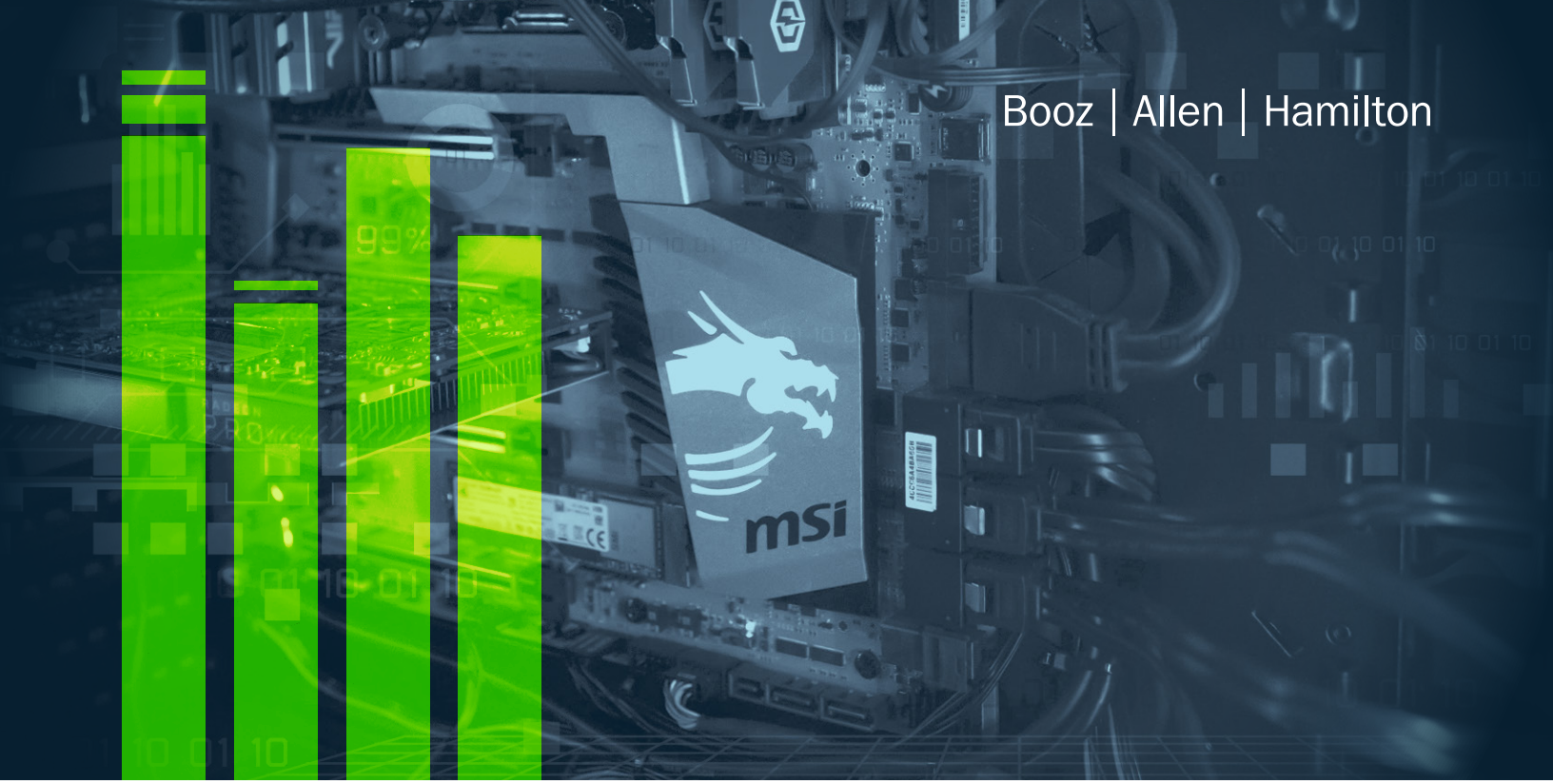
Booz | Allen | Hamilton

2021 TECHNOLOGY SPOTLIGHT

Cyber and AI

CONSULTING | ANALYTICS | DIGITAL SOLUTIONS | ENGINEERING | CYBER



The application of artificial intelligence (AI) to cybersecurity has reached an inflection point. With rapidly improving AI and machine learning (ML), cyber AI can now substantially enhance an organization's defensive posture by augmenting human-driven activities.

Historically, cybersecurity has been a field dominated by resource-intensive, monotonous efforts. Monitoring, threat hunting, incident response, and other cybersecurity efforts are often manual and time-intensive, which can delay remediation activities, increase exposure, and heighten vulnerability to cyber adversaries.

But today, the application of AI in the cyber domain has been shown to transform workflows into more efficient, autonomous, continuous processes that better defend organizations against cyber adversaries and maximize protection. With increased technological advancement over the past five years, AI solutions have matured to the point where they can offer tangible impact to cyber defensive operations across a wide range of organizations and missions. By bringing AI to the cyber mission, along with mature software engineering practices and ever-growing cyber tradecraft, government and business leaders can deliver critical mission success in their efforts to secure the digital future.

WHAT IS THE ROLE OF AI IN THE CYBER ECOSYSTEM?

The cybersecurity technology ecosystem supports efforts related to the protection and securing of people, systems, and organizations from cyber threats. This entails threat detection and mitigation or response activities by a team of specialized cybersecurity experts that work to minimize and prevent malicious attacks. Artificial intelligence is the application of statistical learning systems, or intelligent software and machines, to achieve a desired and defined goal. In cybersecurity's case, AI can be applied across each phase of the cyber lifecycle: monitoring, detection, threat hunting, and response. AI can be used to monitor cyber events across vast swaths of data to detect nuanced adversarial attacks, enhance data-driven decision-making during threat hunts, uncover previously undetectable tampering in operational technology (OT) devices, and quantify the risk associated with current vulnerabilities on IT systems. The role of AI in the cybersecurity ecosystem is only increasing as it continually improves and enhances cyber operations as a force multiplier for seasoned professionals.

A CLOSER LOOK: CYBERSECURITY & AI PROCESSES

Any technology ecosystem can be broken down into a set of core components or core processes. Over time, capabilities and offerings sprout up around these core components or processes as they mature. To fully understand a technology, it is often easier to analyze the individual pieces. We identify the following three (3) core processes in the application of AI to a cybersecurity setting:

Component Processes	Desired Outcomes	Purpose
Attack Detection	The use of AI/ML for advanced detection, through pattern recognition, characterization of threats, and early identification	AI/ML applications in advanced detection are proliferating, as improvements in capabilities lead to a reduction in the number of false positives. As more and more cyber professionals are deploying AI/ML solutions across large organizations, leaders should ensure that AI explainability, interpretability, and transparency are core to cyber-related product and service offerings.
Behavior Analysis	The use of AI/ML to quantify previous, current, and expected behaviors, so that suspicious activity is quickly detected and never-seen-before attacks are uncovered	Using AI to continuously monitor behaviors allows organizations to detect suspicious actions and deviations from controlled and expected activities. Applying AI/ML to learn behaviors for IT or OT devices can help defenders rapidly quantify policy or activity violations, while allowing teams to detect new attacks and threats based on behavioral profiles that may not have defined signatures for detection yet.
Risk Assessment	The use of AI/ML to quantify cyber risks associated with vulnerability and threats	AI can effectively quantify the likelihood of exploits, the impact of exploits, and the potential risks to an organization that are caused by active threats to their systems. This allows decision-makers to make data-driven decisions on patch prioritization, remediation activities, and mitigation actions to maximize efficient reduction of quantified risk.

BENEFITS OF INTEGRATING AI INTO CYBERSECURITY

There are several immediate and long-term benefits of integrating AI into an organization's cybersecurity ecosystem:

Improved cybersecurity effectiveness due to AI's ability to detect nuanced attacks, heighten security, and enhance incident response

Increased time savings as AI expedites the detection and response cycle time, rapidly quantifying risks and accelerating analyst decision-making with data-driven mitigation measures

Increased cost savings for organizations due to enhanced up-front protection as well as improved response, preventing and mitigating cybersecurity breaches and malicious attacks

Improved workforce experience, as cybersecurity professionals can focus on higher-level tasks as opposed to time-consuming, manual actions

Improved customer satisfaction and brand reputation due to heightened cybersecurity protection and increased trust in the organization's security protocols

EMERGING TRENDS IN CYBER & AI

Explainable Cyber AI: As AI/ML's applications to adversarial attack detection are proliferating, the need for Explainable Artificial Intelligence (XAI) is growing. Explainable AI provides insight into the "black box" of AI while maximizing the benefits of using AI tools to support cyber defense. With XAI, Security Operations Centers (SOCs) have insights into the "why" behind their software, allowing for continuous improvement of the cybersecurity lifecycle.

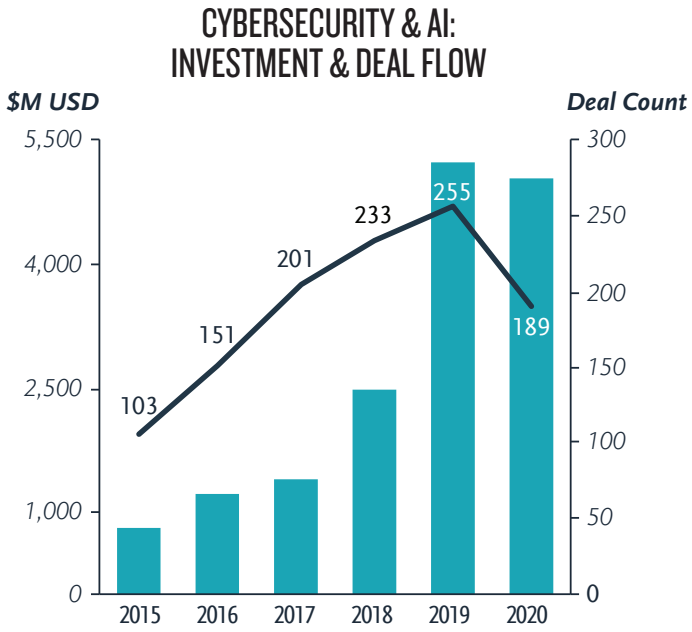
Cyber AI for IoT/OT Security: Behavior analysis use cases for AI are growing in Internet of Things (IoT)/OT environments, particularly at the device security and network security levels. Applying AI/ML to learn behaviors of simple OT devices can help teams more rapidly detect suspicious activities and threats.

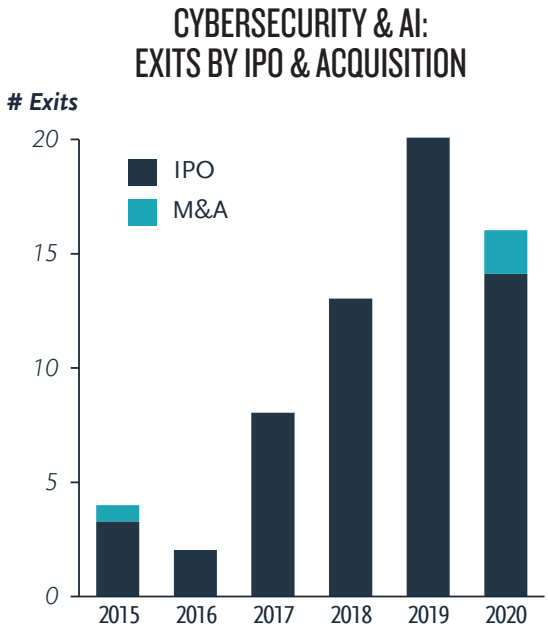
Neuromorphic Computing: This new approach to information processing for AI mimics the neural structure of the human brain. Neuromorphic computing has the potential to enhance AI's role in cybersecurity, producing faster and more accurate results. Companies like Airbus are partnering with academic institutions like Cardiff University to develop better malware detection built on emerging neuromorphic computing chipsets.

A LOOK AT THE CYBER & AI MARKET

Given the benefits of augmenting cybersecurity with AI, the cyber & AI market has seen continued growth over recent years and a significant increase in both deal count and venture capital (VC) investments. During the past two years, nearly $10B has been invested across over 400 deals. Investment more than tripled from 2017 to 2019 and deal count increased as well, reflecting continued growth in the cyber & AI market. Companies such as DarkTrace and SentinelOne utilize AI/ML to augment threat detection and response and provide autonomous endpoint security, respectively, and have each raised over $330M, highlighting the growing relevance of their offerings.

Initial Public Offerings (IPOs) have increased considerably as well in recent years, as startups in this space mature their offerings and look to expand and grow and require more access to capital. A rise in IPOs in this space also reflects a strong demand signal for cyber & AI offerings, as IPOs typically signify substantial year over year revenue generation. Given the dip in funding in 2020, due in large part to COVID-19, there may be a proliferation of acquihire and acquisition opportunities in the AI cybersecurity space in the coming months given decreased funding availability. Charts 1 and 2 provide more insights below.





Charts 1 and 2: *Cyber & AI Market by Investment and Deal Flow and Exits.*
Source: Pitchbook and Booz Allen analysis 2020 decline due to impact from COVID-19 and incomplete year of data

FIVE TAKEAWAYS FOR FIVE AUDIENCES

Booz Allen's tech scouting team monitors fast-moving emerging technologies and surfaces and shares insights from our industry assessments to help build technology acumen for our partners and the general public, and account for the different ways in which people relate to and understand technology.

Takeaways by persona are summarized below:

	STUDENT	FEDERAL LEADER	BUSINESS LEADER	TECHNOLOGIST	INVESTOR
Educational Recommendations	When learning about AI concepts and various use cases, consider cybersecurity applications	Learn about the breadth of AI use-cases for cybersecurity and potential applications to federal missions	Learn more about how AI's role in cybersecurity enhances business value and how to integrate AI into your organization's cybersecurity efforts	Cybersecurity will rely on AI technologies for better results. Learn about ways that your skills in AI can be applied to cybersecurity	Learn about AI's growing role in cybersecurity and encourage AI startups to pivot toward cybersecurity offerings when appropriate
Technology Relevance	AI's increasing role in supporting cybersecurity will broaden the market demand for skilled machine learning professionals with cyber backgrounds	Many DoD and government environments require the highest level of cybersecurity protection – AI can enhance those efforts	Expect a shift from competitors, and a request from customers, related to using AI to improve cybersecurity efforts	Stay abreast of other emerging trends within the cybersecurity and AI overlap, such as neuromorphic computing	Deals in cybersecurity and AI have more than doubled in the past four years, worth over $1.5B in 2019, and the market is expected to continue growing
Upcoming Disruptions	Organizations will hire AI experts for their experience applying AI/ML technology to cybersecurity instead of just looking for traditional cyber skillsets	As AI grows more prevalent it will be easier to augment human capability in government/ DoD cybersecurity roles, expanding impact and efficiency	Work with your cybersecurity teams to find ways they can augment their jobs and workflows with AI to stay ahead of competitors and produce better results	If you don't currently work in fields related to AI, find ways to obtain trainings and certifications related to AI to enhance your cybersecurity career	AI will continue to disrupt and expand the cybersecurity market as the technology "learns" (improves over time) and reduces human error
Suggested Next Steps	With the trajectory set by AI's role in enhancing cybersecurity, you can expect to be augmenting cyber skills with AI. Find ways to do this early and often to stay ahead	Cybersecurity is a massive need within the federal government. Find ways to integrate AI into cybersecurity tactics for enhanced protection	AI will minimize human error related to cybersecurity efforts. Integrate AI tools into cybersecurity teams early on	Identify ways (such as AI detection, behavior analysis, and risk assessment) to enhance cyber efforts when possible. Focus on efforts that require human involvement	AI's ability to support cybersecurity will only grow with time. Investments in AI companies supporting cybersecurity efforts should see large returns
Short Term Recommendations	Pursue an internship or job in AI to gain marketable, relevant skills with a focus on cybersecurity applications	Look for a trusted partner that is experienced in federal and DoD technology that can implement leading AI technologies to enhance cybersecurity	Collaborate with companies tracking the growing role of AI in the cybersecurity ecosystem to find new use-cases to protect your business and new potential product and service offerings	AI is improving and enhancing cybersecurity operations across industries. Seek out employers working on meaningful problems in this emerging space to apply your skills in world shaping ways	Collaborate with firms working in spaces where cybersecurity is lagging, as these groups will have a heightened need for emerging AI solutions to enhance security measures

About Emerging Technologies at Booz Allen

For over a century, Booz Allen has been at the forefront of technology and strategy. We provide strategic advisory services, design, build, and deploy solutions across sectors to a wide range of federal government organizations. We are the only management and technology consulting firm that has invested to establish an innovation network exclusively focused on scouting dual-use technologies for federal government missions. As a result, we successfully partner with the technology community to showcase a wide range of capabilities and deliver innovative solutions to our clients.

Our deep pool of technical talent, access to critical networks in innovation hubs, and experience performing technology scouting across technologies and sectors uniquely position Booz Allen to serve clients who seek to be at the cutting edge.

To learn more, visit BoozAllen.com (NYSE: BAH)