.

Once physical security systems such as cameras and access control were overseen by security guards and IT teams implemented cybersecurity protocols, now both processes were intertwined. By leveraging AI tools for vulnerability scanning and management to help manage all aspects of a security network, programs can learn to spot anomalies across both systems and uncover potential gaps that could be exploited.

As AI tools can analyze much larger data sets with a far smaller margin of error than human security teams can, implementing these programs can help converged physical and cyber security departments better understand the system and focus on areas of concern.

Final word

As more organizations begin to view physical and cyber security protocols as a single consideration, the need for unified security teams to understand the intricacies of each process continues to grow. To successfully bridge skill gaps and achieve effective physical and cyber security convergence, the development of artificial intelligence security management systems seems essential.

By leveraging the learning capabilities and data analyzing functions of modern AI tools alongside existing physical and cyber security protocols, security teams can develop robust defenses and reliable automation designed to provide faster responses and more effective integrated security systems.

References

1. jelvix.com - blog / machine-learning-in-cybersecurity - https://jelvix.com/blog/machine-learning-in-cybersecurity

2. techrepublic.com - article / 58-of-americans-have-hybrid-work-options-but-challenges-remain - https://www.techrepublic.com/article/58-of-americans-have-hybrid-work-options-but-challenges-remain/

3. avigilon.com - blog / school-door-locks-systems - https://www.avigilon.com/blog/school-door-locks-systems

4. forbes.com - sites / forbestechcouncil - https://www.forbes.com/sites/forbestechcouncil/2018/11/28/10-cybersecurity-protocols-every-tech-professional-should-follow/?sh=3eb182673ae8