Digital Intelligence

BAE SYSTEMS

Protocol- and System-aware Effect Development

Cyber and Electromagnetic Activities

Protocol- and System-aware Effect Development

In contrast to EW, CEMA includes techniques that extend further up the technology model – from the physical layer right up to applications. Protocol-aware effects can achieve longer-lasting, controlled impact, with lower probability of detection. However this requires a deep understanding of both the protocol and the wider system in question.

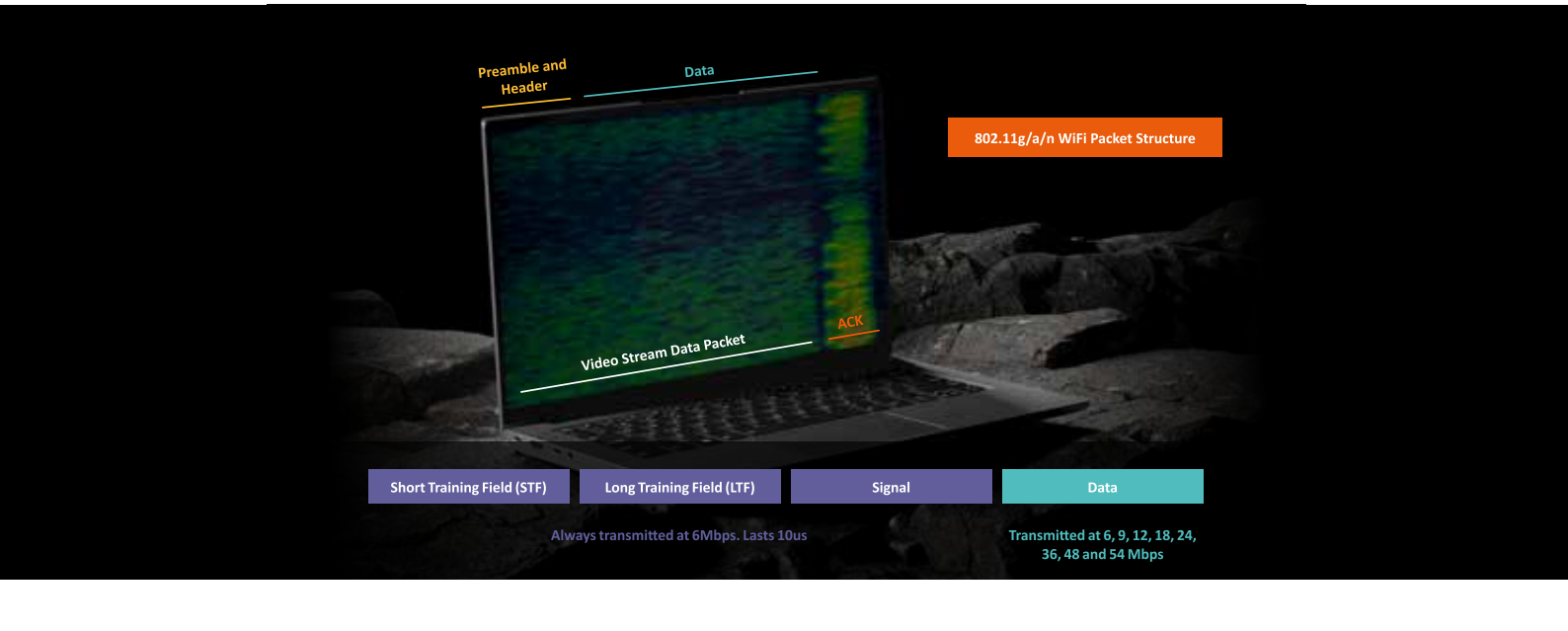
Vulnerability research is an overarching term for the identification of security threats or opportunities in operational systems. This is one of the first steps in the development of novel CEMA, driving the engineering and development of a new capability as part of an iterative approach. For example: identification of a new threat could be followed by automated recognition and later exploitation.

Requirements to Deliver

Developing these high-impact effects requires a team with deep knowledge of communications standards and computer systems, combined with analysis, modelling, simulation, and rapid prototyping capabilities. This must be combined with the ability to capture a new signal of interest and transport it back to expert analysts and developers with ease – a "signals analysis lab" comprising of both appropriate equipment and processes. Finally, it is vital that a responsive effect can be deployed back out to platforms rapidly, so that benefits are realised before the pace of war progresses.

Our expertise in vulnerability research, operational analysis, and development of CEMA capability can take customers from first detect right through to effect. Our skilled analysts have a deep knowledge of waveforms and communications standards, enabling the creation of new effects to deny, degrade, disrupt or deceive.

These skills have been put to use in developing 'fast reaction' electronic attack effects. This form of attack detects and disrupts the headers ('preamble') of a digital communications protocol. In contrast to traditional electronic attacks, they are targeted and low-power – requiring less energy, reducing the probability of detection, and limiting collateral impact.



Cyber and Electromagnetic Activities

The electromagnetic spectrum (EMS) underpins our daily lives, and modern warfare. It enables both communication and sensing. But as the demand placed on it continues to grow, it is increasingly both congested and contested. Cell phones use spectrum close to safety-critical radars, while in combat, commanders wish to deny their enemies' use of the EMS while guaranteeing their own. The increasing complexity and interconnection of wireless systems have blurred the traditional lines between 'cyber' and 'electronic warfare' (EW), leading to the concept of 'cyber and electromagnetic activities' (CEMA).

Increasingly, CEMA is being seen as a fifth domain of warfare. To maintain their defensive strength, states must ensure they have a CEMA enterprise that can operate with:

Speed

Agility

Versatility

BAE Systems Digital Intelligence has over 30 years' experience providing solutions to complex problems across the cyber and electromagnetic environment.

Our expertise in CEMA includes:

- Software-defined Electronic Warfare
- Versatile Low Size, Weight and Power Payloads
- Sovereign Capability Development
- Protocol- and System-aware Effect Development
- Future-proofing Platforms for CEMA
- Synchronisation and Coordination of CEMA
- Tactical CEMA
- Operational Analysis
- Azalea Data & Insights Radio Frequency Mapping

BAE SYSTEMS

To learn more about our CEMA integration capabilities. visit baesystems.com/CEMAintegrator

Europe & ME: +44 (0) 203 296 5900 | Americas: +1 877 277 22315 | Australia & NZ: +61 3 8623 4400 | Asia :+65 6714 2100