INTELLIGENCE AND DETECTION

Picture credit: Sentinel Photonics

As laser technology continues to evolve, so must the strategies and tools used to counter it

Jackson White *on the part lasers play in protecting borders and national security*

Lasers have become ubiquitous in security and defence applications worldwide. Initially developed as precision tools for targeting, range finding and reconnaissance, their proliferation now extends to various adversarial tactics, including counter-surveillance, drone guidance and, of course, hybrid warfare.

As their use expands, so too does the risk they pose. Security forces, infrastructure, and even national sovereignty remain vulnerable without the ability to detect and counter these laser-based threats.

From the battlefields of Ukraine to border conflicts and domestic security threats, lasers are playing an increasingly destabilising role, propelled by advancements in power and wavelength diversity. Understanding the dangers and how to best defend against them is more critical than ever.

This article explores the growing threats of lasers, the importance of laser intelligence (LasINT) in protecting security forces and national infrastructure, and the need for countermeasures to mitigate the threats.

Civil and national security threats

Recent years have seen lasers presenting multiple threats to security and civic life, from targeting and eavesdropping on government departments to gathering sensitive information and assassination attempts.

Civil aviation and law enforcement agencies have reported increased laser attacks on aircraft, particularly helicopters hovering over urban areas. Pilots taking off or landing at major airports and airbases also face potential retinal damage from high-powered handheld lasers. They must decide fast if they will abort their mission or risk never being able to fly again.

Border security forces, too, are facing many new laser-based challenges. During recent geopolitical tensions, adversaries have used handheld lasers to target border patrol officers, dazzling them and reducing their effectiveness. The ease of access to high-powered lasers exacerbates this issue, allowing non-state actors and criminal organisations to fully exploit the technology.

Additionally, protests and civil unrest have seen lasers used to disrupt surveillance cameras, blind security forces, and interfere with law enforcement operations. Laser range finders are increasingly integrated into a growing number of targeting systems and are used to provide precise targeting information by accurately measuring the distance to a target. Potential would-be assassins have used these lasers to pinpoint the location of their target. One of the most recent examples was the assassination attempt on Donald Trump at a rally in July 2024, in which counter-sniper teams retrieved a range finder.

THREATS TO COVERT OPERATORS

Invisible laser systems – sniper finders, rangefinders and designators – are not always used to cause direct harm. Instead, they can help adversaries locate hidden snipers, gather intelligence, and gain information to build greater situational awareness. Since these lasers are invisible to the naked eye, users are unaware of their use, making detection and protection all the more challenging.

Such use of lasers can reveal the position of even the most covert operators – from hidden snipers, security forces, or border guards. When they use any type of magnified optic – rifle optics, night vision goggles, thermal cameras, vehicle periscopes or binoculars – laser light is bounced back to the source by retro reflection, enabling the target to be easily detected.

EAVESDROPPING AND ESPIONAGE

Lasers have also become potent instruments of espionage. Laser microphones, for instance, can be used to eavesdrop on conversations from a considerable distance, threatening national and government security. These listening devices are designed to pick up the vibrations produced by sound waves as they hit resonant materials or surfaces such as windows. Small subtle vibrations can be detected by a laser, which are then translated into audio signals, effectively allowing adversaries to listen to sensitive discussions without ever stepping foot inside the target location.

This is useful because it allows security and counter-terrorism teams to remain concealed. On the flip side, if teams wish their conversations to remain confidential, they must adopt the ability to detect these microphones – similar to the sweep of a room to detect physically installed electronic microphones, space or area can be examined to ensure no laser is being deployed.

Governments, corporations, and security agencies must be aware of this emerging threat, implementing laser detection technologies to sweep for such espionage tools. By identifying and neutralising laser microphones, organisations can protect classified information, corporate secrets and national security interests.

USE IN DEFENCE

Laser designators can guide military attacks with devastating accuracy. They are used to illuminate a target and allow munitions or artillery to follow the target to pinpoint accuracy every time, reducing collateral damage and ensuring a first-time hit.

Recently, in a bid to destabilise the EU, Belarus recently sent refugees to Poland. In response, Poland increased its border guard to control the flow, whom Belarus targeted with handheld lasers to dazzle and cause harm. These short-range lasers are capable of causing eye damage.

RISE IN DRONES

Drones are often considered a significant threat because they can get dangerously close to targets. Onboard laser designators can guide attacks, while other drone-mounted lasers can gather intelligence and information.

In the ongoing Russia-Ukraine war, Russia has deployed laser-guided artillery driven by drones that allow artillery units to engage targets with exceptional accuracy while staying several kilometres behind the front line. A more sinister tactic that has emerged from the conflict is the use of laser-guided suicide drones, adapted to allow long-range, unjammable and deadly accurate targeting.

Drone swarms, which are more challenging to combat using traditional radio frequency methods, have driven the development of laser systems, like the UK's Dragonfire system, to counter these threats by melting and disabling drones mid-flight.

ONCE A LASER SOURCE HAS BEEN IDENTIFIED, INFO CAN PASS QUICKLY TO GROUND TEAMS

THE INVISIBLE THREAT

The use cases are clearly increasing, growing the threat to national security. However, a significant challenge is that many of these lasers operate in non-visible wavelengths, making them undetectable. Without advanced laser detection systems, security forces remain in the dark about when and where they are targeted.

Knowing which laser type is used could mean the difference between life and death. That is why there is a growing need for innovative laser detection systems that keep up with the well-known uses of lasers across a wide spectrum.

To succeed in the face of threats, teams must have a real time understanding of what laser systems their adversaries are using and how these might threaten them. That threat data allows teams to use enemy laser signatures and signals against them and to facilitate laser intelligence (LasINT).

LASER INTELLIGENCE: BENEFITS AND USE BY SECURITY TEAMS

Detecting lasers is about more than protection – it's also about laser intelligence. Understanding what laser events are taking place in a specific environment can help build an accurate intelligence picture.

It can be achieved through laser intelligence (LasINT), which is intelligence derived from laser detection. The key lies in advanced detection systems that provide immediate alerts and precise data about the type of laser being used. The result is enhanced situational awareness, more informed decision-

making, successful counterattacks, deterred future attacks, and even turning the tables on adversaries by feeding their signals back to them.

LasINT allows strategic intelligence to be gathered so that teams can understand which adversaries are deploying laser-based tactics and how they are evolving. Security forces can adapt their countermeasures by understanding how adversaries use lasers.

LAW ENFORCEMENT AGENCIES HAVE REPORTED INCREASED LASER ATTACKS ON AIRCRAFT

Once a laser source has been identified, information can pass quickly to ground teams, who can take necessary action in order to neutralise or alter the course of that particular threat. In essence, collecting data and being able to transfer it as quickly as possible can provide a critical countermeasure to protect teams, critical national infrastructure and security teams.

Integrating LasINT into broader security and military intelligence frameworks will be crucial in addressing the challenges posed by laser-based threats. Governments and security forces should consider their investments in cutting-edge laser detection technologies to ensure they stay ahead of adversaries who are increasingly weaponising this technology.

STAYING AHEAD

As laser technology continues to evolve, so must the strategies and tools used to counter it. Governments, law enforcement agencies, and military forces must embrace LasINT as a critical component of their security operations. The message is clear: those who fail to understand and detect the undetectable will find themselves vulnerable to the growing threats of laser warfare.

In today's increasingly complex threat environment, staying ahead of laser technology is not only important, but essential for ensuring the safety of defence personnel, law and security enforcement, and civil society. Ultimately, organisations seeking to enhance their security posture must invest in detection to avoid being caught unaware.

The widespread availability of high-powered lasers, coupled with their increasing use in military and civilian disruption tactics, underscores the urgent need for advanced laser detection systems, such as those provided by Sentinel Photonics. Whether protecting national borders, securing critical infrastructure, or safeguarding military personnel, the ability to detect and respond to laser threats is essential ●

Jackson White is Head of Commercial at Sentinel Photonics.

The key lies in advanced detection systems that provide alerts and precise data about the type of laser being used

Picture credit: Sentinel Photonics