ASIS QATAR NEWSLETTER

ISSUE 02 | APR 2025

TECHNICAL CORNER

A closer look at the impact of AI in the field of OSINT

INTERVIEW

A discussion with Jacobus Wepener, Director of Security at HMC

SPOTLIGHT:

2ND QATAR SECURITY PROFESSIONALS MEETUP

ASIS INTERNATIONAL™ QATAR CHAPTER

TABLE OF CONTENTS

FROM THE EDITOR'S DESK

PALLAVI BICHU

Dear readers,

What a great start to the year we've had! The grand success of the second edition of our Security Professionals Meetup in January was certainly the highlight of the first quarter. Our members also attended Intersec 2025 in Dubai, UAE, exploring opportunities for collaboration. ASIS Qatar was also proud to host the first edition of our Security Speaker Series, with an insightful discussion on aviation security by Mr. Prabhu Jawahar of Qatar Airways. In February, chapter officers also attended the US OSAC security briefing, gaining valuable insights into the regional geopolitical situation and associated risks. During the Holy Month of Ramadan, we had the International Women's Day event, where fantastic speakers and women in security met for an empowering day of knowledge sharing and collaboration, as well as the annual Iftar distribution event, always a great success.

Just like last time, this edition too is packed with insightful articles, interviews, and information to make the most of your ASIS membership. We have technical pieces on the impact of AI on the security industry, which are sure to be illuminating for our readers. Our team also conducted an interview with the Head of Security at Hamad Medical Corporation, Mr. Jacobus Wepener, where he spoke about the state of security in the healthcare industry in Qatar.

As ASIS Qatar continues to scale new heights, we invite you to write in with your opinion pieces and ideas for events. We were heartened with the strong response to our last edition, and enjoyed reading your submissions. Keep them coming!

Signing off,

Pallavi Bichu,
Editor-in-Chief
Chapter Communications Chair

QUARTERLY UPDATES

IFTAR EVENT

On March 22, ASIS Qatar hosted a special Iftar at a labor camp in the Industrial Area, bringing the spirit of Ramadan to the unorganized sector. The event was generously sponsored by Motorola Solutions. Unlike traditional corporate Iftars, this initiative reached workers in their living spaces, fostering a true sense of belonging and appreciation. In total, 130 Iftar boxes were distributed. The beautiful event highlighted the importance of supporting those often overlooked during Ramadan. Volunteers Alex Geans, Pandiyarajan Murugesan, and Ranjv Abraham were instrumental to the event's success.

MAR
22

MAR
08

INTERNATIONAL WOMEN'S DAY 2025

The ASIS International Qatar Chapter celebrated International Women's Day 2025 with an empowering event that brought together 40 women, including two Qatari participants, to focus on leadership, resilience, and action. Speakers included Xiomara Henriquez, who discussed impactful leadership qualities, and Maria Angelica Avila, who led an interactive activity where attendees created a "Wall of Inspiration." All participants received commemorative IWD 2025 memorabilia. Special recognition was given to dedicated women chapter volunteers for their invaluable contributions.

ASIS QATAR ATTENDS OSAC RISK BRIEFING

On February 25, several ASIS Qatar chapter officers and members attended the "Global Risk Forecast 2025" event at Al Messila Resort and Spa, hosted by Crisis24 in partnership with the US Overseas Security Council (OSAC) Qatar. The keynote speaker, Ms. Manon Fakhoury, presented an in-depth analysis of geopolitical risks in the Middle East, highlighting critical security challenges and economic factors that influence businesses in the region. This event further reinforced ASIS Qatar's partnership with OSAC Qatar, ensuring that security professionals are equipped with the latest knowledge and strategies to navigate emerging global risks.

FEB
25

FEB
22

INAUGURATING 'SECURITY SPEAKER SERIES'

The ASIS International Qatar Chapter, in collaboration with the Transport Security Community, launched the first edition of the Security Speaker Series on February 22nd, focusing on "Aviation Security Culture: The Unseen Force Behind Safety & Trust." The session, led by aviation security expert Mr. Prabhu Jawahar, emphasized the critical role of fostering a security-conscious workforce through awareness, responsibility, and proactive engagement. Special thanks were extended to Transport Security Liaison Pandiyarajan Murugesan, volunteer Ajith U, and Program Chair Alex Geans for their support in making the event a success. Chapter Chair Ranjiv Abraham delivered the welcome address and presented a memento to the speaker. This session marked the beginning of a series aimed at strengthening security culture across industries.

ASIS QATAR ATTENDS OSAC BRIEFING

The ASIS Qatar Chapter participated in the Overseas Security Advisory Council (OSAC) Qatar event "Navigating the Digital Minefield" on January 28, held at the West Bay Qabila by Marriott Hotel. Ranjiv Abraham introduced the ASIS Qatar Chapter, setting the stage for insightful discussions led by experts who explored the challenges of digital misinformation, cyber threats, and navigating today's complex digital landscape.

SEP
15

JAN
16

INTERSEC EXPO DUBAI

From January 14–16, ASIS International Qatar Chapter members participated in Intersec Expo Dubai. Chapter Chair Ranjiv Abraham attended a key meeting with ASIS Middle East & North Africa leaders, including Sami AlAjmi and Hamad Almelaihi, along with officers from the Dubai and Dhahran Chapters. The meeting highlighted the importance of strengthening partnerships and collaboration within Region 12. A major event was the signing of a Memorandum of Understanding (MoU) between the ASIS Dhahran Chapter and Intersec Saudi Arabia, marking a strategic partnership to advance security standards. ASIS Qatar continues to actively engage in global and regional initiatives, reinforcing its presence in the security industry.

JAN

08

QATAR SECURITY PROFESSIONALS MEETUP– 2ND EDITION

On January 8, the ASIS International Qatar Chapter hosted the highly anticipated 2nd Edition of the Qatar Security Professionals Meetup at the Wyndham Westbay Hotel in Doha, which saw over 120 attendees.

The event was chaired by Chapter Chair Ranjiv Abraham and honored by the presence of Lt. Col. Ali Al-Suwaidi, Director of the Security Systems Department, Ministry of Interior, Qatar, as the Chief Guest. Guests of Honour included Philip Jonathan Bamber from Hamad International Airport, Jacobus Wepener from Hamad Medical Corporation, and Senior RSO Jeffrey W. Crockett from the US Embassy in Qatar.

The event featured a presentation on Enterprise Security Risk Management (ESRM) by Vice Chair Vitthal Teli, as well as the 2024 Chapter Report and Achievements presented by Chapter Chair Ranjiv Abraham. The launch of the chapter newsletter, edited by Communications Chair Pallavi Bichu, and an interactive live security quiz by Aamer Sohail Mohamed were also highlights.

The meetup culminated in the annual Chapter Awards, recognizing the dedication and contributions of key members and past chapter officers. The following were the esteemed organizations and individuals who received awards and appreciation at the event:
Emerging Partner of the Year: GSS Certis International
Enterprise Partner of the Year: Hamad Medical Corporation
Community of the Year: Next Gen Community (Led by Sharon P.V)
Volunteer of the Year: Alex Geans (Program Chair)

Special mentions were also awarded for:
Academic Excellence: Vitthal Teli CPP, PSP, PCI, MSI, CC (Vice Chair)
Membership Growth: Sreejith SV, CPP, MSyI, (Community Liaison)

A DISCUSSION WITH... JACOBUS WEPENER

Director of Security at Hamad Medical Corporation (HMC)

How did you first get involved in the field of healthcare security, and what has been the most rewarding aspect of working in this specialized area?

i initially built my security career through experiences in both police and military roles, followed by several years managing security in the hospitality and tourism sectors. However, when the opportunity arose to transition into healthcare, I recognized the immense scope this field offers. Healthcare security calls for a broad spectrum of skills—emergency response, tactical incident management, risk assessment, policy formulation, and employee training—so I knew I'd be able to draw upon my entire background.

Since joining HMC, the most rewarding aspect has been witnessing our transformation from a purely support-oriented security operation into an integral partner within the healthcare ecosystem. With strong support from my leader and a shared vision, we created a cohesive environment in which security staff recruitment, training, quality control, and technology all work in tandem.

On a day-to-day basis, it's incredibly gratifying to see our efforts realized: security teams responding seamlessly to an incident, backed by thorough training and the right resources. When our response is effective, it affirms that our proactive planning and continuous process-improvement efforts truly make a difference.

And even when we encounter challenges, we have the structure and expertise to analyze shortcomings and refine our approach for the future.

You gave an insightful talk at the ASIS Qatar event in January, focusing on security within healthcare. Could you briefly share the unique security challenges healthcare facilities face and how HMC handles these?

Absolutely. Healthcare security is often underestimated, but the challenges are immense. At Hamad Medical Corporation (HMC), we oversee a broad range of facilities that require distinct security strategies. Unlike typical corporate environments,

healthcare settings have to ensure the safety of patients, staff, and visitors while still maintaining the flow of critical services. For example, in emergency departments, we balance the urgency of medical care with protecting staff from potential harm. In mental health facilities, we face the challenge of safeguarding patients who may be at risk of self-harm or harm to others. Each setting requires tailored approaches, from robust access control in hospitals to sensitive procedures for child protection in pediatric areas. The key is maintaining a balance between open access for medical needs and stringent security measures to ensure safety.

What role does Enterprise Risk Management (ESRM) play in HMC's security strategy?

ESRM has been central to our approach. It's not just about reacting to incidents; it's about understanding risks in a holistic way and aligning them with the organization's objectives. At HMC, we use ESRM to evaluate risks across various facilities—whether it's managing access in hospitals, securing sensitive pharmaceuticals, or even protecting our ambulance hubs. By tying these risks directly to our assets, we make more informed decisions and prioritize what matters most. For instance, integrating AI into our CCTV systems under ESRM has helped reduce incidents of workplace violence by 10% last year, contributing to a safer environment for both patients

and staff. We're even developing predictive analytics to anticipate potential security breaches, which could revolutionize how we manage risks in the future.

The ESRM framework works best when it's supported by a solid foundation of skilled people, effective training, and cutting-edge technology. Our security team at HMC comprises around 3,000 personnel—both in-house and contracted—who are the backbone of our operations. It's crucial that we recruit the right people, support their welfare, and provide them with ongoing professional development. Training is tailored to different roles, ensuring that everyone from security officers to managers is prepared for their responsibilities.

Technology plays a huge role in this as well. For example, we've implemented advanced visitor access management systems, video analytics, and Power BI dashboards, all of which streamline operations and enhance security efficiency. Together, these elements create a strong, adaptive security system that allows us to address risks in real-time while planning for the future.

How do you ensure that your team stays prepared for the ever-changing security landscape? How can ASIS help with this, in your opinion?

I see security much like a sports team—success comes from preparation, practice, and adaptation. Our security teams are always learning, whether through internal training, collaboration with partners like ASIS, or analyzing past incidents to understand where we can improve. We regularly review our performance, much like a team reviewing game footage, identifying strengths to build on and weaknesses to address. In a world where threats evolve rapidly, our strategy is to stay agile—adopting new technologies, refining policies, and continually improving our response mechanisms.

Platforms like ASIS offer a 'training ground' for security professionals, helping us stay competitive in an increasingly complex landscape. By sharing ideas and learning new tactics, we fortify our collective defense.
What made it even more special was seeing Qatar being recognized on the global stage as a key contributor to the security profession. This achievement has given us an incredible sense of pride and motivation. It has strengthened my resolve to continue building a stronger, more impactful chapter that not only serves its members but also inspires others across the region.

Becoming an ASIS member is a fundamental part of our commitment to continuous improvement. It ensures that our security managers and key team members have access to the latest standards, guidelines, and best practices in the security industry.

Currently, about 40 of our team members are active ASIS participants. This not only enhances their skills but also fosters a culture of professional growth. ASIS certifications like CPP or APP provide our team with internationally recognized credentials that help us maintain a high level of professionalism and adaptability, especially as security threats evolve. It's about staying ahead of the curve, and ASIS is an invaluable resource for that.

Given the growing importance of cybersecurity, how do you see the integration of physical and cyber security evolving in Qatar's healthcare sector? Are there any specific initiatives you're particularly excited about at HMC?

Within HMC, we have a dedicated Information Security (InfoSec) team under our Healthcare Information and Communication Technology Department, and we partner closely to ensure both physical and digital realms are well-secured.

This collaboration involves crafting robust policies for system access control, integrating cybersecurity into our physical infrastructure and developing joint incident response plans.

Our security department—managing one of the largest CCTV networks in Qatar—employs its own cybersecurity specialist to ensure ongoing security assessments, vulnerability scans, and real-time threat detection.

We're currently working on initiatives that strengthen our cybersecurity within the CCTV network , such as unified platforms for threat monitoring and incident response. This is crucial in healthcare, where not only are our patients' safety and privacy are on the line, but also high-value medical equipment and sensitive data.

I'm particularly excited about advancing our risk management framework to reflect both physical and cybersecurity considerations, paving the way for more proactive threat mitigation in an increasingly interconnected environment.

What about AI? What do you think about the role of AI in securing medical facilities, and where is Qatar in the adoption of such tools and measures?

We have a dedicated AI team within our CCTV Department that is actively researching and refining the AI solutions we deploy across our security operations. By leveraging advanced analytics, including predictive modeling, real-time anomaly detection, and behavioral analysis—we can move from a purely

reactive stance to a more proactive, intelligence-driven approach.

From a cost-optimization perspective, we anticipate that AI can streamline at least 40% of our current security tasks. For example, AI-driven systems can handle basic surveillance and recognize potential issues before they escalate, freeing up security personnel for more complex or sensitive duties.

We are also investigating how AI-enabled pattern recognition can help us more accurately forecast incident patterns based on historical data.

Qatar has shown a forward-thinking stance toward AI adoption across multiple sectors—healthcare included. With a strong national push toward smart technologies, we see AI-driven security becoming ever more integral to safeguarding our facilities, not only in CCTV surveillance but also in areas like access control, visitor management, and automated incident reporting.

The synergy between a well-trained security workforce and cutting-edge AI tools promises a future in which security and efficiency continually advance in tandem.

Can you share a particularly challenging situation you've faced in your career at HMC, and how your team overcame it? What lessons did you take from that experience?

The COVID-19 pandemic was by far the most demanding crisis we have faced. Almost overnight, our security department was tasked with providing security for multiple quarantine facilities—an entirely new mission for our organization.

With no existing local framework, we had to innovate at rapid speed, taking insights from international best practices and adapting them to on-the-ground realities in Qatar. Under tremendous time pressure, our team adopted a "do, then act, then check, and plan" approach —basically reversing the usual project-management cycle to move faster than ever before.

We devised and tested security models, refined them in real time, and then scaled them across the country once they proved effective. This demanded extraordinary coordination: at times, we had to replace entire security teams overnight when personnel were exposed to the virus.

Our security training team responded by creating fast, repeatable, and easily deployable security tarinings.

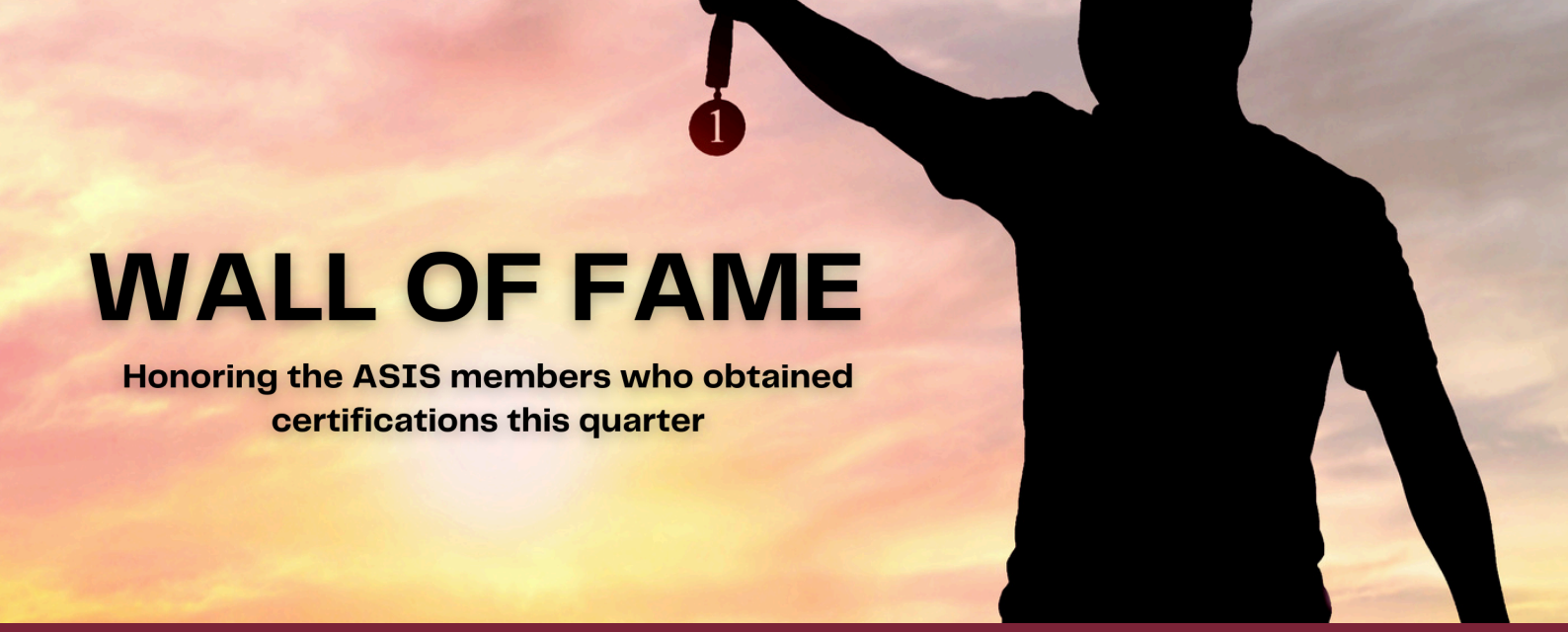
In the end, our model was recognized and adopted by the Ministry of Public Health, and we deployed teams across more than 30 quarantine facilities.

From this experience, we learned the importance of maintaining flexibility and a solutions-oriented mindset. Rapid, comprehensive training initiatives and the ability to pivot swiftly were crucial. Most importantly, we saw how critical close collaboration and unified communication are during a crisis. That close partnership among our security team and within the larger HMC organization —was fundamental to our success.

Do you have any thoughts on the future of healthcare security or advice for fellow security professionals?

Security is always evolving, and the threats we face are growing more sophisticated. As security professionals, we must embrace change and be willing to adapt. The future of healthcare security, especially, will be shaped by emerging technologies like AI and predictive analytics, which can help us anticipate risks before they happen.

My advice is to keep learning, stay connected with peers, and never underestimate the value of collaboration. Whether you're in healthcare, corporate, or another sector, the principles of risk management, training, and technological integration will serve you well. Security is not a one-size-fits-all approach; it's about continuously improving and staying ahead of the curve.



WALL OF FAME

Honoring the ASIS members who obtained certifications this quarter

CORINA VALENTINA ELBAYER, PSP

ASIS ID: 18926511

Corina is the first woman to earn the PSP certification from the ASIS International Qatar chapter, a significant milestone for our community. She currently serves as the Security Systems & Hardware Support Manager at Hamad International Airport.

MOULOUD ASKARNE, CPP

ASIS ID: 18944184

Mouloud Askarne, who serves as Security Manager at Teyseer Security Services and is part of the Healthcare Community, has earned the prestigious CPP certification from the ASIS International Qatar chapter.

Scan the QR code to view other Certified Professionals from the **Qatar Chapter** and also check **Global Directory**

TECHNICAL CORNER

Valuable insights contributed by our community

OSINT in the Age of AI

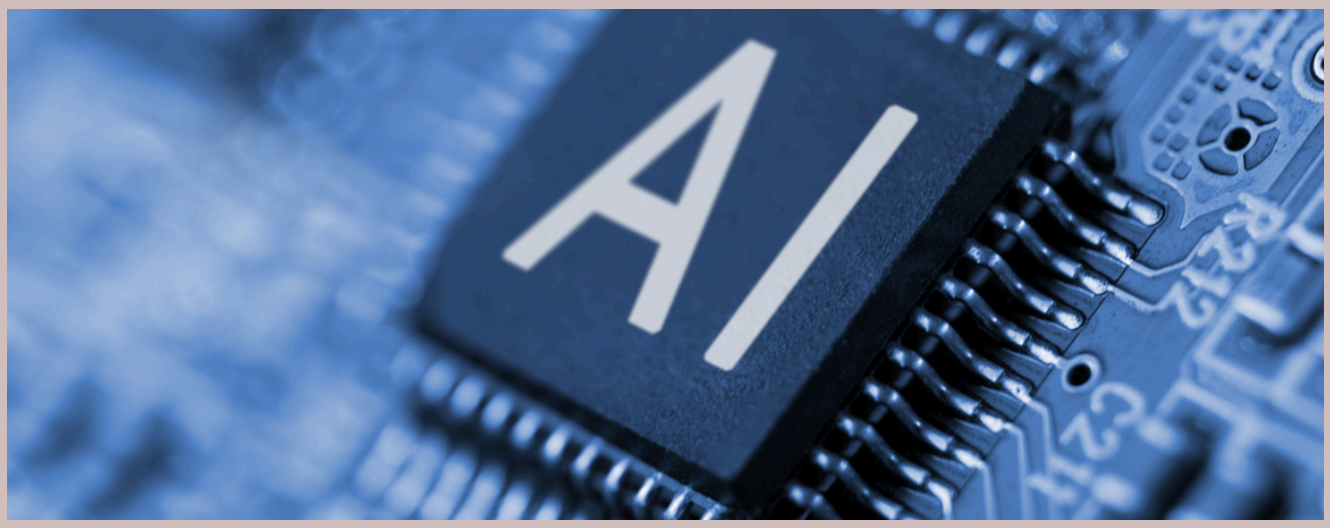
By Pallavi Bichu

What is OSINT?

OSINT refers to Open Source Intelligence. The scope of what qualifies as "open source" has widened a lot over time. Traditionally, OSINT might have meant sifting through publicly available news outlets, government publications, or academic papers. Today, it encompasses a much broader spectrum, including social media platforms, blogs, forums, videos, and more obscure sources like public records or crowdsourced intelligence repositories. There are even analyst teams whose main task is trawling for these threats on the dark web.

It may seem like publicly available information is just a Google search away, but that isn't always the case. OSINT risk analysts often use a variety of tools and databases to aid their searches, and have extensive domain knowledge gained through education and experience. They synthesize and verify information from these massive data sets to produce actionable risk reports for clients or for public. These searches could run the gamut from tracking geopolitical developments and policy changes to finding targeted threats towards companies and individuals or information on shadowy criminal groups. One of the most notable examples of the impact of OSINT techniques was the 2020 Bellingcat investigation of the poisoning of recently-deceased Russian opposition leader Alexei Navalny, where a team of of researchers and journalists analyzed publicly available flight data, phone metadata, and photographs to identify the Russian federal security agents who followed Navalny and ultimately poisoned him with the Novichok nerve agent.

When I started my career in OSINT seven years ago, the words ChatGPT and GenAI were definitely not part of common parlance. As a fresh Economics graduate entering the world of security through sheer fluke, it took a while to convince my near and dear ones that I was not, in fact, training to become a security guard or working for the CIA. The industry was certainly smaller, more opaque, and more labor-intensive than it is today. However, the more data you have, the harder it becomes to distinguish between what is relevant and what is noise- misinformation, disinformation, bias, and irrelevant chatter- an issue that's grown exponentially with the rise of AI in the field.



Use of AI in OSINT

Over time, AI has fundamentally reshaped the way intelligence is collected, analyzed, and distributed. In the beginning, it was used for simple automation, such as keyword-based search engines or pattern-matching algorithms. These early tools were primarily able to help analysts quickly process large volumes of data, but they weren't able to validate findings and draw conclusions- that was where analysts would come in.

Developments in the areas of machine learning (ML), natural language processing (NLP), and neural networks unlocked the potential for more sophisticated OSINT capabilities. AI tools began to understand not just the surface-level data, but also context and meaning. Text recognition and sentiment analysis became central to OSINT operations, enabling analysts to automatically detect patterns in language or tone that might signal potential threats.

The rise of generative AI (GenAI) tools like OpenAI's ChatGPT, Microsoft Copilot, and Perplexity AI further changed the landscape. These and others can now analyze unstructured data and summarize vast amounts of text, with Perplexity AI even able to provide references for its summaries. With the right prompts, one can also generate preliminary reports. This was a game-changer for OSINT analysts, who were traditionally buried in data. AI tools can instantly highlight trends and detect anomalies, thus saving analysts time and giving them the opportunity to work on deeper analysis. Another, later key innovation that has improved analysts' abilities to decipher information is AI's ability to conduct entity extraction. Tools like Maltego can now identify key people, places, events, or topics, enabling analysts to sift through social media, lengthy news articles, and other large bodies of text. AI can also translate and analyze data in multiple languages, further improving global intelligence collection.

Pitfalls of the use of AI in OSINT

With great power comes great responsibility. AI is not a catchall solution that can magically replace analysts in the OSINT industry. There are several aspects of the intelligence cycle that AI has trouble with, namely:

- **Misinformation and disinformation spotting:** AI tools are great for collection of information, but they are not immune to fake and misleading data. Human analysts are prized specifically for their critical thinking, intuition, and experience to assess the reliability of sources, which AI may not have the same instinct for– thereby further amplifying the problem of misinformation and disinformation.

- **Bias:** AI models are only as good as the data they are trained on, and if a model is exposed to a skewed information set, that bias is likely to perpetuated in its output. For instance, if an AI model is predominantly trained on Western news sources or English-language data, it may struggle to accurately interpret information from other parts of the world. If it is exposed primarily to a particular political narrative in a set of news stories of social media posts, its analysis and findings are unlikely to be well-rounded.

- **Information overload:** While AI tools are capable of collecting and even filtering through vast amounts of information, it is still often up to analysts to prioritize the findings. Analysts may then find inundated with data, spending as much time managing AI outputs as they did analyzing raw data.

Overall, while AI tools are great at processing large datasets quickly, they still struggle with complex reasoning, assessing the reliability of sources, drawing conclusions, and contextual understanding. For example, when analyzing a potential threat or geopolitical shift, analysts can factor in history, human behavior, and unspoken societal cues– elements AI can't yet fully comprehend. Due to these and many other reasons, OSINT analysts must exercise caution in their use of AI. Ultimately, AI can enhance, but cannot replace the human analyst's role in critical decision making... and OSINT analysts remain in great demand in today's geopolitically charged world!

Meet the Author

ASIS Member ID: 18845571

Pallavi Bichu is an experienced geopolitical threat analyst and corporate security manager, with over six years helping individuals, private organizations, and public entities secure facilities and people. She has worked across India and the GCC, and is an expert in intelligence analysis, conducting OSINT trainings for diverse audiences, and delivering regional security briefings to all levels.

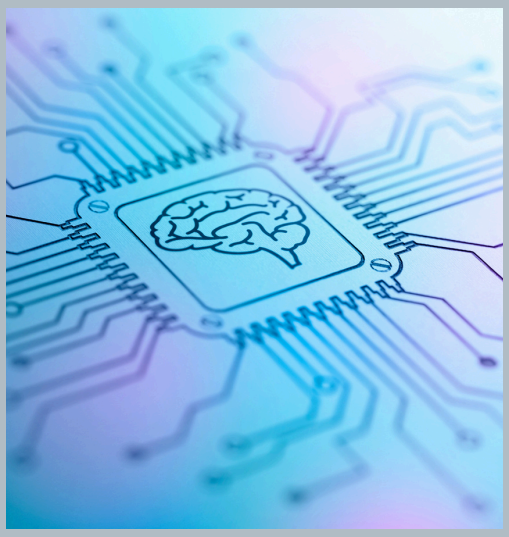
She is currently the ASIS Qatar Chapter Communications Chair and the Editor-in-Chief of the ASIS Qatar Newsletter. She holds a Masters and Bachelors in Economics and is an avid reader.

TECHNICAL CORNER

Valuable insights contributed by our community

The Impact of AI on Security: Lessons from Qatar

By Rahmatullah Khan Mohammed



Artificial Intelligence (AI) is transforming the security landscape, redefining how threats are detected, analyzed, and mitigated. Recent advancements, particularly by companies like DeepSeek, have introduced open-source AI models that require significantly less computational power and resources compared to industry leaders such as OpenAI, Google, Meta, and Microsoft. This development presents both new opportunities and unprecedented challenges for he security profession, especially in the realm of CCTV surveillance—a critical component of security operations across Qatar, including high-risk environments like healthcare facilities, commercial centers, and government infrastructure.

AI-Driven CCTV Systems: Enhancing Surveillance Efficiency

Traditional CCTV systems have long relied on human operators to monitor live feeds and revie\\w recorded footage. However, AI-powered video analytics are revolutionizing this process by introducing real-time threat detection, predictive analytics, and automated anomaly identification. AI-driven solutions can analyze hours of footage within seconds, identifying suspicious activities, unauthorized access, and potential security breaches with greater accuracy than human monitoring alone.

In Qatar, the Ministry of Interior's Security Systems Department (MOI SSD) has approved the deployment of advanced CCTV systems equipped with sophisticated facial recognition algorithms. These systems are utilized in various settings, including healthcare facilities, commercial buildings, malls, and hospitals, to enhance security measures by identifying individuals in real-time and monitoring access points.

AI in Traffic Violation Detection

Beyond stationary surveillance, AI has been instrumental in monitoring and enforcing traffic regulations in Qatar. The General Directorate of Traffic has implemented a unified radar system that automatically detects violations such as the use of mobile phones while driving and failure to wear seatbelts. This system employs advanced cameras and sensors to monitor driver behavior continuously, thereby enhancing road safety and reducing accidents.

AI and the Changing Role of Security Professionals

As AI takes on more analytical and monitoring tasks, the role of security professionals is evolving. Security personnel are no longer just passive observers but strategic decision-makers who interpret AI-generated insights and respond to threats in real time. AI augments human capabilities by providing enhanced situational awareness, but it also necessitates continuous upskilling of security professionals.

For instance, CCTV operators in Qatar's healthcare sector must now be trained in AI-based analytics to understand how algorithms flag unusual behaviors, differentiate between false positives, and respond to automated alerts effectively. Additionally, security teams must develop expertise in cybersecurity to protect AI-driven CCTV systems from hacking attempts, data breaches, and adversarial AI threats.

Challenges and Ethical Considerations

While AI-driven surveillance offers numerous advantages, it also raises concerns related to privacy, bias, and data security. Facial recognition technology, for example, can enhance security but may also introduce risks if not properly regulated. Security professionals must navigate the ethical implications of AI-powered monitoring while ensuring compliance with Qatar's stringent data protection regulations.

Furthermore, AI's reliance on vast datasets means that biases in training models can result in false alarms or discriminatory profiling. To mitigate these risks, organizations must adopt transparent AI policies, conduct regular audits of AI systems, and implement human-in-the-loop (HITL) approaches where security professionals validate AI decisions before taking action.

Preparing for the AI-Driven Security Future

For security teams in Qatar, embracing AI is no longer optional—it is essential for staying ahead of evolving threats. Organizations should invest in AI training programs, integrate AI-powered tools with existing security infrastructure, and collaborate with AI technology providers to customize solutions that meet Qatar's specific security needs. As AI continues to reshape the security landscape, the synergy between human expertise and machine intelligence will define the next generation of surveillance. By leveraging AI responsibly, Qatar's security sector can enhance efficiency, reduce response times, and create a safer environment while upholding the highest ethical standards in surveillance and monitoring.

Meet the Author

ASIS Member ID: 18955498

Mohammed Rahmatullah Khan holds a Bachelor's in Electronics & Communication Engineering and a Master's in Digital System Engineering. With extensive experience in the security domain, he has worked in the Hospitality industry in Katara hotels in Qatar, in the Oil & Gas sector at Qatar Shell and the healthcare industry at Hamad Medical Corporation. His strong IT background includes a role as Support specialist in the Technical Assistance Center supporting Avaya Routing and switching product lines. Rahmatullah is certified specialist in Cisco Networking, Genetec OTC, ETC, Milestone, ITIL, Aviatrix multi-cloud platforms, and various security software solutions, making him a well-rounded expert in integrated security systems and emerging technologies.

MEMBERSHIP FAQs

How do I become a Member of ASIS International?

- **Join ASIS International** via the official website: **www.asisonline.org**
- **Choose Membership Type:** Select Regular, Emerging Market 1 OR 2, Student, or CSO Center Membership.
- **Submit Application:** Complete the form and pay the required fee.

How do I become a Member of the 'Doha, Qatar Chapter?

- By default when you **Join** ASIS International using 'Qatar' as your primary address you will be automatically affiliated to 'Doha, Qatar Chapter'. There is no separate membership registration for the Local Chapter..

How do I verify my Chapter Membership?

- Log into ASIS International with your Credentials.
- Navigate to My Account: Click on "My Information" > "My Account" > "My ASIS Activities" > "My Memberships" > "My Chapter Memberships".
- If your Chapter is listed elsewhere Transfer Affiliation: Scroll down to "Interested in Changing Chapters?", and click on "Transfer your affiliation today." Navigate to "New Chapter", select "Qatar: Doha, Qatar" and click "Change Chapters".

How long is the Membership Valid?

- Generally valid for 1 year from your date of Payment for Student, EM1 & 2 Membership. Regular Membership can be paid for 1 year or 3 years.

How can I get a membership certificate and Badge?

- You will receive an email from Credly Stating your Digital Badge. A regular membership certificate can also be downloaded from the profile.

What are the Immediate Benefits of Membership?

- Discount on all ASIS Certification Exam Fee & Study Materials.
- Volunteering Opportunity with Local Chapter.
- Exclusive Access to Local Chapter Events & Workshops.
- Exclusive Access to Study Groups & Chapter Library.
- Exclusive Access to Members via Whatsapp Community.

How to contact if I have more queries?

- Chat / Online form at www.asisqatar.org
- Chat with Chapter Officers via Members Only group

+974-7744-5721 support@asisqatar.org www.asisonline.org

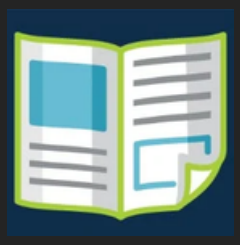
MEMBERSHIP BENEFITS

Making the most out of your ASIS membership starts with understanding all the benefits available to you, from free webinars to earn CPEs to volunteer roles available through chapters, communities, and ASIS's mentoring program. There are so many ways to get engaged, motivated by your peers, and grow professionally while giving back.

ASIS Board Certifications

Advance your career and elevate your earning potential by acquiring one of ASIS's prestigious board certifications.
APP, CPP, PCI, PSP

Security Management Magazine

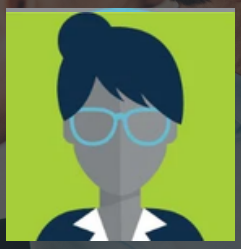


Stay well-informed by reading the latest articles from ASIS's award-winning magazine. Sign up for daily or weekly Security Management newsletters through your communications preferences in your ASIS account.

Standards & Guidelines

Keep current on security's best practices with free, unlimited access to all ASIS Standards & Guidelines in E-Book form. Check out the ASIS Store for publications covering all aspects of security management and enjoy member discounts.

Global Networking with ASIS Connects

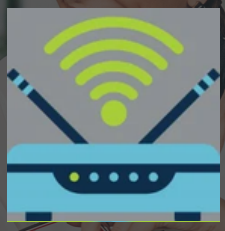


ASIS Connects, your 24/7 link to ASIS's 34,000 professionals, to ask questions, share stories, contribute knowledge, grow your network, and collaborate on the challenges you face in our Subject Area Communities.

Scholarships, Grants, and Awards

Grants and scholarships are available to all ASIS members through the ASIS Foundation. Awards are given to chapters, councils, and individuals to recognize their contributions to the security profession.

Free Webinars with Certificate



New! All ASIS webinars are now free for members so you can earn CPEs and engage in quality professional development year-round.

+974-7744-5721 support@asisqatar.org www.asisonline.org

OUR SPONSORS

AL SRAIYA SECURITY SERVICES

CERTIS

GROUP SECURITY SYSTEM

NAFFCO

Gulf Networks

MOTOROLA SOLUTIONS

Hanwha Vision

MANNAI CORPORATION