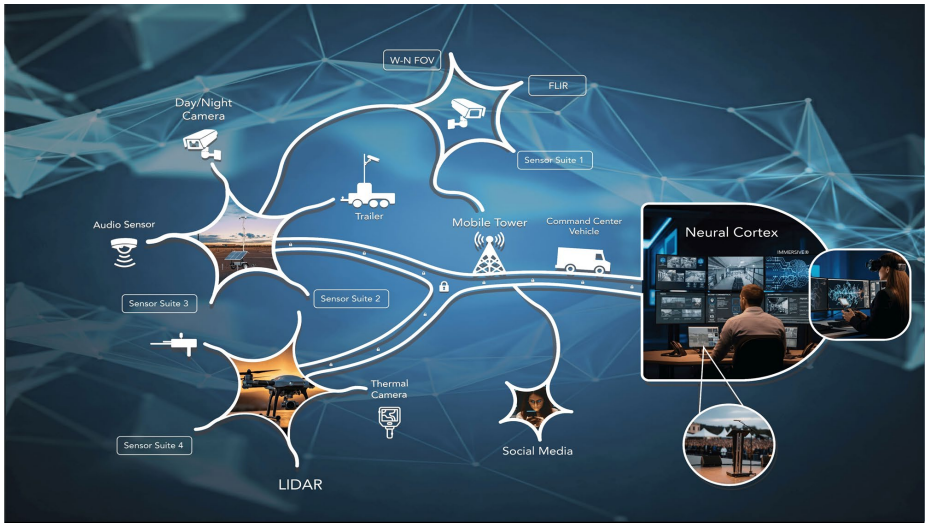
An IMMERSIVE® White Paper © 2025

11435 Allendale Drive
Peyton, CO 80831
(719) 331-8930
WWW.FSPScorp.com



Neural Perimeter Security Network℠

Beyond the Human in the Loop Learning Model - an IMMERSIVE® Review

By: Pat Morgan, President & CEO

January 2025

Contents

Introduction

The Neural Perimeter Security Network℠ (NPSN) focus developed in this IMMERSIVE® White Paper is used to provide insight to the topology needed for engaging the elemental asymmetric shifts in Human in the Loop models which are now dated. [1]. The basic definition of Human in the Loop[2] (Human Factors) is: *a model that requires human interaction, allowing humans to modify the output of the system.* The correlation to Neural Perimeter Security Networks℠ is that current R&D funding is technology decision-based, not developed as an asymmetric threat analysis resultant. This IMMERSIVE® White Paper in no way can begin to review the myriads of security programs and departmental Crime Prevention Through Environmental Design (CPTED) theory[3] and systems. However, it will instead correlate human-based decision "Kill Chains" that must leverage technology but not abrogate human responsibility for the event's outcomes.

Problem Centered Approach[4] will Drive the Perimeter Security Model

This approach focuses towards defining and understanding the security problem prior to designing and then evaluating the protective mitigation system (Garcia, 2008, p. xvii).

Recent law enforcement incidents within the protective security perimeter have underscored that organizational malaise, whether in federal, state, or local agencies, or enterprise campuses, can be attributed to the relevancy of their teams and tools. The security vision and mission must be focused on a highly evolving threat landscape by

[1] https://www.af.mil/About-Us/Fact-Sheets/Display/Article/104463/air-force-research-laboratory/%20/lang/air-force-research-laboratory/

[2] AI generated on: Artificial Intelligence and Deep Learning in Pathology, 2021 ScienceDirect(Elsevier)

[3] American Institute of Architects, 2004, p. 45

[4] Garcia, 2008, p. xvii

trained professionals, not managed hierarchy or stock portfolio maximization.

Security Body of Knowledge

The security practice and industry has been historically focused on tiered extracts of criminology and industrial threats that makes for a systemic development of components, than overall "Force on Force" planning. The use of force, especially deadly force, is not sociologically acceptable as when executed within the LE community.

Team IMMERSIVE® Solution

Our Team's solution to transformational perimeter security design and development is to place the responsibility for protecting the asset, within the perimeter, conclusively in reactive Kill Chain Human in the Loop execution. The three main areas of the Neural Perimeter Security Network are:

1. Command and Control
2. Awareness and Surveillance
3. Asymmetric Threat Elimination

Typically, in the Physical Security and Emergency Management Incident Management protocols, the hierarchy of process elements are: Detect, Analyze and Respond. [5] Our team sees a key precursor to these elements as being Normalization of the area of responsibility. In order to affect the Detection phase of the incident protocols, a baseline of the normative environment needs to be developed. The various security models and theories relegate the surveillance aspect of an incident to a peripheral role, and recent events have shown that if persistent surveillance had been rendered into a holistic view of the area, key indicators of activities and threats would have changed the outcome of a deadly force encounter, both on the perpetrator and LE community's reaction.

Benefit 1

The team's solution of utilizing strategic and low observable reconnaissance assets produces a baseline from which a wide range of sensors that neural analytics (AI) can be applied. An LE perimeter response plan based upon active awareness has a substantial advantage in Time To Mitigation above a reactive model. Reactive security models are not only inefficient but can execute the wrong application of force level for an evolving asymmetric threat.

Benefit 2

The Neural Perimeter Security Network℠ (NPSN) integrates into the Human Element at the pre-incident stage and optimizes the rapidly evolving AI-based sensor technologies and behavior analytics to segue' into the Detection phase of incident management. Use of wide spectrum video, audio, social media and LIDAR imaging analytics are just a few examples of presenting situational anomalies to the security decision makers to expedite potential and actual detection of developing threats to personnel and property.

[5] FEMA, NIMS 3rd Edition, Oct 2017

Benefit 3

The Team's NPSN architecture responds as an active interruption of the adversary's Kill Chain processes. The application of NPSN responses to the threat's origination, rather than when an attack is occurring can dramatically reduce the damage. The adaptive NPSN model is strongly rooted in pre-empting the asymmetric threats now expanding by both technology and bad actor use of surveillance gap analysis.

A moldable NPSN development environment requires that the Decision Makers are central to the neural paths of technology and human inputs and live streams.

Implementation

The Team IMMERSIVE® recommendation is to foster a collaborative neural problem-centered development environment. The NPSN will be enabled by the private, commercial, federal and academic communities joining forces to transition from process-driven security models to end state result-driven architectures.

Point: The resulting neural topology will revolutionize the security of live and fixed perimeters.
Counterpoint: Great care must be considered in this societal facing market to not look too heavy-handed yet instill confidence of the protected personnel and assets. Society is experiencing extreme aggression and destruction of property in our diverging and extended global societies.

Summary

Team IMMERSIVE's ® perimeter security solution is based upon developing our unique "system of systems" approach. This neural network problematic-based asymmetrical proactive architecture will and must be centered and yet expanded from current Human in the Loop security threat models. The neural network combined with trained watch keepers can deliver a level of asset and destruction reduction needed in support of a rapid threat expansion exploiting the technology curve now descending upon us as a global community. [6]

Contact us for further information on our IMMERSIVE® systems-based Neural Perimeter Security Network℠ design and integration services.

Office: 719.331.8930
Email: PMorgan@FSPScorp.com
http://www.FSPScorp.com/

[6] Credit: Michael Coole PhD Thesis
May 2015 Curtin University