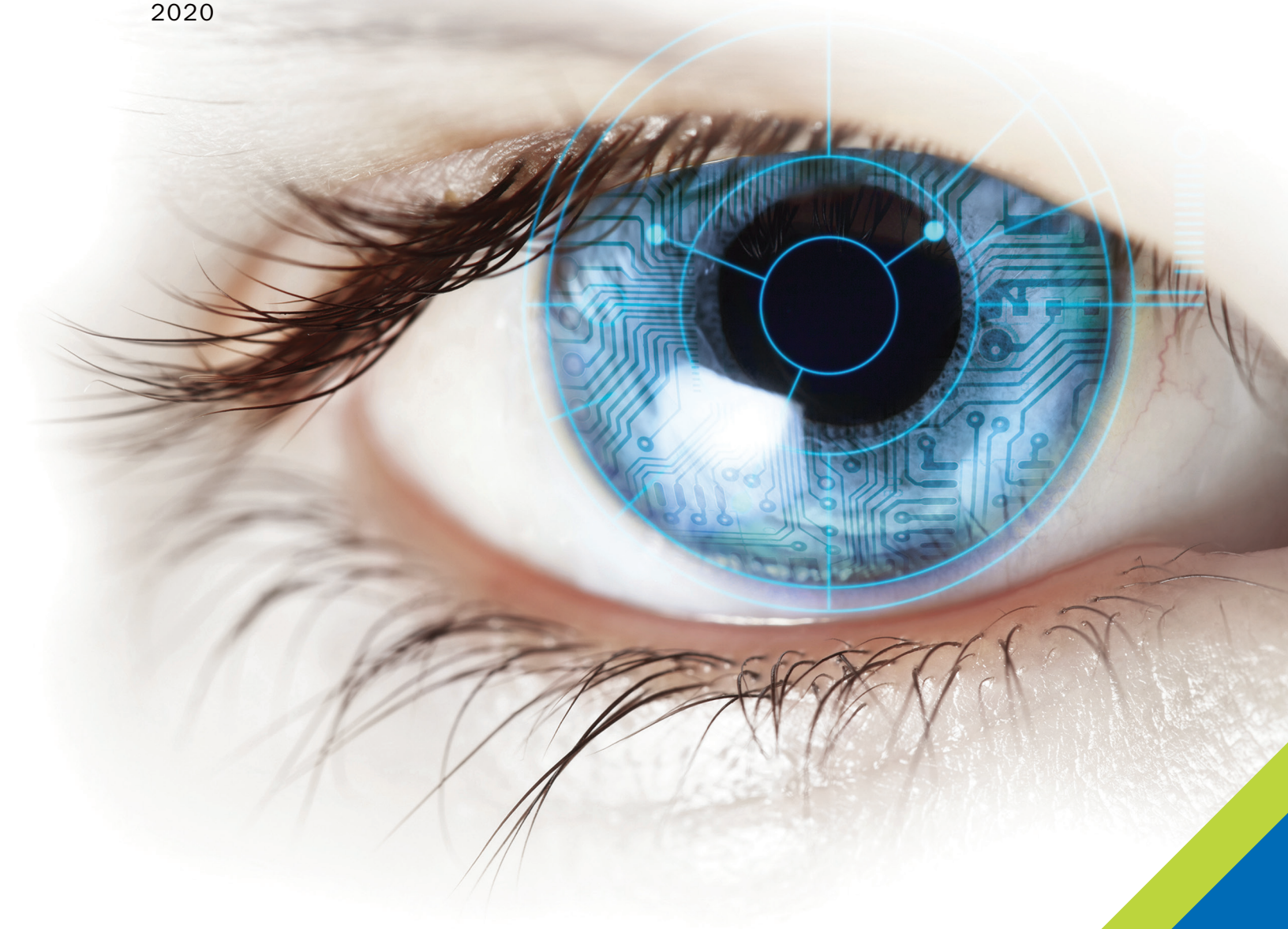
—ADVANCE TODAY

INTELLIGENCE COMMUNITY TRENDS

2020



SAIC®

IC TRENDS

As a service for our customers, SAIC offers a few insights from our thought leaders on trends and emerging technologies in the intelligence community.

Adapting at the speed of mission, requires a grasp of environment, domains, emerging technologies, and workforce talent. SAIC's leading experts weigh in on:

- Operating within the challenges of COVID (including cyber resilience)
- Leveraging commercial innovations and technologies
- Novel applications of artificial intelligence
- Enhancing decision making capability through workforce development and digital engineering

This discussion is presented at a high level. We invite you to contact our team if you have other topics of interest or would like more details regarding the following observations and considered solutions.

Want More?
Throughout this summary, we will offer hyperlinks to more detailed resources like blogs and features.

Where We Work: Does our IT environment meet the demands of pandemics, evolving threats, and emerging technologies?

COVID 19 has highlighted the need to consider new ways of working effectively, but also securely. Balancing health-related safety with secure missions has sparked a variety of approaches and new challenges. With the COVID 19 pandemic and the need to protect the workforce, working from unsecure locations, such as a personal residence, has raised new challenges and an unfamiliar work experience for many. SAIC's Information Technology (IT) experts and security specialists are teaming to address network demands, common access card solutions, computer certification, and a multitude of other innovative solutions and capabilities that may allow for safer and secure telecommuting.

While some trends may be temporary, others are laying the groundwork for a new future state. Technology like Commercial Solutions for Classified (CSfC) and Virtual Desktop Infrastructure (VDI) help with teleworking and enable work from lower-cost contractor facilities. From a software development and IT delivery perspective, the IC should consider accelerating efforts, as much development as possible, to move to the low side, where remote access is easier and more affordable, which helps in times of crisis and opens up the possibility to leverage a larger development talent pool, including innovators from commercial industry. By adopting DevSecOps, Infrastructure as Code, and Policy as Code, the need for developers, engineers, and administrators to interface directly with high-side production systems can be significantly reduced. DevSecOps methodologies, enabled by cloud native platforms, modern, loosely-coupled application architectures, and everything-as-code, enable rapid insertion of new services and updates to existing services in production safely and securely.

To this end, the IC is leveraging more commercial IT solutions and adding their "specific requirements" at the application layer thus reducing their time to market and overall sustainment cost. The historic classified working environment is maturing into a broader information sharing environment that incorporates a wide array of traditional and non-traditional sources. The intelligence workforce and operators need to function in a high velocity information sharing environment integrating all sources of information, including greater reliance on unclassified information, to enhance mission execution. Many aspects of the IC's work, from business functions to software development to cybersecurity, require access to unclassified systems. IC customers are looking to deliver unclassified work environments that fully enable their workforce to better perform critical functions. Challenges like network security, collaboration, and supply chain control are informing SAIC in its internal research and development spending. SAIC technologists are currently deploying cloud-based security, analytic platforms, and collaboration tools from our various services and products as well as block chaining technology in an innovated way to ensure software development outside of a secured environment is not changed or tampered with. SAIC believes these technologies have direct application to the IC and the IC's customers' operational requirements.

Innovative GEOINT Application Provider Program at the National Geospatial-Intelligence Agency is a good example. Investments in cloud-based operations, a unique acquisition model that leverages commercial developers, and distribution of solutions through a mobile app store are all well suited to serve geographically distributed intelligence officers and warfighters.

The IC's relationship with technology market leaders like SAIC, emerging technology companies, and universities are instrumental in creating an ecosystem for accelerating the development of analytic frameworks and intelligent software architectures, compressing timelines from rapid prototyping to solution readiness, and igniting technological and business transformation.

– Kuan Collins, master solutions architect, software, at SAIC.

Learn more about SAIC investments in DevSecOps and emerging technology through its Innovation Factory.

Read more on intelligent software.

Read how SAIC is partnering with the Air Force on Cloud One – Learn more about our cloud strategy.

Read more on how the NGA is adapting to circumstances.

IC TRENDS

Read more on how modern cyberattacks require a zero trust model.

THE ROLE OF CYBER

The IC is designing a multi-zone defense in which they are leveraging the strength and policies of each agency to close the gaps in attempting to solve the cyber problem. They are using advanced technologies based on data analytics, machine learning, and artificial intelligence (DA/ML/AI) to response at the speed of the network and lessen human interface, which means policies and laws are baked into the technology solution.

Software defined networking (SDN) will make networks more flexible and resilient, and it will also enable adoption of true zero-trust networking models at-scale.

The increase in telework means that more data is crossing the open internet – with not only increased traffic but increased threat activity. The US Defense Department recognized the need to "Defend Forward" in its latest strategic plan. Now even more federal organizations can't worry only about protecting activity inside their own perimeter. SAIC cyber specialists are currently exploring DNS and BGP– items previously just considered the internet "plumbing" to those not in open internet operations. By looking at global BGP routing data, SAIC has indeed seen a significant increase in routing changes since the start of COVID 19 outbreak.

SERVING IC SINCE
1971

MEMBER OF
INSA BOARD OF DIRECTORS

14,300
CLEARED PERSONNEL

SAIC'S IMPLEMENTATION OF IGAPP
"CREATES MAGIC."
VICE ADMIRAL SHARP

DATA ANALYTICS COHORT

GEORGE MASON UNIVERSITY PARTNERSHIP

- **9** DATA ANALYTICS ENGINEERING MASTERS DEGREES
- **11** DATA ANALYTICS GRADUATE CERTIFICATES
- **21** NEW STUDENTS KICKED OFF COHORT #4

How We Work: New and Novel Approaches to Data Analytics, Machine Learning, and Artificial Intelligence

SAIC has seen a new commitment in funds and mission needs based on DA/ML/AI demand. Senior leaders within the IC have placed a new emphasis on this technology, and they are developing much of their next generation of advanced analytics using ML/AI. While research divisions within the IC have been in this field for more than a decade, it has only been in the past several years that the operations and capabilities divisions have started to push this technology into the mission space.

Given the potential of DA/ML/AI for IC applications, SAIC has made significant investment in various problem sets and developing DA talent. By applying historical and doctrinal knowledge to create forecasting rules, we can help analysts predict enemy activities with more certainty. Predictive analysis with a structured object service equips customers with automated rule sets. Using a new open source intelligence tipper generator for the U.S. Army - the time needed to format intelligence reports decreased from 15-20 minutes to 2-3 minutes.

SAIC is also exploring the application of machine learning at the tactical edge. We now have an architecture where multiple IoT/commercial sensor streams are processed at the edge on lightweight/rugged form factor compute nodes. ML models, which are pre-trained, execute on remote platforms like people, unmanned aerial vehicles, ground vehicles, etc. Each model is optimized for the data stream (video, facial, biometric, cyber, etc.). At the command post or higher echelon, teams of data scientists do the back end training and optimization and then push optimized models back "out" to tactical edge.

Finally, for IC customers operating satellites, we are seeing great potential in ML applied to space operations like space traffic management and joint all domain command and control.

The Workforce

DA/ML/AI is only as good as the analysts applying it. Machines augment human analyst effectiveness. To this end, SAIC has partnered with George Mason University to create a Master's program in Data Analytics that is building data scientists. In fact, some customers have had the opportunity to send employees through the program as well.

By applying machine learning, the government will accelerate mission tasks, do what was previously unachievable, and improve security at relatively little cost.

– Bryn Stark, applied mathematician and lead data scientist in SAIC's AI lab

Read how SAIC data scientists apply machine learning to vital mission work.

Read how AI can assist in intelligence forensics.

Read more on AI and how it applies to space missions.

Read how SAIC funds a tailored, data analytics cohort program with George Mason University.

IC TRENDS

Digital engineering enables our customers to be more informed and move our nation's warfighters forward at the speed of relevance against fast-evolving threats.

– Ken Running, modeling and simulation expert

Read more on decision modeling and digital engineering.

Read how SAIC is making this possible for the U.S. Space Force.

Collaboration is important as mission needs become more and more nuanced. A primary force multiplier for the government is to develop an open source methodology. Building or acquiring open source platforms allows rapid deployment of new applications against government data stores. Industry is innovating and developing at an incredibly fast pace, and the IC has an opportunity to partner with industry to implement frameworks, platforms, and architectures that allow the Government to implement this innovation quickly.

The digital engineering discipline is placing extremely powerful decision making tools into the hands of the IC. The complexity of systems of systems engineering is brought under control for logical and effective mission execution. The modeling and simulation components are deployed with some of our customers, enabling runs of billions of scenarios for the best possible solution to highly complex problems.

Beyond enhancing worker effectiveness, technology can play a part in training more effectively. Organizations can leverage ML tools to:

- Capture and collect multiple formats of training data according to user-driven requirements and interface with and process digital data in virtually any format.
- Aggregate data from structured and unstructured training sources (systems, instrumentation, simulation, observers, etc.) and ensure data is aligned with defined training requirements and standards.
- Tag and curate data automatically to ease its organization, and perform automated information processes to identify linkages that are not readily visible to users.
- Enable relevant, accurate information to be viewed quickly through intuitive and organic search and retrieval functions.

We are also seeing IC customers apply virtual environments to training. For instance, a secure command center may not yet be built, but operators can don headsets and experience the environment before day 1, and they can do it while geographically dispersed.

Summary

Threats are constant and constantly changing. The IC will need to put architectures and solutions in place that outpace evolving adversaries. Innovation and adaptability underpin mission success. We hope some of the insights and resources outlined here help you advance, and maybe even leapfrog, your solutions. Please contact us if you'd like more information, or if you'd like to see how any of these ideas might be tailored to your unique challenges.

Contact
ic@saic.com

21-465