Cyber is a **data problem**

Agencies can outsmart cyberthreats with the help of machine intelligence

Barry Leffew
Senior Vice President and General Manager of National Security Software, SAP National Security Services Inc.

IT'S IMPORTANT TO understand that cybersecurity is actually a data problem. Data and endpoints across every organization are expanding at an exponential rate. Traditional approaches that rely on known threats fail to keep pace. By leveraging artificial intelligence to monitor in-memory behavior, agencies can identify and neutralize ever-changing threats in real time — before their systems are compromised.

Cyberthreats continue to grow and evolve at lightning speed. State-sponsored organizations are staging highly complex, well-funded attacks, and they are expected to have a worldwide economic impact of $8 trillion by 2022. Attacks on power grids have plunged hundreds of thousands of people into darkness. Cryptocurrency and U.S. financial systems are constantly targeted for exploitation. With the volume of data and endpoints growing faster than ever before, all levels of society and defense are vulnerable.

Cyber battles will be won on artificial turf

Guarding the cyber perimeter is no longer enough. Organizations must counter with a new, stronger approach. The counter to these threats involves the combined power of a human/machine team. Human intelligence assisted by AI to outpace and out-think our enemies is fast becoming the new conventional battlefield — one that's both physical and virtual.

As cyber capabilities become more pervasive and disruptive, they shift long-standing notions of national defense and force projection. We now live in an era of algorithmic warfare, where AI and machine learning must augment human capabilities. Detecting threats through traditional methods is no longer sufficient. We must evaluate and analyze massive amounts of data, make predictive assessments and deliver actionable intelligence — at scale — far faster than ever before.

This is where AI and machine learning will play a crucial role by giving us an edge against our adversaries. By applying machine-learning principles to cyber data, we can go beyond both current and legacy approaches and add behavior-based capabilities to our cyber defense arsenal. Behavior-based detection observes devices through the data they're producing and processing to detect anomalies in behavior, identifying threats before they can cripple a network, steal data or wage an attack. The technique is used to isolate new vulnerabilities created by outside entities, as well as threats coming from inside an organization.

deepOV/RedlineVector/Shutterstock/GCN Staff

Humans cannot possibly monitor, manage and analyze the volume of data quickly enough; they **must be supported by machine learning**.

Maintaining our competitive and strategic edge

In this way, machine learning enables organizations to shift from reactive to proactive cybersecurity with automated, continuously evolving cyber detection and response. Humans cannot possibly monitor, manage and analyze the volume of data quickly enough; they must be supported by machine learning. And because the cyberthreats never cease, it's critical to develop a continuous risk and evaluation model that captures data, predicts outcomes and remediates threats.

Armed with multiple motives and an increasingly sophisticated set of tools, state-sponsored bad actors will continue to be a serious and viable threat to our national security. Our competitive and strategic edge as both an economy and a nation are driven by our advancing technological lead. Public awareness, improved collaboration and better use of our bedrock technical capacity will sustain an edge over our competition and adversaries to win on today's and tomorrow's virtual and physical battlefields. ■

Barry Leffew *is senior vice president and general manager of national security software at SAP National Security Services Inc.*

Today's explosion of data and endpoints are growing at an exponential rate. Traditional approaches, relying on known threats, fail to keep pace.

Leveraging AI to monitor in-memory behavior can identify and neutralize evolving threats in real time, before you're compromised.

For more information on how SAP NS2 is solving this complex problem, visit **carahsoft.com/IIG-Emerging-Cyber/SAPNS2**

At SAP NS2®, we leverage the most advanced commercial technology from SAP. We're focused on data intelligence, advanced analytics, machine learning and cyber—to help you protect the lives, assets and information of American citizens.

NS2 Solutions | NS2 Cloud | Secure Services | Secure Support

Contact us to get started, today: info@sapns2.com

Independent, U.S. Subsidiary of SAP