Authority Magazine

Sarbari Gupta Of Electrosoft On Pushing the Boundaries of AI

Relationships are the most valuable assets for your future success.

Artificial Intelligence is transforming industries at a breakneck pace, and the entrepreneurs driving this innovation are at the forefront of this revolution. From groundbreaking applications to ethical considerations, these visionaries are shaping the future of AI. What does it take to innovate in such a rapidly evolving field, and how are these entrepreneurs using AI to solve real-world problems?

As a part of this series, I had the pleasure of interviewing Sarbari Gupta. Dr. Sarbari Gupta is the Founder and CEO of Electrosoft Services, LLC headquartered in Reston, Virginia. Electrosoft, which specializes in cybersecurity, supports federal civilian and military organizations in advancing cyber resilience, achieving digital transformation, and adopting agile approaches that improve operational efficiency and security. This award-winning company is known for its focus on innovation and excellence, a posture

recently elevated by accepting a strategic investment from a leader in enterprise artificial intelligence solutions. With this force multiplier, Electrosoft stands ready to push the boundaries of AI use in cybersecurity.

Thank you so much for joining us in this interview series.

Before we dive in, our readers would love to learn a bit more about you. Can you tell us a bit about your childhood backstory and how you grew up?

I grew up in Kolkata, India, the middle child of three. My father was an engineer and my mother a homemaker. My family moved to Chicago for a few years while my father completed an MBA at Roosevelt University. I loved math and science and excelled at them. My father encouraged me to pursue engineering as a career, so I matriculated at the Indian Institute of Technology, Kharagpur, India. Upon graduation, I came to the United States to pursue graduate studies in electrical engineering at the University of Maryland. There, I discovered a novel area: computer and data security. I have been focused on the cybersecurity arena ever since.

Can you share the most interesting story that happened to you since I began your career?

When starting my entrepreneurial journey, my plan was to partner with a former boss who was looking for his next venture. I drew comfort in knowing he would guide me through the initial phases of setting up a new business and acquiring customers. Days before our launch date, he informed me that he was unable to move forward with our plan for personal reasons. I then had to choose between looking for my next job or embarking on the entrepreneurial journey alone. I decided on the latter path. I sometimes ponder: If events had unfolded differently, would I have become a founder and entrepreneur? I'd like to believe the answer is yes.

None of us are able to achieve success without some help along the way. Is there a particular person who you are grateful towards who helped get you to where you are? Can you share a story about that?

I've had many mentors who've helped me along the way. One of the biggest influencers was a former employer. He taught me about cybersecurity technology

and federal government contracting, especially the bookkeeping requirements. He offered guidance during the initial years of my entrepreneurial journey, giving counsel, making partnering referrals, and expressing unwavering confidence in my abilities.

Can you please give us your favorite "Life Lesson Quote"? Can you share how that was relevant to you in your life?

A favorite original quote is: "Relationships are the most valuable assets for your future success." Some early relationships include my father who always encouraged me to do my best and pursue my dreams; a graduate professor who helped form my interest in cybersecurity; and a former boss who mentored me in government contracting and assisted my early efforts to make Electrosoft a success. My husband's encouragement and support throughout the various ups and downs of establishing and running a business have kept me in the game and inspired me to greater heights. My network of fellow professionals, both inside government and out, have provided a wonderful sounding board and a source of inspiration. In fact, one long-time colleague just became a strategic investor in my firm, helping to advance our efforts to incorporate AI in cybersecurity solutions.

You are a successful business leader. Which three character traits do you think were most instrumental to your success? Can you please share a story or example for each?

Without doubt, perseverance, integrity, and fearlessness form the triad underlying my success.

Nothing was given to me in life. Hard work and perseverance brought me to where I am today. For example, upon founding Electrosoft, I recognized that being part of the Small Business Administration 8(a) program was vital to my company's success, as was securing a spot on a government multiple award schedule. The volume of paperwork associated with both endeavors was daunting, and I was a one-person firm. I persevered day-by-day, page-by-page to complete the necessary documentation and acquire those fundamental credentials.

I've always ascribed to the saying that one's character is evidenced by what one does when no one is watching. From my very first job till today, this principle has guided me. It's often tempting to take shortcuts, but you only hurt yourself by doing so. Reputation is paramount, and it is not easily retrieved once lost.

Fear of failure is a primary reason why most don't actualize their dream of starting and running a business. Often, people dwell on the negative outcomes of taking a

risk rather than weighing the potential positives and charting a course forward, when warranted. I've always researched the pros and cons, made a go–no-go decision, and been both fearless and optimistic upon saying "go," believing I will succeed. Electrosoft would likely not exist today if I hadn't had the courage to proceed when my partner unexpectedly withdrew — and if I didn't believe I could be successful alone.

Ok super. Let's now shift to the main part of our discussion. Share the story of what inspired you to start working with AI. Was there a particular problem or opportunity that motivated you?

Cybersecurity, the core competency of Electrosoft, motivated me. We do everything from helping develop federal guidelines and standards to standing up and operating Security Operations Centers (SOCs) for federal agencies. The latter experience opened my eyes to the amount of data and threats these analysts must address every day. Even the most competent analysts cannot keep pace, much less identify actual threats or recognize and act on patterns quickly. Yet, in cyber, speed is everything.

As I learned about AI, I recognized its capacity to automate threat detection, analysis, and response; recognize patterns and automatically move from reactive to proactive postures; apply behavioral analytics; and more. I was inspired to incorporate AI in our cybersecurity solutions.

I established a Technology and Innovation Directorate within Electrosoft to develop and advance the firm's unique cybersecurity solutions by incorporating AI. Most recently, I accepted a strategic investment from DigitalNet.ai to innovate and scale cyber defense by applying that firm's groundbreaking AI solutions and service offerings. I see the partnership as a force multiplier that will push the boundaries of AI with autonomous cyber defenses that unify detection, prediction, and response through mission-grade, multi-agent intelligence using ATLAS, its AI-driven cybersecurity platform.

Can you describe a moment when AI achieved something you once thought impossible. What was the breakthrough, and how did it impact your approach going forward?

One moment that fundamentally shifted my perspective on what AI can achieve came from our work helping customers build and operate Security Operations Centers (SOCs). For years, SOCs have relied on the traditional, human-centered model of monitoring, triage, and analysis. While effective, it became increasingly clear that this approach simply cannot scale to meet the volume, velocity, and sophistication of today's cyber threats.

As we partnered with DigitalNet.ai and explored their AI-enabled cybersecurity solution ATLAS, we witnessed AI agents performing analyst-level tasks with speed and consistency that would have seemed impossible just a few years ago. Seeing AI autonomously investigate alerts, correlate signals, and recommend actions was a breakthrough moment — it demonstrated that AI isn't just a tool to enhance SOC operations; it can fundamentally reshape how they function.

This realization has transformed our strategy. We are now rearchitecting our SOC implementations to integrate agentic AI at multiple layers, shifting from a people-dependent model to a hybrid, AI-first approach designed for scalability, resilience, and continuous improvement.

Please talk about a challenge you faced when working with AI. How did you overcome it, and what was the outcome?

One of the biggest challenges I've encountered when working with AI is attracting and retaining talent who are not only technically proficient, but who also possess the strategic vision required to advance AI-driven cybersecurity.

To address this, I launched a Technology and Innovation Directorate in January 2025 and appointed a highly technical, broadly experienced director to lead it. Under his leadership, the team has been actively evaluating AI models, chatbots, and automation tools to streamline our internal operations and design solutions that address emerging customer pain points and evolving mission needs.

Also, as referenced earlier, I established a strategic partnership with DigitalNet.ai. Their strengths in AI, digital modernization, and data analytics have significantly expanded our capabilities. This collaboration has served as a true force multiplier — enhancing both our technical capacity and our access to specialized talent.

Together, these efforts have not only helped us overcome the talent challenge but also positioned our company to innovate more rapidly and deliver AI-enabled cybersecurity solutions at scale.

Can you share an example of how your work with AI has had a meaningful impact (on others, on business results, etc.)? What was the situation, and what difference did it make?

The directorate I established built an AI assistant and chatbot off-cloud that can collect security data from six live sources in support of Security Operations Centers. The directorate also has developed AI/automation use cases for three federal customers that will support innovation, economy, and efficiency in

accomplishing their missions. Our ability to meet customer needs economically and efficiently with advanced technology sets the stage for better addressing our customers' needs and expanding federal and commercial business opportunities.

My focus on AI also opened the door for a strategic investor focused on AI. Previously, I had thought that a minority private equity partner might help Electrosoft attain the scale needed to bid on bigger prime and unrestricted contracts. However, a mutual interest in AI and cybersecurity gave me the scale I sought.

Here is the main question for our discussion. Based on your experience and success, can you please share "Five Things You Need To Know To Help Shape The Future of AI"? (Please share a story or an example, for each.)

1. Governance Is Critical

AI development and deployment must be accompanied by guardrails that ensure responsible, ethical, and safe AI use. So much is unknown about AI's potential pitfalls, even luminaries in the field — Musk, Altman, and Zuckerburg — can't reach consensus. Few could have predicted the recent lawsuits involving OpenAI's ChatGPT or chatbots associated with Character.AI and Chai.

2. Provenance

We cannot blindly purchase AI technology without knowing who developed it, where, and the source of component parts. While off-the-shelf technology offers

many cost advantages, it comes with many risks that must be fully understood prior to integrating them with our systems and networks. Consider the experience of SaaStr when the firm used Replit. It modified the firm's production code and even eliminated the production database. Further, its AI coding component hid bugs and other issues by creating fake data, fabricating reports, and manufacturing test results.

3. Data

AI technology relies on algorithms and training employing datasets. We must ensure that the algorithms are correct and data is appropriate, accurate, and unbiased — and originates from clean, verifiable sources. The media is filled with reports of racial bias in healthcare algorithms, gender bias in hiring software, and problems with facial recognition when it comes to people of color.

4. Human Element

It's critical that AI technology assist humans rather than replace them. There is no substitute for humans' ability to learn in real-time and their emotional intelligence when decisions need to be made. For this reason and more, humans must occupy a key position in decision-making loops. Zillow's iBuying Algorithm is a prime example. The system lacked the capacity to recognize sudden market changes, costing the firm about $500M.

5. Fallibility

With every new advance, we tend to trust that everything AI produces is correct, unbiased, and non-discriminatory. We must understand that AI is not perfect. We must test and retest. The four preceding items offer a cautionary tale on possible sources of deep fakes and hallucinations. I'm reminded of an incident involving a Deloitte report to an Australian government unit. It created fake citations and footnotes referring to non-existent books, reports, and court cases. Once identified, Deloitte had to refund part of its contract funding. However, the reputational damage it suffered is incalculable.

When you think about the future of AI, what excites you the most, and how do you see your work contributing to that future?

It's no secret that cyber criminals seem to possess limitless resources to launch persistent threats that quickly evolve in sophistication. I believe my work, which combines deep corporate expertise with an easily integrated cyber platform possessing a wealth of differentiators, will help the security of public and private

entities evolve at an equal or greater pace. Incalculable costs attend cybercrimes, so much so that some organizations never fully recover. I'm excited by a future where we outsmart these criminals and even turn their own tactics against them.

What advice would you give to other entrepreneurs who want to innovate in AI? Can you share a story from your experience that illustrates your advice?

I would encourage them to evaluate the risks associated with becoming an innovator and proceed accordingly. It's a field replete with opportunities for anyone bold enough to enter the space. Further, it's a broad field when it comes to applications. AI can be a game changer in movie making, agriculture, finance, healthcare, insurance, marketing, and many more verticals beyond cybersecurity. As I've emphasized as part of my story, if you don't take calculated risks, you'll likely not achieve the future you envision for yourself.

Is there a person in the world, or in the US with whom you would like to have a private breakfast or lunch, and why? He or she might just see this, especially if we tag them. :)

I am inspired by Jeff Bezos' business acumen and technical prowess, especially using AI. I would enjoy having a one-on-one conversation with him to see how he approaches problems and/or opportunities.

How can our readers further follow your work online?

The best source is our website, especially our News Posts and Newsletters. Our corporate LinkedIn page and my personal LinkedIn profile

Thank you so much for joining us. This was very inspirational, and we wish you continued success in your important work.