THE HUMAN FACTOR

ARTIFICIAL INTELLIGENCE VS HUMAN ANALYSIS FOR RISK ASSESSMENT AND MITIGATION

BY JOHN CAUTHEN | **MEDAIRE**

MedAire
An International SOS Company

Control Risks

THE CHANGING LANDSCAPE OF RISK AFTER MANCHESTER, BARCELONA & LAS VEGAS

In 2017, terror events shook the world as more and more cities once thought to be safe experienced mass casualty events no one had foreseen. Post-event implications resulted in governments and various organisations enacting contingency plans and emergency response protocols to react and respond to future incidents.

Beyond security incidents caused by humans, 2017 natural disasters like hurricanes, earthquakes and flooding destroyed infrastructures and shut down entire countries, creating a perilous environment and uncertainty for residents and visitors.

Social media sites are no longer simply venues for sharing family moments or photos of a meal at a new restaurant, they are often exploited to achieve nefarious ends. The world is connected like never before, and the formation of virtual groups provides validation and the encouragement to incite violence in any (and all ways) possible.

EUROPEAN COUNTRIES IMPACTED MOST BY TERRORISM

Global Terrorism Index Score

Turkey | 7.5	**Belgium** | 4.7
Ukraine | 6.6	**Greece** | 4.1
France | 5.9	**Sweden** | 3.8
UK | 5.1	**Ireland** | 3.1
Germany | 4.9	**Italy** | 2.8

CHALLENGES ORGANISATIONS HAVE ENSURING MOBILE WORKFORCE HEALTH & SECURITY

53%
Educating employees about travel risks

44%
Communicating with employees during a crisis

44%
Confirming employees have read pre-travel information

35%
Having resources to manage health & security efforts

39%
Tracking employee travel

According to author C.R. Sunstein, "If like-minded people stir one another to greater levels of anger, the consequences can be dangerous. Terrorism is, in large part, a problem of hearts and minds, and violent extremists are entirely aware of that fact. They use social media… to inspire 'lone wolves' to engage in murderous acts."[1]

Today's security environment is dynamic and complex, especially within the aviation industry, which demands high-fidelity situational awareness. In this environment, then, one must consider advanced preparation while simultaneously developing contingencies for unexpected events that threaten the people and assets crucial to the continuity of your business.

THE ADOPTION OF TECHNOLOGY TO AUTOMATE AND STREAMLINE ANALYSIS

Technology surrounds us and has undoubtedly improved the lives of millions of people. People can now access previously inaccessible information or shine a light on social issues and local events without having to wait for the media to take notice.

Organisations are capitalising on social media analytics. Firms use this information to predict and verify people's activity to find new business opportunities or to modify their business objectives.

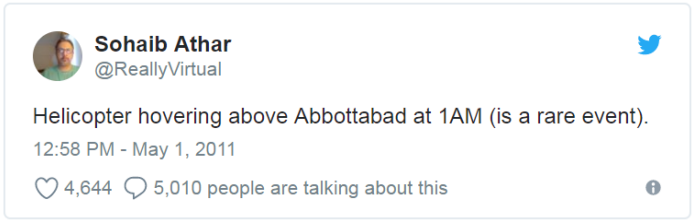
Similarly, security organisations are increasingly using social media data to validate reports and to prepare for or modify their travel advice recommendations for clients. Chatter on social media can often alert you to a situation well before the news media are reporting the story.

With all this data - 1.4B people log into Facebook every day, spending an average of 35 minutes on the site per day[3], and Twitter users tweet 21M times per hour.[4] – how can a human being keep up? They can't.

Instead, humans are increasingly relying on technology such as machine learning and algorithms designed to remove the clutter and identify the most credible data. Because humans develop the software and algorithms it necessarily follows that a human should validate and analyse the output of these sources to provide insight and understanding; a function technology cannot yet achieve.[5]

To develop a comprehensive picture of your travel-related risks your organisation needs to harness the power of both technology and the interpretive proficiency of experienced human analysts.

The interface between these two complementary systems – human and machine – to develop actionable information and derive knowledge from vast quantities of noise is critical for a proper understanding of the current and ever-shifting global security landscape.



The first known mention of the raid killing Osama Bin Laden in 2011 provided by a local man[2]

In fact, national level intelligence has embraced this approach, signalling that in isolation neither is adequate for the present and future security environment. In 2016, the U.S. National Geospatial-Intelligence Agency (NGA) in its 2020 Concept of Operations argued that the "future approach to [geospatial intelligence] GEOINT will grow with technology, supporting human insight with artificial intelligence and automation."[6] Have we already arrived at this symbiosis? Hardly, the human analyst remains paramount.

Realistically nothing can be done to accelerate this vision of the future. Machines and technology do not and cannot provide insight; this is a function still reserved for humans. Computers and artificial intelligence will be "servants" to human analysts, allowing people to "emphasize critical thinking, [develop] specific solutions, and [intervene] when real-world events are not modeled or anticipated." [7] This ideal pairing is still many years off, but it is the likely model for the future and will pay high dividends to intelligence and security practitioners.

HOW ARE ARTIFICIAL INTELLIGENCE & MACHINE LEARNING BEING USED TODAY?

Global artificial intelligence in the aviation market is expected to be valued at USD 152.4 Million in 2018 and is likely to reach USD 2,25 Billion by 2025, at a CAGR of 46.65% from 2018 to 2025.[8]

The primary factors driving the growth of the AI in aviation market include the use of big data in the aerospace industry, a significant increase in capital investments by aviation companies, and rising adoption of cloud-based applications and services in the aviation industry.[9]

With the rapid pace of progress and near science fiction level development of today's technology – inclusive of AI and machine learning – why is the inherently flawed human element still required for analysis? These seemingly routine tasks are undoubtedly suitable for automation.

According to authors of a recent report to the United States Congress, "This growth has advanced the state of Narrow AI, which refers to algorithms that address specific problem sets like game playing, image recognition, and self-driving vehicles."[10]

As prevalent and promising as AI and machine learning are in today's business lexicon, illustrated by recent headlines, even consumer-level technologies are not perfect. Would you trust the safety of your mission to a machine alone? In reality, these technologies are too immature and narrow in scope and reach to supplant human judgement.[11]

SCIENTIFIC AMERICAN | April 13, 2018

CAN AI REALLY SOLVE FACEBOOK'S PROBLEMS? | READ ▶

CNN | March 8, 2018

AMAZON'S ALEXA IS LAUGHING AT USERS AND CREEPING THEM OUT | READ ▶

USA TODAY | March 26, 2018

ARIZONA HALTS UBER SELF-DRIVING CAR TESTS AFTER FATAL CRASH | READ ▶

FORTUNE | December 27, 2017

HOW GOOGLE AI WAS TRICKED INTO THINKING THIS PHOTO OF MACHINE GUNS WAS A HELICOPTER | READ ▶

FORTUNE | May 7, 2017

ARTIFICIAL INTELLIGENCE FAILS ON KENTUCKY DERBY PREDICTIONS | READ ▶

BEST PRACTICES FOR RISK MITIGATION REQUIRE HUMANS TO INTERPRET DATA

Relying on the promise of machine learning and AI have significant limitations. "[A]ll of the AI technologies invented thus far – or are likely to appear in the foreseeable future – are forms of narrow AI," which means their algorithms are narrow in scope and cannot be applied to other applications.[12] In short, they do one thing well. Activities such as "characterising patterns of activity, modelling knowledge, anticipating outcomes, developing insight, creating sourcing opportunities, and identifying gaps," may be difficult or impossible to automate with current AI and machine learning.[13]People are still critical and cannot yet be removed from the "loop," if ever.[14]

"There are risks associated with reporting on threats that have not been confirmed, assessed and put into context. Releasing alerts without proper human analysis can lead an organisation to wrong conclusions which can jeopardise successful business operations."

JASON NYGREN | **GLOBAL SECURITY MANAGER**
MEDAIRE

The ability to scan and sort the massive quantities of noise generated on a daily basis and then to confidently analyse, assess, and advise a client is the mark of a mature and professional security operation. These practices are being executed today, but only by organisations willing and able to invest in the right human capital, while simultaneously monitoring the technological ecosystem for tools appropriate to augment those very same people. The exact nature of the intelligence and security relationship is still very much dominated by the human analyst with tailored assistance provided by machines.

Information in and of itself is only part of the security equation; we should be wary of conflating the abundance of noise with useful information, knowledge, and insight. The other and most critical half of this equation is how one's organisation should apply all of this to their business interests. With a robust team of security analysts, information is transformed into knowledge, packaged, and transmitted as insight to interested parties. Organisations must ensure proper strategies are developed to contend with and mitigate the uncertainties of dynamic security situations, all of which could have enormous implications for any number of global business operations and continuity.

Experienced and highly trained teams of human analysts are not only more agile than today's machines, but these people-based organisations can assess complex information to derive actionable advice that AI is too one dimensional to match. As a recent Deloitte paper asserts, "Algorithms can augment human judgment but not replace it altogether; at the same time, training people to be better forecasters and pooling the judgments and fragments of partial information of smartly assembled teams of experts can yield still-better accuracy."[15]

"AI systems also fail in unexpected ways, with some analysts characterizing the technology as "brittle and inflexible." Dr. Arati Prabhakar, the former DARPA Director, commented, "When we look at what's happening with AI, we see something that is very powerful, but we also see a technology that is still quite fundamentally limited ... the problem is that when it's wrong, it's wrong in ways that no human would ever be wrong."[16]

The fundamental limitation with today's AI is embedded within the models and the narrow scope in which AI can and is deployed.[17] It must be remembered that humans still create AI and the models under which they operate, and these are necessarily narrow in focus and prone to bias, usually capable of analysing significant volumes of data, historical or otherwise, but they may also yield nothing of value from a forecasting standpoint. Human analysts are, of course, prone to the same narrow focus and bias, but through rigorous selection and training, recent research has indicated these traits can be minimised.[18] And humans are still the only ones capable of making judgements and creating useful insight from the vast repositories of data that ultimately become information.

Most have heard the phrase in one form or another that correlation is not necessarily causation. Analyzing reams of data can produce attention-grabbing associations, and, under the right circumstances, valuable insight, but it may indeed also result in erroneous assumptions, meaning, and significance. As a recent McKinsey paper suggests, "Sometimes lost in the hype surrounding machine learning is the fact that artificial intelligence is as prone to bias as the real thing it emulates…We cannot afford to believe in the myth of machine-perfected intelligence. Genuine limitations to machine learning must constantly be addressed by humans."[19]

"Dawn Meyerriecks, Deputy Director for Science and Technology at the CIA, expressed concerns about convincing national decisionmakers to trust AI judgments, arguing, 'Until AI can show me its homework, it's not a decision quality product.'"[20]

MILITARY MISSLE TESTING

SHOULD YOU BE ON ALERT?

MedAire Security receives intel from a number of sources which stream in every minute of every day. Analysts use risk thresholds and other tools to help sift through the data and to catalogue events that may indicate a credible security threat. An internal alert calls for further analysis of the data when that threshold is met.

Military agencies around the world participate in drills and exercises throughout the year. Sometimes these exercises are used as cover for an actual military strike which could pose a threat to civil aviation. To know if there is a real threat, one would have to take into account the group engaging in misdirection. If there is a history of this practice or a diplomatic reason it is probable, the threat is more than likely an interloper covering strikes, for example, in Syria. There would be no need for an antagonist to cover these activities since the military operations in that region are widely known. Reacting to a threat, in this case, would be sensational.

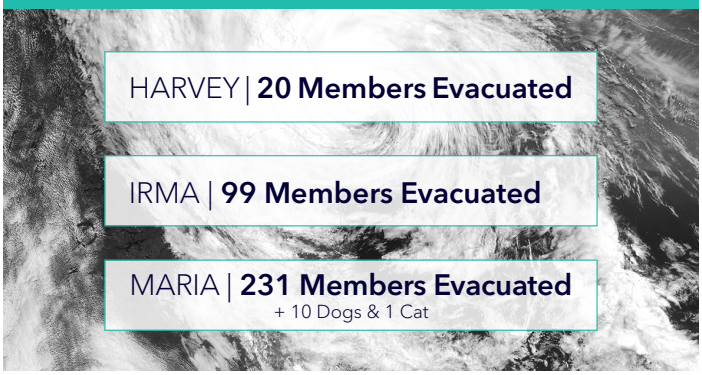
MedAire's approach is to cut through any implicit bias and exaggeration, avoiding unsubstantiated speculation to provide the most relevant and valuable information available.

THE VALUE OF REGIONALISED EXPERTISE

The value of human analysis can be further demonstrated by having vetted local resources to provide intel from within a region. These assets provide better data because of their intimate understanding of language, culture, risks and the associated threats. They will also be your best resource to assist if you have travellers in the region at the time of a significant security incident.

Humans must again intercede to take what a machine can filter and collect to analyse, create useful information from the noise and then render a careful assessment that provides insight. "[T]he lesson," the Deloitte authors write, "is that generally speaking, big data and machine learning algorithms should be regarded as supplements to – not replacements for – human judgment and traditional forms of analysis."[21] Machines and the technology behind AI are impressive and will undoubtedly continue to improve, but there is little dispute that they can replace the "characteristically human ability to make judgments under uncertainty."[22] Insight is a fundamental human skill not yet mastered by machines.

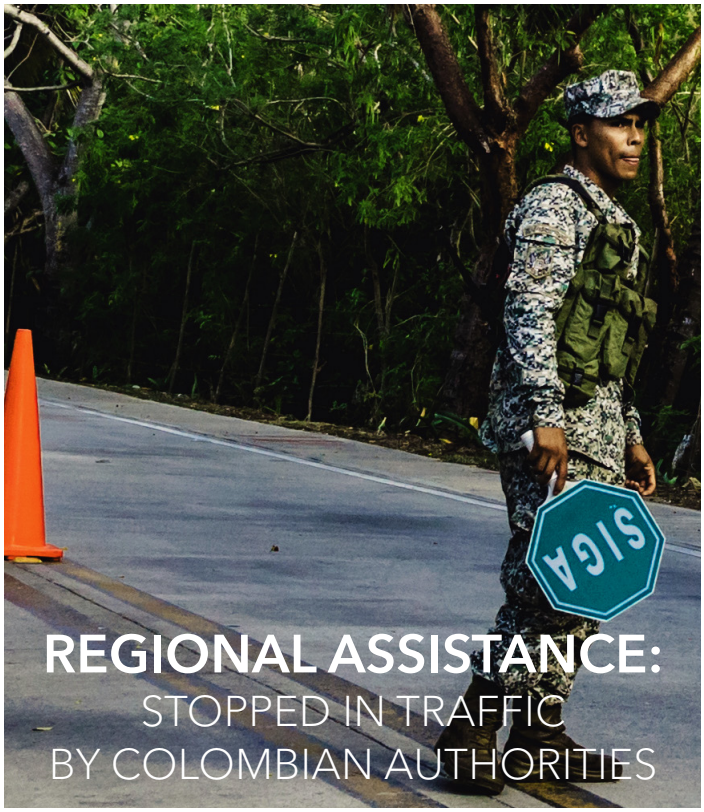
WHEN HURRICANES DEVASTATED NORTH AMERICA, MEDAIRE SECURITY ASSISTED MEMBERS GETTING THEM HOME SAFETY.



Mature organisations excel by "tapping into the wisdom" of experienced teams using honed processes. Human analysts work in conjunction with various programs to scan vast amounts of noise, aggregating the relevant data, analysing it systematically, and then advising its stakeholders in a way a less robust security operation would not be able to match. Excelling by "tapping into the 'wisdom' of well-structured teams can result in improved judgments and forecasts," and this is how harnessing current technology and pairing it with humans results in consistently superior outcomes.[23] But this is not accomplished by using AI as it is commonly understood, a process of automation to supplant human capabilities that is many years off. Instead, we must deploy available technologies and pair it with experienced teams of human analysts to provide pertinent insight that machines are ill-suited to replicate.

You can prepare for a large number of contingencies or avoid locations during your mission. Unexpected security incidents like civil unrest, terrorism and natural disasters still happen during your mission; it is important to partner with a team that can quickly mobilise to assist you when needed.

MATT BRADLEY | **REGIONAL SECURITY DIRECTOR**
INTERNATIONAL SOS



REGIONAL ASSISTANCE:
STOPPED IN TRAFFIC BY COLOMBIAN AUTHORITIES

While travelling in Cartagena, Colombian law enforcement officials stopped a member for DUI. Police corruption is relatively common in local districts, and the police will target foreign travellers.

MedAire Security Assistance has an extensive network of security personnel around the world. The supervisor asked for the Officer's credentials to escalate the incident to contacts with the Colombian Ministry of Interior and the United States Embassy.

These actions resulted in an immediate apology from the arresting officer and the member was released, allowing them to complete their trip without further incident.

MedAire Security Specialists used their global network of relationships to diffuse the situation before it ended with the member paying a bribe or spending time in jail.

The stress of this event prompted MedAire to offer the member and their family Emotional Support Services to help process their emotions following the incident.

SUMMARY OF ADVICE

Analysing security threats is a complex and variable process. **The best-prepared flight departments will use a hybrid system of computer-guided and human-reviewed intel.** Exploiting the benefits of both technology and human analysts is essential. There is no one single source for assessing security threats; it will always take multiple data points from a myriad of sources to put together an accurate picture of vulnerabilities, risks and threats.

As technology advances and the types of data we can analyse changes, our processes need to adapt to evaluate new sources. **Build a solution for security risk mitigation using the best of computer-assisted guidance and human oversight to prepare for many possible outcomes.** While you cannot avoid all risks, you need to be able to set thresholds which allow you to execute against the goals of your business. Some regions cannot be avoided, but mitigation will prescribe how to engage when operating in and around those regions.

It is more important to prepare beyond avoiding risk by incorporating regionalised human resources. Having location-based support on call and available to assist when the unexpected happens closes the loop on your security event mitigation. Invest in a solution that will support your operations until your resources are safe at home, rather than only planning around a perceived threat.

The joint venture between MedAire, International SOS and Control Risks combines the world's leading medical and security risk specialists. These resources and expertise provide a comprehensive suite of travel risk services for mobile workers. MedAire offers unique and unrivalled access to 2,300 security experts, a multicultural team speaking more than 60 languages, providing timely, actionable security intelligence, advice and on-the-ground assistance.

Contact MedAire for a complimentary analysis of your current security protocols and resources. Together we can identify the best tools and resources for your organisation.

AMERICAS: INFO@MEDAIRE.COM
EUROPE: INFO-EU@MEDAIRE.COM
ASIA, PACIFIC, MIDDLE EAST & AFRICA:
INFO-APMEA@MEDAIRE.COM

CONTRIBUTORS

JOHN CAUTHEN
DIRECTOR OF SECURITY, MEDAIRE | AUTHOR

John joined MedAire in 2018 as the Security Director, Aviation and Maritime. Previously, he managed law enforcement flight operations in Arizona for the City of Mesa Police Department. John also spent 11 years as an active duty naval aviator flying helicopters and serving on various military staffs, to include time with NATO and the U.S. Coast Guard. He remains in the Navy Reserve where he flies helicopters with a squadron in San Diego, California.

JASON NYGREN
GLOBAL SECURITY MANAGER, MEDAIRE

Jason joined MedAire in 2013 after working for the Defense Intelligence Agency (DIA) as an intelligence officer for technical collection supporting counter-terrorism operations in Iraq, Afghanistan, and Africa. Before that, Jason spent 9 years in the US Air Force as a non-commissioned officer working on special operations and airborne intelligence collection platforms in Europe and the Middle East.

MATTHEW BRADLEY
REGIONAL SECURITY DIRECTOR, INTERNATIONAL SOS

Matthew joined International SOS as Regional Security Director, Americas in October 2014. Prior to joining ISOS, he was the Security Director for the largest mobile service provider in Honduras. Matthew spent 14 years with the CIA with overseas postings in Chile, and Argentina.

SOURCES

1 Sunstein, C. R. (2018). #Republic: Divided Democracy in the Age of Social Media. Princeton, NJ: Princeton University Press, 9.

2 @ReallyVirtual, Twitter, May 1, 2011.

3 FACEBOOK

4 TWITTER

5 Castellanos, Sara and Steve Norton, "Inside Darpa's Push to Make Artificial Intelligence Explain Itself," The Wall Street Journal, August 10, 2017, https://blogs.wsj.com/cio/2017/08/10/inside-darpas-push-to-make-artificial-intelligence-explain-itself/

6 United States National Geospatial-Intelligence Agency, NGA GEOINT CONOPS 2022, 2016, 2.

7 Ibid.

8 Artificial Intelligence (ai) In Aviation Market Expected ... (n.d.). Retrieved from https://www.prnewswire.com/news-releases/global-22-bn-artificial-intelligence-in-aviation-market-2018-2025-market-to-grow-at-a-cagr-of-4665-300618741.html

9 Artificial Intelligence (ai) In Aviation Market Expected.

10 Hoadley, Daniel S., and Lucas, Nathan J. Artificial Intelligence and National Security. Congressional Research Service, 2018, 2.

11 Guszcza, J. and Maddirala, N. (2016). Minds and machines: The art of forecasting in the age of artificial intelligence. Deloitte Review, Issue 19. 12-20.

12 Guszcza and Maddirala, 15.

13 United States National Geospatial-Intelligence Agency, 4-5 & Hoadley and Lucas, 2. "Experts generally agree that it will be many decades before the field advances to a state of General AI, which refers to systems capable of human level intelligence across a broad range of tasks."

14 Guszcza and Maddirala, 15.

15 Ibid, 10.

16 Hoadley and Lucas, 28-29.

17 Guszcza and Maddirala, 13-18 and Tobias Baer and Vishnu Kamalnuth, "Controlling Machine-Learning Algorithms and their Biases," McKinsey & Company, 2017, 3.

18 United States Geospatial-Intelligence Agency and Guszcza and Maddirala. 16.

19 Baer and Kamalnuth, 7.

20 Hoadley and Lucas, 31.

21 Guszcza and Maddirala, 16.

22 Ibid, 18.

23 Ibid, 19.