

E8 - Imaging Technology Used to Detect Hidden Explosives

Weapons and Security Threats

2026 Spring Symposium

Abstract

Imaging technology plays a critical role in detecting hidden explosives, weapons, and other security threats across military, aviation, and public safety. Advanced systems such as x-ray and computed tomography (CT) help with the non-invasive inspection of people, baggage, and cargo to analyze undetected security threats. As security threats continue to evolve, ongoing advancements in imaging are essential to maintain effective threat detection. Imaging technology is also a vital component of military security operations. Imaging helps the military detect injuries, explosives and weapons when in a combat zone. These technologies help integrate automatic threat recognition with artificial intelligence. This paper explains cybersecurity as a whole and how imaging plays a crucial role in military advancements.

Imaging Technology Used to Detect Hidden Explosives

Weapons and Security Threats

Introduction

From airports to medical checkpoints, imaging plays a critical role in identifying hidden explosives and security threats that are not visible to the human eye. People don't normally think about the science and background information of cybersecurity. Imaging helps to detect cyber-attacks and other unknown threats. Along with imaging used in cybersecurity, it also plays a very important role in the military. Whether it's medical clearance using imaging prior to military acceptance or imaging on the battlefield, x-ray is the most important aspect of military medicine. This paper will discuss what cybersecurity is, how imaging goes hand in hand with cybersecurity, and the crucial role that imaging plays in the military.

Discussion

What is Cybersecurity and What is it Used For?

Every day, companies and individuals rely on digital software to store information and data. This process is called cybersecurity. Cybersecurity can be defined as the practice of protecting people, systems and data from cyberattacks by using various technologies, processes and policies. (Lindemulder, 2025) Cybersecurity was designed to aid computer networks and information programs against various cyber-attacks. Cybersecurity can be used in numerous ways, including digital forensics, data preservation, cybersecurity forensics, medical imaging, and forensics imaging. Digital forensics is known as creating exact copies of data and analyzing the data from a cyberattack. Data preservation helps to make sure the data is untouched and usable for legal processing. Cybersecurity forensics helps forensics create exact

copies of data without making alterations to the original evidence. As seen in figure 1, cybersecurity displays an image, and if any threats are detected.



Figure 1 [Mettler Toledo](#)

Medical imaging cybersecurity protects patient information, and forensic imaging detects pictures that were captured of potential threats. Cybersecurity is used in almost every aspect of everyday life; you just might not know it. Without cybersecurity, the United States would experience major setbacks such as financial loss and identity theft. Cybersecurity relies strongly on the use of imaging technology.

How is X-ray Used in Cybersecurity

As radiology systems become increasingly digital and complex, cybersecurity is essential for protecting patient data and ensuring safe and reliable medical imaging technology. X-ray scanners in cybersecurity are essentially incisive tools that “strip search”, sweeping data in its entirety. (Reason Labs, para 2) That being said, x-ray has certainly evolved throughout the last several decades. X-ray was established in 1895 by a brilliant man by the name of Wilhelm Conrad Roentgen. Following this discovery, the first portable machine was made in 1909. The portable x-ray machine was a huge advancement for x-ray, especially in the medical setting. Portable imaging was such a big advancement because it allowed for easier patient interaction, more opportunity to get exams completed faster and less restriction with needing an x-ray room. Fast forward several years to 1970, x-ray used a one-dimensional scanner that

focused on the detection of weapons, contrabands and explosives. Along with this advancement, picture archival and communication systems (PACS) was introduced. PACS allowed for a safer, more effective, better management and communication with patient medical records and imaging. The use of CT scanners was becoming significantly more popular allowing for greater detail. CT scanners also help reveal smaller and more hidden objects that could be potential threats. With all of those aspects intertwined, imaging is now the primary foundation for cybersecurity. Imaging is used every day in airports and business to help detect incoming cybersecurity threats.

The Future of Cybersecurity

Looking ahead, the future of cybersecurity will rely heavily on advanced technology such as x-ray imaging in order to secure information hardware. However, some advancements have to be made with x-ray and cybersecurity. One of those ways is to start implementing more AI technology for the sole purpose of a higher speed and accuracy than the human ran scanners. As previously stated, we are using CT more now than ever to expose hidden threats. As cyber threats become increasingly more frequent and complex, automation is emerging as a critical tool in the building blocks of stronger cybersecurity. Automation is defined as “the application of technology, programs, robotics or processes to achieve outcomes with minimal human input” (IBM, para 1). Automation is said to be a big advancement, as it will make x-ray machines more efficient and capable of detecting real time threats as well as automatic classification of objects being scanned. Another improvement in the future of cybersecurity is portable imaging. Research teams are working to develop even more portables to make them more affordable and accessible to technology users and create a broader range. With the advancements of AI, the speed and accuracy of threat detection will increase.

Security Threats in Airports

It's no surprise to anyone that airports are an easy target for cyber-attacks. This year alone, the aviation industry has experienced a significant rise in cyber-attacks affecting millions of passengers (Garcia, 2025). The security prevention measures that are present in airports include perimeter security, crowd management, baggage screening, parking control, pedestrian safety, cybersecurity attacks and evolving threats. Perimeter security is the first line of defense places such as airports. "Airports must maintain tight perimeter security to prevent unauthorized individuals from accessing buildings, runways, and taxiways." (Delta Scientific, 2025). An example of perimeter security in the airport setting are the 10-foot fences around the whole airport. These fences serve as a deterrent, made to ensure that no one is able to harm the planes or passengers. When there are a lot of people, it's natural that people may spread out, covering some emergency exits. Covering emergency exits can affect the screening procedures that need to be taken. This is called crowd management. This issue may reduce visibility for staff and delay emergency responses, because people are crowding in front of the exits. This results in frustrated travelers, causing staff to skip important security measures. Staff shortages and increasing passenger rates introduce new screening challenges for TSA. With baggage screening being one of the most important parts of airport security, TSA is working with new technology to improve the timing and accuracy of the machines. Airports now offer a 3-dimensional scanner which is beneficial for scanning electronic devices and tightly packed travel bags. In figure 2, you can see an example of the 3-dimensional scanner image of a carry-on bag. You can see how detailed the scanners have to be in order to detect any and all threats. The normal colors that will appear on a CT baggage scanner are blues, oranges and greens. These colors indicate there are no threats, those are just the standard colors of more materials due to different types of

fabrics. Although colors are helpful, personnel have to be diligent about looking at the shapes as there are some threats that will show up those colors because of their material.



Figure 2 [Prep Terminal](#)

Parking control limits access of vehicles in designated areas. Thousands of vehicles come in and out of airports every day, causing concerns with traffic and flow, which endangers passengers and staff. Some ways airports are implementing parking control are ticket booths, control beams, and shuttles. Pedestrians are constantly being monitored to ensure their safety. Pavement markings and designated signs are put into place to help keep pedestrians safe while at the airport. Using new technology at airports means more room for hackers to gain control of the system. An example of cybersecurity is employees and contractors having access to the systems data as well as customers and traveler information. A way to prevent is regularly scheduled updates, effective staff training, and all endpoints.

The Use of X-ray in the Military

In the military, x-ray technology supports national security by detecting concealed threats and safeguarding crucial equipment. X-ray plays multiple roles in the military, from identifying injuries on the battlefield to screening for contrabands and ensuring structural integrity (Carlson, 2024). X-ray is essential for identifying fractures, dislocations, and other injuries. The use of x-ray is critical in battle, because you need an immediate diagnosis for treatment. X-rays also can pinpoint the location of shrapnel and bullets or other objects that have

been embedded in the body, helping with surgical removal and minimizing long lasting effects. Orbital x-rays are very important for MRI clearance to check for potential bullet fragments that got caught in the eye. Chest x-rays are utilized to monitor certain lung conditions, ensuring readiness and health of all military personnel. Imaging is essential prior to entering the military, during active duty, and post-military.

Modalities Used in the Military

Computed Tomography

Computed tomography scanning is the workhorse of the battlefield (Gourley, 2019). CT scans are the quickest and most detailed imaging machine used in the military. However, that comes with a price. CT has the highest amount of personnel usage, resulting in the most radiation. Using that much radiation affects the ALARA guidelines. ALARA is radiation dose protection guidelines that stand for as low as reasonably achievable, which advocates for the reduction of radiation doses to both patients and personnel for their protection. ALARA is hard to maintain when you could have multiple parts to scan on just one soldier. In figure 3, you can see a bullet is detected using a CT scanner.



Figure 3 [Fine Arts America](#)

Magnetic Imaging Resonance

Magnetic Imaging Resonance is important in military medicine. MRI is a non-invasive imaging technique that uses radio waves and strong magnetic fields to view soft tissue structures

and organs. MRI is the preferred choice of imaging in the military because of its versatility. Its versatility allows for functioning images, assessment of blood flow, brain activity and tissue characteristics. The MRI machine used in the military is special. MRI exams include T1 and T2 weighted images. T1 and T2 help to accurately look depict images of the brain and the structures of the brain. These features can help identify injuries in white matter. MRI plays a crucial part in military imaging because it helps to identify injuries and diseases, which could impair military personnel on the battlefield.

Interventional Radiology

Interventional Radiology is very important in military imaging especially in a compact environment. Interventional radiology is termed as a type of medical specialty that uses imaging to perform minimally invasive procedures in order to treat serious medical conditions. Interventional radiologists perform procedures to stabilize the condition of critically ill soldiers in trauma situations. The radiologists treat injuries that occurred in combat such as blood clots, fractures, or other traumatic medical conditions. In figure 4, you can see the interventional radiologist performing a procedure in the military OR under a sterile field. A sterile field is an area that is kept clean and free of germs and microorganisms during a medical procedure. Interventional radiology has quickly become an essential tool in the military, allowing for life-saving procedures to be performed quickly, precisely, and with minimal invasiveness.



Figure 4 [API](#)

Conclusion

As security threats become more complex, imaging technologies will continue to remain the critical line of defense in preventing attacks. Ongoing improvements in resolution, automation, and detection capabilities will further strengthen the role of imaging in protecting people and businesses. Although imaging is not the only aspect of cybersecurity and protection, it is a significant element in the overall resolution of cybersecurity. Military medicine is also reliant on imaging. Without accessible imaging on the battlefield, our troops would suffer and could risk the possibility of not receiving life-saving measures. Without strong cybersecurity, even the most advanced technologies cannot operate safely or reliably.

References

- Admin. (2023, December 29). *The evolution of Forensic X-ray body scanners: A historical perspective - linev innovations*. Linev Innovations -. <https://linevinnovations.com/articles/the-evolution-of-forensic-x-ray-body-scanners-a-historical-perspective/>
- Carlson, R. (2024, April 21). *How are X-rays used in the military?: [February updated]*. TheGunZone. <https://thegunzone.com/how-are-x-rays-used-in-the-military/>
- Gourley, S. R. (2019, December 9). *Military medicine: Imaging technology*. Defense Media Network. <https://www.defensemedianetwork.com/stories/military-medicine-imaging-technology/>
- Jonker, A., Lindemulder, G., & Kosinski, M. (2026, January 27). *What is cybersecurity?*. IBM. <https://www.ibm.com/think/topics/cybersecurity>
- Master the TSA X-ray ort with an extensive question bank and expert prep*. Prep Terminal. (2025, August 19). <https://www.prepterminal.com/tsa-cbt-x-ray-object-recognition-test>
- ReasonLabs. (n.d.). *What are X-ray scanners?.* What are X-Ray Scanners? Enhanced Cybersecurity Network Scanners. <https://cyberpedia.reasonlabs.com/EN/x-ray%20scanners.html>
- Scientific, P. authorBy D. (2025, March 25). *7 common airport security challenges: Delta scientific*. Delta Scientific Corporation. <https://deltascientific.com/2025/03/25/7-airport-security-challenges/>
- Singh, A. (2024, June 18). *Enhancing threat detection with X-ray imaging*. AZoOptics. <https://www.azooptics.com/Article.aspx?ArticleID=2635>

Team, C. E. (2024, May 4). *Advancing military operations through the use of portable imaging devices - combat axis*. My Blog. <https://combataxis.com/use-of-portable-imaging-devices/>

Thorpe, J. (2024, October 8). *The future of security X-ray technology* . Security Journal UK. <https://securityjournaluk.com/the-future-of-security-x-ray-technology/>

TSA issues new cybersecurity requirements for airport and aircraft operators | Transportation Security Administration. Transportation Security Administration . (2023, March 7). <https://www.tsa.gov/news/press/releases/2023/03/07/tsa-issues-new-cybersecurity-requirements-for-airport-and-aircraft>

Tyson, J., & Grabianowski, E. (2023, August 18). *How airport security works*. HowStuffWorks Science. <https://science.howstuffworks.com/transport/flight/modern/airport-security4.htm>

What is cybersecurity? | cisa. America's Cyber Defense Agency . (2021, February 1). <https://www.cisa.gov/news-events/news/what-cybersecurity>