

FORCENET

E-ZINE

Magazine for military veterans in the corporate
November 2024, Volume VI, Issue 11

DEMYSIFYING CYBERSECURITY

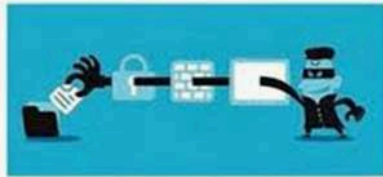
DECCAN
Chronicle
(19.07.2018 Page.12)

SOCIAL MEDIA: A HAVEN FOR CYBER CRIMINALS

INDIAN YOUTH IS THE THIRD HIGHEST NUMBER OF SOCIAL MEDIA USERS AFTER CHINA AND THE US WITH AN ESTIMATED NUMBER OF OVER 381 MOBILE PHONE SUBSCRIPTIONS WITH INTERNET CONNECTIVITY.

DR JAYANT MURALI

When I joined the Indian Police Service in 1991, there was no internet and therefore no type of cybercrime. Had anyone uttered the word cybercrime or Whatsapp back then, I would have mistaken it to be science fiction. Fast forward to today, the internet has become ubiquitous and omnipresent. It now traverses each and every corner of this planet touching more than 3.2 billion people. The number of people who have gained access to the internet has witnessed a sevenfold increase from 6.50 per cent of the global population in 2000 to 43 per cent of the global population in 2015.



India has over 460 million internet users today, and this figure is sure to rise to 635.8 million by 2021. There will be an estimated 358.2 million social network users in India by 2021, from the 216.5 million in 2016. The birth of the internet coupled with the formation of the World Wide Web appears to have paved the way for the evolution of the social media. The launch of Web 2.0 in 2004 which moved the static HTML to a more interactive and dynamic experience, spawned the mushrooming of social media sites over the world.

Cybercriminals tend to target social media with massive user bases, such as Facebook, LinkedIn, Twitter, Instagram etc. Majority of current attacks have been designed on lines of 'Kooftag' or 'war'. The attack user information and even their identities. This is then used to impersonate the user.

way for family friends and strangers to keep in touch. By luring millions of users to spend a considerable amount of time and share a great deal of information on the sites, the networking platforms were transformed into enormous repositories of data on potential victims. Why do criminals rob banks? Because that is where the money is! In the same way, cybercriminals are attracted to the social media sites because they are a treasure trove of data of millions of unsuspecting victims waiting to be ripped off.

Social media sites are awash with high denomination currency notes of gold left on the waiting to be picked up. This is not just the case of Samayam, but of all the other social media sites over the world.

Most perpetrators of cybercrime are using social media sites to lure victims into a trap. They are using the social media sites to lure victims into a trap. They are using the social media sites to lure victims into a trap.

66% cybercrimes against women committed by youth: Maha Police

Experts say ease of creating fake identities, limited understanding of internet harassment to blame

Cops detect only 31% of total cybercrimes

3733 CASES REGISTERED IN MUMBAI

STATE CYBERCRIME REPORT 2018

People who have grown up with computers and digital technology are more likely to be victims of cybercrime than those who are not. This is because they are more likely to be targeted by cybercriminals who are using their skills to exploit their vulnerabilities.

India is fast emerging as hub for cybersecurity innovations

As new malware emerge faster than ever, R&D centres are fighting back

BIG IMPROVEMENT IN QUALITY OF INDIAN CYBERSECURITY TALENT

India is fast emerging as a hub for cybersecurity innovations. As new malware emerge faster than ever, R&D centres are fighting back. A big improvement in the quality of Indian cybersecurity talent is also being noted.

India's first cyber security cluster to come up in Hyd

It Is Modelled On The Hague Security Delta

A CRADLE OF COLLABORATION

HSC will be a platform where research institutions, government bodies and cyber security firms will together drive innovation, product development and create awareness about cyber security and electronic warfare



The MoU was signed between the Government of Telangana and The Hague Security Cluster (HSC)

A meeting of major stakeholders was held in November last year. A delegation from state visited HSC recently

HSC will be a replica of the Hague Security Delta (HSD), the biggest cyber security cluster in the world which houses over 200 organisations

happen on a collaborative model. The HSC will become the hub for cyber security and help in setting up satellite cyber security clusters in Tier I and Tier II cities across the country. Cyber warriors will also be trained to combat cyber threat to Aadhaar security, banking and the like.

The first initiative of the HSC — Hague India Summer school — will be kickstarted in July. The HSD and the Netherlands will hand hold, share knowledge and work closely on the alliance between HSD and HSC for setting up the cluster. The basic aim of the HSC is to build an imperative ecosystem on cyber security, focus on capacity building and the PPP model which the Netherlands has expertise in. HSD and HSC have scheduled to organise a summer school in July. A soft-landing programme for Dutch companies who want exposure in the Indian market and vice versa are also being planned under this corporation, said Vikas Kohli, senior policy advisor. The Kingdom of Netherlands Embassy adding that the initiatives would give a cutting edge to cyber security students and young professionals.

₹712 cr fund scam busted, nine held

15,000 people fell prey to cyber crime

PINTO DEKAP | DC HYDRABAD, JULY 22



City police commissioner C.V. Anand speaks to the media about the investment fraud, in Hyderabad on Saturday.

Money was used to fund terror: Police

Nation's cyber security never more important

JAMES PATERSON

As we look at the world's most advanced nations, it is clear that cyber security is becoming a critical infrastructure for every nation. It is not just about protecting data, but about protecting the very fabric of our society.

SCAN ME



FORCENET



THE NETWORK THAT WORKS

FOCUS | PASSION | IMPACT

From the Editor

Dear Readers,

This month we celebrate the festival of lights. Wishing you all a **Very Happy Deepawali**. Light up this Diwali with Cyber security. In recent years, cybersecurity has emerged as one of the most sought-after fields in the workforce. For military personnel transitioning to civilian life, cybersecurity presents a unique and promising career path that leverages skills honed during military service. However, the journey from military service to **cybersecurity** can seem daunting. Let's **demystify** this transition by examining why veterans are ideally suited for this field and how they can navigate the path forward.

Military service instills discipline, strategic thinking, and the ability to perform under pressure, some qualities that are invaluable in cybersecurity roles. Veterans have extensive experience handling classified information, securing critical assets, and following strict protocols to manage risk. These attributes align well with the cybersecurity domain, where data security, threat detection, and proactive risk management are paramount. Their experience in the military has also equipped them to remain vigilant and respond decisively in high-stakes situations, a skill crucial for responding to cyber incidents where timing can make the difference between containment and catastrophe.

While veterans bring a strong foundation to cybersecurity, breaking into the field often requires formal training and specific certifications, which serve as both knowledge validation and entry points into the industry. Cybersecurity is often depicted as purely technical, but veterans should remember that soft skills—such as communication, teamwork, and leadership—are equally valuable. Transitioning from military service to cybersecurity is a promising pathway that offers job stability, intellectual challenge, and the opportunity to make a real difference in defending critical infrastructure and information.

In cybersecurity, veterans don't just find jobs; they find missions. The opportunity to protect and defend in a new capacity provides a renewed sense of purpose that resonates with many who have served. Cybersecurity, as a field, needs the dedication, strategic mindset, and resilience that veterans bring. With the right guidance and resources, transitioning military personnel can bridge the gap from service to a cybersecurity career.

I hope that you will enjoy reading this edition. You can email me your feedback, directly at forcesnetworkz@gmail.com . Stay resilient, stay curious, and venture boldly into the world of Cyber Security.



Yours Cyberknot

Capt Rajesh Nair
Editor, ForceNet E-Zine

**15 YEARS OF HUM FAUJI INITIATIVES
A JOURNEY OF COMMITMENT AND CAMARADERIE**

**15
YEARS**

We've reached remarkable milestones that reflect our commitment to **'Empowering Faujis'** and the trust you've placed in us

- ◆ 88% Business Growth in past 2 years
- ◆ Rs 1550 Cr of Assets Under Management
- ◆ Rs 6.05 Cr SIPs currently per month
- ◆ Awards this year itself: India's Most Future Ready Organisation (ET), Lifetime Achievers (FFFP), Social Impact recognition at the Global Financial Planners' Summit
- ◆ Global Expansion: One World Advisory Service
- ◆ 66,663 Jawans financially empowered through Workshops
- ◆ 5000 sq ft office, 60 Team Members now

Financial Planning
Retirement Planning
Corporate Bonds & FDs
Mutual Funds
Tax Planning
Wealth Creation
Central and State Govt Bonds
Insurance - Life & General
and much more

At the core of everything we do is **'Our Values. Your Trust.'**
Together, we've built a legacy—thank you for being part of our journey.



Schedule and visit, Hum Fauji Initiatives
1st & 2nd floor, Bimal Plaza, Pocket 4 Market, Sector 11, Dwarka, New Delhi - 110075
Email: contactus@humfauji.in
Company working hours: 9.30am – 6pm [Mon-Fri, 1st & 3rd Saturday]

EXCLUSIVE
INVITE



studio pepperfry

Hazratganj, Lucknow

Saluting The Defence Forces

Contact Now

For Best Deals | Pre and Post Order Assistance
For All Items Bought Through Us Pan India!

studio pepperfry

Sapru Marg, Hazratganj, Lucknow

☎ 9305216506

STUDY IN IRELAND



- World-class education ... Steeped in history
- Education is in the DNA of Ireland
- Second highest exporter of software after India
- Ireland has third highest GDP per capita in the world, - after Luxembourg and Switzerland
- Universities with high world-rankings

We are specialists for Critical Skill Work Visa after studies

We provide help for admissions to study Medicine in Europe



HEPTA CONTINO INC



A STUDENT RECRUITER TO IRELAND WITH A DIFFERENCE

www.heptacontino.com

Email: heptainformation@gmail.com

Phones: +353 8949 14324, +91 72176 26824

We support our students to select courses based on their education and experience and give them support to integrate with European countries



FINVISION FINANCIAL SERVICES

Change Adapt & Grow with Finvision

About us

Finvision Financial Services is one of the fastest growing investment firm across India and as on date we are managing multi-hundred crore investments of 1000+ armed forces personnel and generating the best risk-adjusted returns.



Proactively manage portfolios

Emphasis on risk management

Continuous monitoring & periodic re-alignment of portfolio

Focus on customized services & sound fundamentals

+91-7508055826
+91-9654341212

Change Adapt and Grow with Finvision

www.finvision.in

FOLLOW US



Contents

From the Editor	2
General Humour : Col Amit Dalvi	9
Demystifying Cyber Security - Theme Articles:	
-----By Lt Col Iqbal Singh.....	11 - 16
-----By Mr Anish Jairath.....	17 - 22
-----By Maj Ashish Chauhan.....	23 - 25
-----By Col Atul Kumar.....	26 - 33
-----By Capt Sam Armstrong Kappala.....	34- 40
Survey - Member Speak:	42 - 47
Star of Forces Network: Col KPM Das	49 - 56
Author of the Month: Col Sunil Kotnala	58 - 67
Stars on the Horizon: Ms Ariya Nair	68 - 75
Author of the Month: Col Dharamdatt Goel	76- 81
Moment in Time:	82 - 84
The Deepfake Dilemma: Navigating Corporate and Personal Cybersecurity Threats: By Capt Rupa Mittapalli.....	86- 89
Ageing Gracefully: By Col Dinesh Dutt Sharma.....	90 - 93
If Karma Balances Everything Then Why Bad People Prosper And Good People Suffer !!!: By Maj Tarun Pratap Singh.....	95 - 103

[A NOTE FOR THE READERS](#)

This is an interactive e-magazine with active links on many pages, including the advertisements, which can be used by just tapping or clicking on them.

For ease of providing feedback, such links have been provided at the end of the articles too.

Disclaimer: The opinions expressed within this e-magazine are the personal opinions of the authors and interviewees. Thus, the information and viewpoints presented in the articles do not represent those of Forces Network, and neither does Forces Network accept any duty or responsibility for them.

Online Feedback / Review

We would be featuring Feedback received from users post clicking on the interactive active links of the e-magazine. These links can be used by just tapping or clicking on them. For ease of providing feedback, such links have been provided at the end of each articles.

Feedback on: EXPATRIATE INTERVIEW - LT COL HARINDER SOOD,
YSM (RETD) - FEB 2023 VOL 5_2

An inspiring insight into an Officer's service tenure and his post retirement stint going on with the UN Headquarters NEW YORK, USA. It was of much interest reading his chronology of postings and missions. Also I would request if I can be connected to Lt Col H Sood(R) through Forces Network.

Additional Suggestions:

Everything is good about the magazine. Keep up the good job

MAJ SHASHANK SHARMA



Short story behind this sketch.

It is a kind of real life story. That is to say, this has actually happened in our unit, back in Jan 1995. We were based in a very remote place , middle of nowhere, in the Eastern Command. Our higher HQ, was about 40 odd kilometers away. We had purchased an assembled computer recently (out of Regiment Fund, my guess, but I could be wrong). It was a 386 processor unit. Not many were aware how to use it. In addition to a team of clerks, the Doctor was the only Computer Literate in the unit. One day, the computer was slower in its response than usual. One of the clerks, just mentioned to another in passing, that the computer may have a virus. The news spread like wildfire. Many stalwarts, from various walks of (unit)life, came forward with solutions. A syndicate solution was arrived at. The doors and Windows were shut. (Remember, that was an era when we used to remove shoes outside the computer Room). Eventually, the Doctor was summoned to cure it.

AUTHOR

DEMYSTIFYING CYBER SECURITY AS A CAREER

A SUNRISE SECTOR



A SPECIAL FEATURE

Theme Article

The Impact of AI on Cybersecurity: A Transformative Shift

BY IQBAL SINGH

The integration of AI and Generative AI (GenAI) into various sectors has sparked significant discussion regarding its potential benefits and challenges. In cybersecurity, the implications of GenAI are particularly profound. As cyber threats evolve in sophistication and scale, the need for innovative solutions becomes increasingly urgent. This article explores how GenAI is reshaping the cybersecurity landscape, what changes are on the horizon, the potential impact on jobs, the emergence of new roles, and the essential skills needed in this evolving field.

AI, or artificial intelligence, refers to technology that simulates human intelligence and applies it according to the use cases. Thus, AI machines can think like human beings, which includes analytical and problem-solving skills. Undoubtedly this technology is revolutionising almost every industry including the field of cybersecurity. According to a recent research, the market of **AI cybersecurity** products was around \$15 billion in 2021, but it will be extended to \$135 billion by 2030.

Thus, the role of artificial intelligence in cybersecurity includes handling the tasks that require human intelligence and analysis. However, the greatest benefit of using AI is that it can automate tasks that save time and cost and increase efficiency. So, it solves numerous challenges of cybersecurity with multiple techniques like natural language processing, machine learning, pattern recognition, etc.

The Transformative Impact of AI on Cybersecurity

Artificial intelligence (AI) and machine learning (ML) are revolutionizing the cybersecurity industry. The emergence of ML as a tool for detecting, predicting and responding to security threats has been a game-changer. AI's ability to process vast amounts of data, learn from patterns, and adapt to new threats makes it an invaluable asset in cybersecurity.

Here are some key areas where AI is poised to revolutionize the field:



AI can power bot the Hacker as well as the Defender Source: AI generated image
Imagen 3

Enhanced Threat Detection and Prevention:

- **Real-time anomaly detection:** AI algorithms can analyze network traffic, user behaviour, and system logs to identify suspicious activities that may indicate a cyberattack.
- **Predictive analytics:** By analyzing historical data, AI can predict potential threats and vulnerabilities, allowing organizations to take proactive measures.
- **Malware detection and prevention:** AI-powered systems can detect and block new and unknown malware variants, even before they are widely recognized.

Automated Incident Response:

- **Swift and efficient response:** AI can automate routine tasks such as isolating infected systems, containing the spread of malware, and restoring systems to their original state.
- **Intelligent decision-making:** AI can analyze incident data to identify the root cause and recommend the most effective response strategies.
- **Improved Security Operations Center (SOC) Efficiency:**
- **Automation of mundane tasks:** AI can automate repetitive tasks, freeing up security analysts to focus on more complex and strategic activities.
- **Enhanced threat intelligence:** AI can analyze threat intelligence data to identify emerging trends and threats.



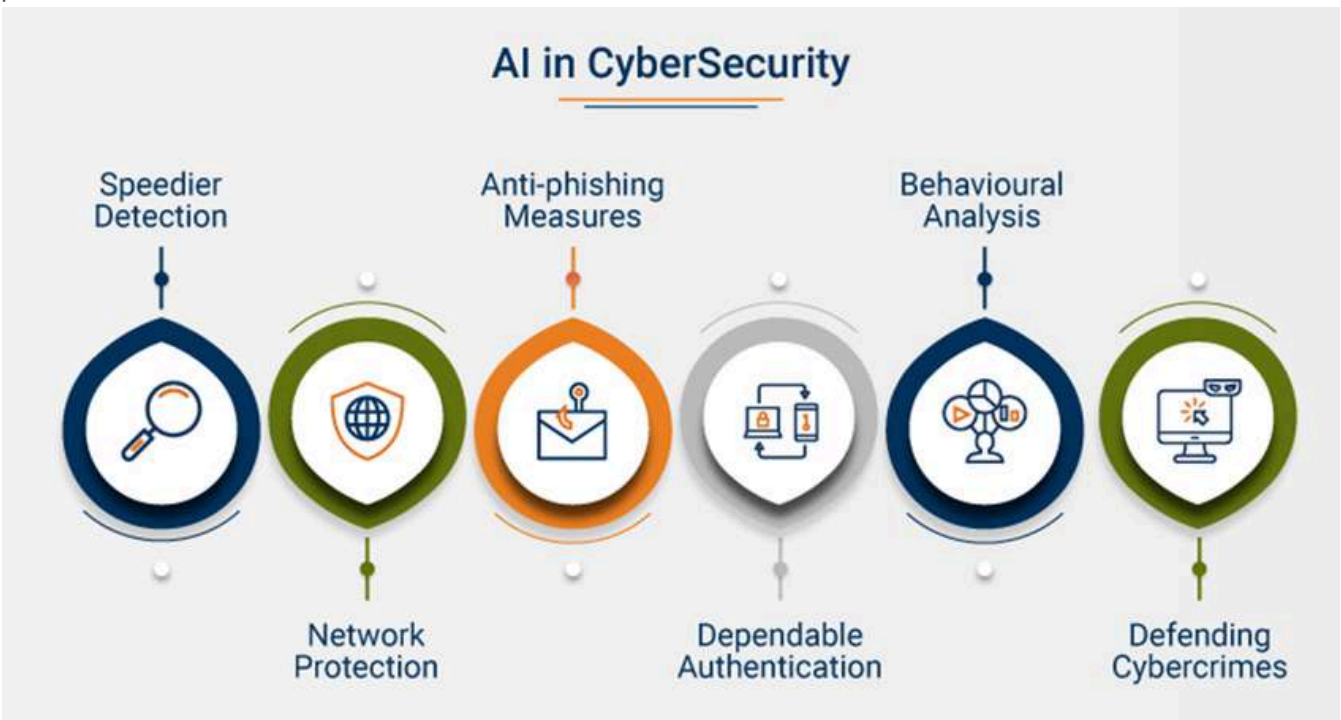
Security Professional Manning a SOC

Source: AI generated image

Advanced Security Analytics:

- **Behavioural analytics:** AI can analyze user behaviour to detect anomalies and identify potential insider threats.

Network traffic analysis: Cybersecurity professionals can use AI powered tools to analyze network traffic and easily identify suspicious patterns and detect advanced persistent threats (APTs).



The Various Facets of Cyber security that would be impacted by AI Source: Readwrite.com

The Changing Landscape of Cybersecurity Jobs and Roles

The integration of AI into cybersecurity will significantly alter the job roles and skills required of cybersecurity professionals. While AI will automate many routine tasks, it will also create new opportunities for those with specialized skills.

1. Increased Demand for AI Specialists:

- **AI engineers and data scientists:** These professionals will be responsible for developing and implementing AI-powered cybersecurity solutions.
- **AI security analysts:** These analysts will use AI tools to analyze threat data, detect anomalies, and respond to incidents.

2. Evolving Role of Security Analysts:

- **Strategic thinking:** Security analysts will need to shift their focus from manual tasks to strategic planning, threat intelligence analysis, and incident response management.
- **Collaboration with AI:** Analysts will need to collaborate with AI specialists to leverage AI's capabilities effectively.

3. New Roles and Opportunities:

- **AI ethics and governance specialists:** These professionals will ensure that AI is used ethically and responsibly in cybersecurity.
- **AI risk assessment experts:** These experts will assess the risks associated with AI-powered security solutions and develop mitigation strategies.

The Impact on Hackers, Law Enforcement, and Blue Teams

AI will also have a significant impact on hackers, law enforcement, and blue teams. Hackers may leverage AI to develop more sophisticated and evasive attacks, while law enforcement and blue teams can use AI to investigate cybercrimes and identify perpetrators.

1. Hackers and AI:

- **Advanced attack techniques:** Hackers can use AI to develop more sophisticated and targeted attacks, such as deepfakes and AI-powered malware.
- **Automated attacks:** AI can automate the process of launching attacks, making them more efficient and scalable.

2. Law Enforcement and AI:

- **Enhanced investigation capabilities:** AI can help law enforcement analyze digital evidence, identify patterns, and track cybercriminals.
- **Proactive threat intelligence:** AI can be used to predict and prevent cyberattacks before they occur.

3. Blue Teams and AI:

- **Improved threat detection and response:** Blue teams can leverage AI to detect and respond to threats more effectively.
- **Enhanced security posture:** AI can help blue teams identify and address vulnerabilities in their security infrastructure.



This is how a Future SOC may look like

Source: AI generated

Essential Skills for the AI-Driven Cybersecurity Era

To thrive in the AI-driven cybersecurity landscape, professionals will need to develop a diverse set of skills. Here are some key skills that will be in high demand:

- **AI and machine learning:** A strong understanding of AI and machine learning algorithms is essential for developing and implementing AI-powered security solutions.
- **Data analysis and visualization:** The ability to analyze large datasets and visualize the findings is crucial for identifying trends and patterns in threat data.
- **Cybersecurity fundamentals:** A solid foundation in cybersecurity principles, including network security, cryptography, and risk management, is still essential.
- **Ethical hacking and penetration testing:** Understanding the techniques used by hackers can help security professionals identify vulnerabilities and strengthen defences.
- **Problem-solving and critical thinking:** The ability to solve complex problems and think critically is essential for navigating the ever-evolving cybersecurity landscape.

Up-Skilling for the Future of Cybersecurity

To stay ahead of the curve, cybersecurity professionals will need to continuously up-skill and acquire new knowledge. Here are some ways to do so:

- **Online courses and certifications:** There are numerous online courses and certifications available to help professionals develop the skills they need.
- **Professional development programs:** Many organizations offer professional development programs to help employees stay up-to-date on the latest trends and technologies.
- **Networking and collaboration:** Building relationships with other cybersecurity professionals can provide valuable insights and opportunities for learning.

Conclusion

AI is poised to have a profound impact on the future of cybersecurity. By enhancing threat detection, automating incident response, and improving security operations, AI can help organizations protect themselves against the growing threat of cyberattacks. However, the successful integration of AI into cybersecurity will require a skilled workforce with a deep understanding of AI, machine learning, and cybersecurity principles. By investing in training and development, organizations can ensure that they have the talent they need to thrive in the AI-driven cybersecurity era.



Lt Col Iqbal Singh is an infantry officer who is now working with a Big Tech firm based at Gurgaon. He is also the Founder of Forces Network. Iqbal took premature retirement from the Indian Army in 2008. He has in the past worked with Satyam Computers at Hyderabad and Nokia at Noida. He is fond of public speaking, writing and training and loves to share his knowledge with others. He has mentored hundreds of military officers in their transition journey into the corporate.

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor

Theme Article

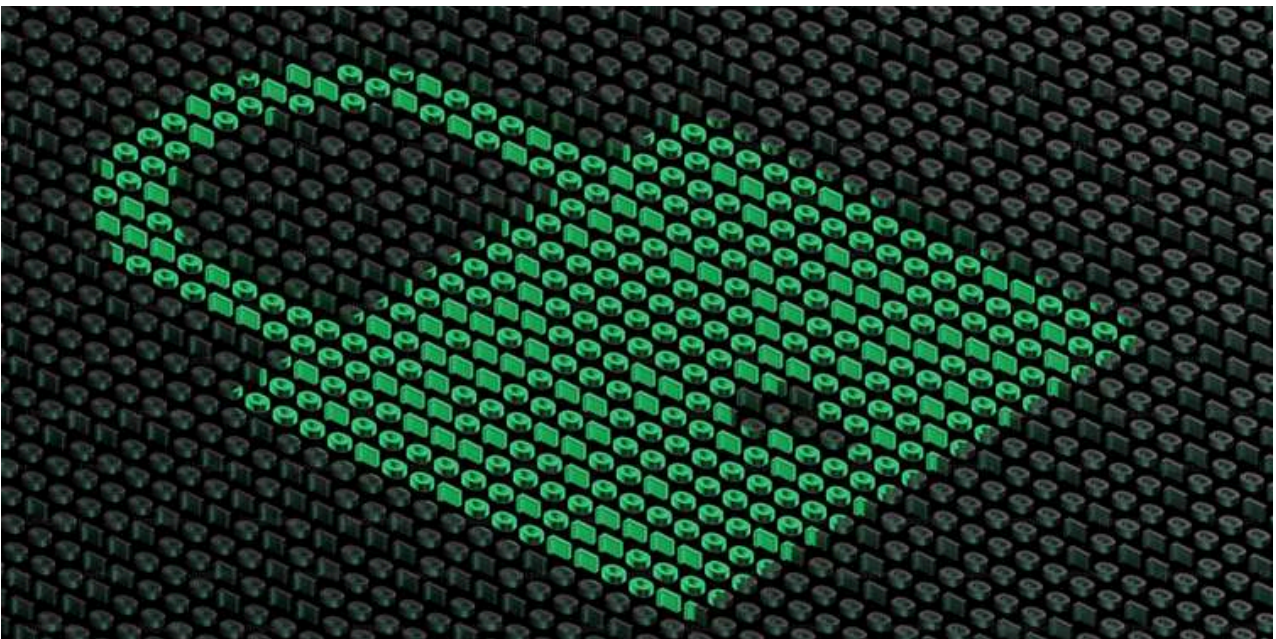
Demystifying Cyber Security

BY ANISH JAIRATH

In today's digital age, cybersecurity has become one of the most critical domains for protecting businesses, governments, and individuals. As organizations increasingly rely on digital infrastructure, the demand for skilled professionals who can safeguard sensitive information and combat cyber threats is skyrocketing. For military personnel transitioning to civilian careers, cybersecurity presents an attractive and promising career path. The strategic thinking, discipline, and problem-solving abilities honed during military service make veterans particularly well-suited for this rapidly evolving field.

This explores the opportunities within the cybersecurity domain, how military skills translate into success in this field, and the steps veterans can take to build a thriving career in cybersecurity.

Cybersecurity involves the practice of protecting systems, networks, and data from digital attacks, unauthorized access, or damage. These attacks may come from hackers, cybercriminals, or even nation-states, with motives ranging from financial gain to espionage and sabotage. Cybersecurity professionals are responsible for identifying vulnerabilities, preventing attacks, and responding to security breaches when they occur. As technology becomes more integral to every aspect of modern life, the scope of cybersecurity has expanded to include areas such as cloud security, data privacy, encryption, and even artificial intelligence (AI)-driven threat detection. This growth has led to an increased demand for cybersecurity experts across industries—from finance and healthcare to government and defence.



Ensures All Data and Intellectual Property is Secured and Protected ~Shubham Dhage, Unsplash

Why Cyber Security is a Great Fit for Veterans

1. Mission-Oriented Mindset

Just like in the military, the cybersecurity domain is focused on protecting critical assets and maintaining a strong defense against potential threats. Veterans are accustomed to operating in high-stakes environments where every decision matters. This mission-oriented mindset is a perfect match for cybersecurity, where professionals must think strategically, anticipate risks, and act decisively to protect digital infrastructure.

2. Experience in Security Protocols

Military personnel are well-versed in maintaining security protocols, whether it's safeguarding classified information or protecting physical assets. Cybersecurity similarly involves creating and following strict security protocols to ensure that sensitive data and systems remain protected from unauthorized access or attacks.

3. Problem-Solving Under Pressure

Military training emphasizes quick decision-making and problem-solving in high-pressure environments. In cybersecurity, threats can emerge at any time, and professionals must be able to assess the situation, identify vulnerabilities, and respond rapidly. Veterans' ability to remain calm under pressure and think critically in the face of uncertainty gives them an advantage in this field.

4. Adaptability to New Technologies

The military often involves learning and adapting to new technologies, whether it's advanced communication systems, weapons, or logistics tools. Similarly, the cybersecurity field is constantly evolving, with new threats and technologies emerging regularly. Veterans' ability to adapt to new tools and techniques positions them well for success in this ever-changing domain.

5. Teamwork and Leadership

Veterans are experienced in working as part of a team, often in hierarchical structures where clear communication and leadership are essential. In cybersecurity, teamwork is crucial, whether it's collaborating with IT teams, upper management, or law enforcement agencies during an investigation. Veterans with leadership experience can also excel in managerial roles within cybersecurity.

Key Verticals in the Domain

1. Network Security

Network security focuses on protecting an organization's internal networks from cyber threats. This includes safeguarding data, monitoring traffic, and implementing firewalls and encryption to prevent unauthorized access.

Veterans with experience in military communications, IT systems, or signal intelligence are well-suited for network security roles. Their knowledge of secure communications and monitoring systems can be directly applied to network security.

Key Responsibilities in Network Security:

- Designing and implementing security solutions to protect network infrastructure.
- Monitoring network traffic for suspicious activity or unauthorized access.
- Managing firewalls, VPNs, and other security protocols to ensure data protection.
- Conducting regular security audits to identify vulnerabilities and recommend improvements.

Career Pathways in Network Security:

- Network Security Engineer: Designs and implements security systems to protect network infrastructure.
- Security Administrator: Manages the security protocols and systems within an organization's network.
- Network Security Analyst: Monitors network traffic and identifies potential threats or vulnerabilities.

2. Incident Response and Threat Hunting

Incident response involves detecting, analyzing, and responding to cybersecurity incidents, such as data breaches or malware attacks. Threat hunters proactively search for signs of cyber threats within an organization's network to prevent attacks before they occur. Veterans with experience in military intelligence, reconnaissance, or rapid response teams may find incident response and threat hunting to be a natural fit. The ability to analyze threats, respond quickly, and coordinate team efforts is critical in this area.

Key Responsibilities in Incident Response and Threat Hunting:

- Investigating and responding to cybersecurity incidents in real time.
- Analyzing malware, breaches, or unauthorized access attempts to determine the cause.
- Identifying potential vulnerabilities in an organization's network before they can be exploited.
- Developing and implementing incident response plans and protocols.

Career Pathways in Incident Response:

- Incident Response Analyst: Handles real-time response to cyber incidents and investigates security breaches.
- Threat Hunter: Actively searches for potential threats within the organization's systems and networks.
- Forensic Analyst: Specializes in investigating and analyzing cybercrime incidents to determine the origin and impact of attacks.

3. Cyber Risk Management

Cyber risk management focuses on assessing and mitigating the risks associated with cyber threats. This includes identifying potential vulnerabilities, developing strategies to reduce the likelihood of attacks, and ensuring compliance with cybersecurity regulations.

Veterans with leadership, strategic planning, and risk assessment experience are well-suited for cyber risk management roles. Just as military leaders assess risks during missions, cyber risk managers evaluate potential threats and develop strategies to protect organizations.

Key Responsibilities in Cyber Risk Management:

- Assessing the likelihood and impact of various cyber threats on the organization.
- Developing risk mitigation strategies to minimize vulnerabilities.
- Ensuring that the organization complies with cybersecurity regulations and industry standards.
- Conducting regular risk assessments and updating security protocols as needed.

Career Pathways in Cyber Risk Management:

- Cyber Risk Manager: Develops strategies to identify, assess, and mitigate cybersecurity risks.
- Compliance Officer: Ensures that the organization meets all relevant cybersecurity regulations and standards.
- Information Security Officer: Oversees the organization's cybersecurity risk management efforts.

4. Ethical Hacking and Penetration Testing

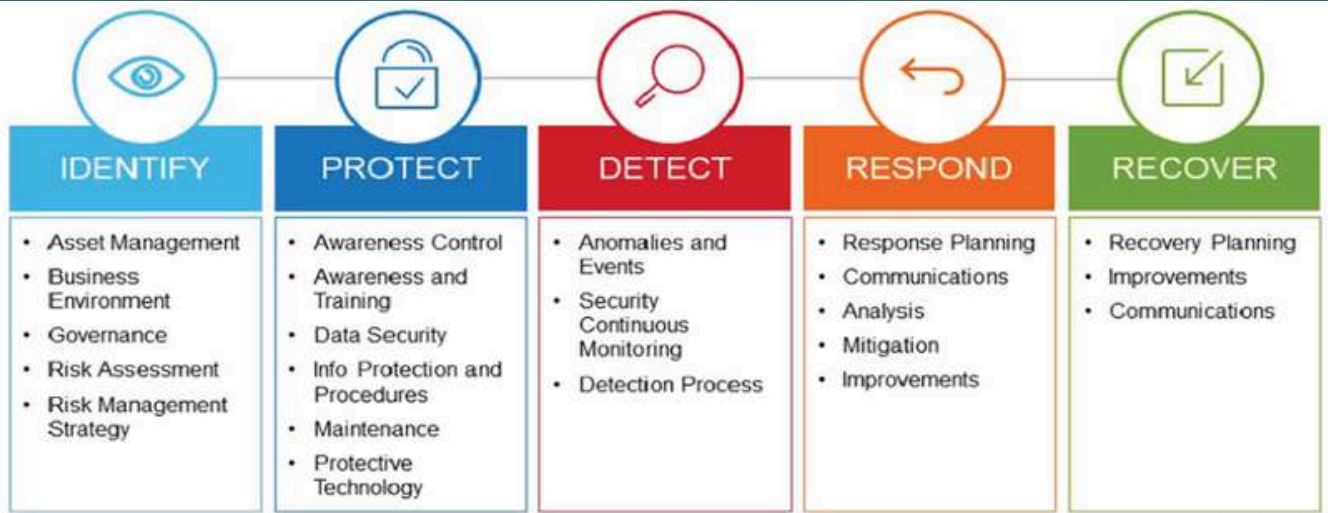
Ethical hackers and penetration testers simulate cyberattacks on an organization's network to identify vulnerabilities before malicious actors can exploit them. This proactive approach helps organizations strengthen their defences. Veterans with a background in military intelligence, counterintelligence, or reconnaissance can apply their skills in identifying vulnerabilities and understanding the mindset of potential adversaries to become ethical hackers.

Key Responsibilities in Ethical Hacking:

- Conducting penetration tests to identify vulnerabilities in an organization's network.
- Simulating cyberattacks to assess the effectiveness of security measures.
- Reporting findings to the organization's IT and security teams with recommendations for improvement.
- Staying up-to-date on emerging threats and hacking techniques.

Career Pathways in Ethical Hacking:

- Penetration Tester (Pen tester): Simulates cyberattacks to test an organization's security.
- Ethical Hacker: Identifies and reports security vulnerabilities through authorized hacking activities.
- Security Consultant: Provides expert advice on how to improve an organization's security posture.



The Basic Framework of Cyber Security

~NC4, Google Images

Steps to Successfully Transition into Cyber Security

1. Leverage Military Experience

Veterans should highlight the cybersecurity-related aspects of their military service when applying for civilian roles. Experience in secure communications, intelligence gathering, risk assessment can be directly applicable to cybersecurity roles. Veterans can also emphasize their leadership, problem-solving, and crisis-management skills.

2. Pursue Relevant Certifications

Certifications are highly valued in the cybersecurity field and can help veterans build the technical skills needed for specific roles. Some recognized certifications include:

- **CompTIA Security+:** An entry-level certification that covers basic cybersecurity concepts.
- **Certified Information Systems Security Professional (CISSP):** A more advanced certification that demonstrates expertise in designing and managing cybersecurity programs.
- **Certified Ethical Hacker (CEH):** A certification for professionals who specialize in ethical hacking and penetration testing.
- **Certified Information Security Manager (CISM):** A certification focused on risk management and governance.

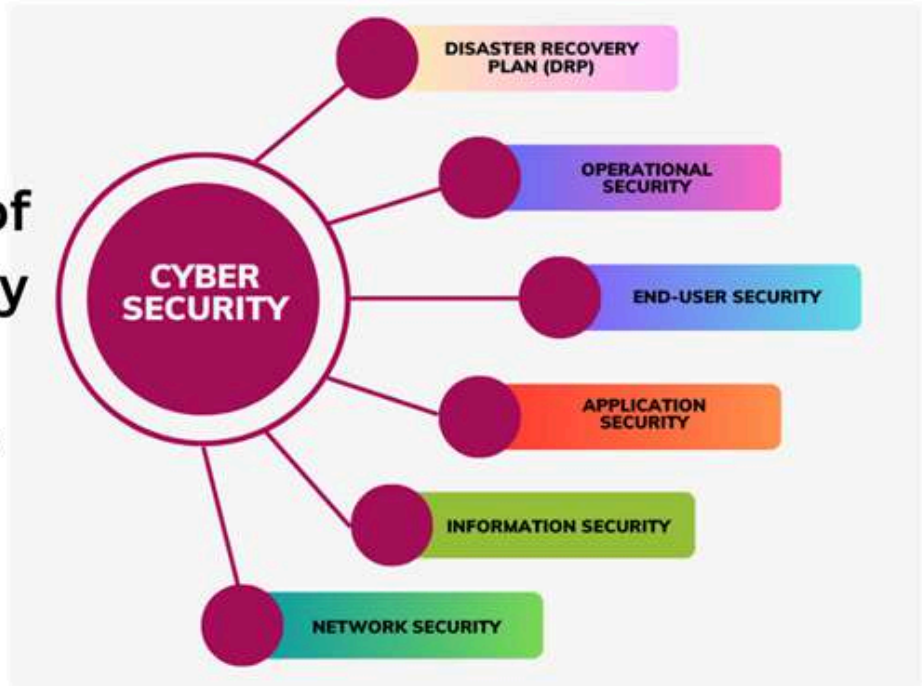
3. Gain Hands-On Experience

Practical experience is crucial in cybersecurity. Veterans can gain hands-on experience through internships, entry-level roles, or even volunteer opportunities in cybersecurity. Many organizations offer veterans' programs that provide training and job placement assistance in the cybersecurity domain.

4. Join Veteran Cybersecurity Networks

Many veterans' organizations and cybersecurity groups offer networking opportunities, mentorship programs, and resources specifically designed for veterans entering the cybersecurity field. Joining these networks can help veterans build connections, find job opportunities, and gain valuable advice from professionals already working in the industry.

Importance of Cybersecurity Tools and Techniques



Conclusion

~ ICSS India, Google Images

For transitioning military personnel, cybersecurity offers an exciting and fulfilling career path that leverages many of the skills acquired during service. Veterans bring a unique blend of strategic thinking, adaptability, leadership, and crisis management, all of which are invaluable in combating cyber threats and safeguarding digital environments. With the cybersecurity industry rapidly expanding and becoming critical across all sectors, veterans are uniquely positioned to thrive, especially with the right certifications and practical experience.

As the digital world continues to expand, the demand for cybersecurity professionals will only grow, offering veterans an opportunity to protect critical systems and contribute to the safety of organizations and individuals alike. With the right guidance, resources, and determination, veterans can build successful and impactful careers in the cybersecurity domain. Whether through roles in network security, incident response, or ethical hacking, veterans have the opportunity to protect critical infrastructures and contribute to global security in new ways. As they step into this domain, the expertise they gained in the military will serve as a solid foundation for building rewarding careers in one of the fastest-growing and most impactful industries today.



Anish Jairath is currently pursuing his undergraduate degree in Journalism at the University of Regina, aiming to leverage his strong research and writing skills to excel across various media platforms, including print, television, and online social media. Anish's goal is to seamlessly integrate his capabilities to create compelling content that engages audiences across different mediums. He is committed to staying updated with the latest trends and technologies in journalism and media, as he understands the importance of adaptability in this ever-evolving industry. By developing skills in digital storytelling, data journalism, and multimedia production.

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor

Theme Article

Demystifying Cybersecurity Domain as a Career for Transitioning Military Personnel: My Journey and Learnings

BY ASHISH CHAUHAN

Transitioning from military life to the civilian workforce presents both exciting opportunities and significant challenges. When I left the armed forces, I was eager to find a career that would allow me to leverage my leadership skills, discipline, and mission-driven mindset developed while being in the forces. After exploring several options, I chose the field of physical security, and later migrated to cybersecurity - a domain which is futuristic, scalable and that aligned with my skillsets developed during and post my army career.

In this article, I'll share my journey and learnings as a military veteran who transitioned into cybersecurity. I'll also provide practical advice for veterans considering a similar path and offer insights into why this field is an excellent career choice in today's world.

Why Cybersecurity?

Cybersecurity is one of the fastest-growing and most essential fields in the modern world. The digital landscape has evolved rapidly, and with it, so have the threats facing governments, businesses, and individuals. The numbers tell the story:

- **A Global Shortage of Talent:** According to the (ISC)² 2023 Cybersecurity Workforce Study, there is currently a shortage of over 3.4 million cybersecurity professionals worldwide. This massive gap in talent means that organizations across industries are urgently seeking skilled professionals to protect their systems and data.
- **Cybercrime Costs Are Soaring:** Cybercrime is projected to cost the world \$10.5 trillion annually by 2025, according to Cybersecurity Ventures. These staggering costs are driving limitless demand for cybersecurity solutions across every sector, from finance to healthcare and government.
- **Increased Attack Surface:** With the rise of remote work, cloud computing, and IoT devices, the attack surface has expanded significantly. A 2023 report by IBM noted that data breaches cost organizations an average of \$4.45 million per incident, making cybersecurity investments a critical business priority.

For veterans transitioning to civilian careers, this creates a wealth of opportunity. The skills developed in military service like, strategic thinking, risk management, and leadership under pressure are all directly transferable to cybersecurity roles.

Lessons from My Transition

- **Understanding the Industry Landscape:** One of the first things I did was take time to understand the breadth of the cybersecurity domain. From ethical hacking and penetration testing to governance, risk management, compliance and incident response, there are many career paths within cybersecurity. Veterans should identify the roles that align best with their skills and interests.
- **Beginner-Level Certifications:** If you're new to the cybersecurity domain, certifications are an excellent way to get your foot in the door. Some entry-level certifications to consider include – CompTIA Security+, Certified Ethical Hacker (CEH), ISC2 Certification for Cybersecurity, etc.
- **Certifications for Veterans with Cybersecurity Experience:** If you worked in a military role related to cybersecurity, you might already have hands-on experience with network defense or cyber operations. In that case, consider pursuing certifications like Certified Information Security Manager (CISM), Certified Cloud Security Professional (CCSP), Certified Information Systems Security Professional (CISSP), which will acknowledge your expertise.
- **Transferable Skills Matter:** While cybersecurity may seem highly technical, veterans bring a set of core competencies that are invaluable to the field. These include:
 - **Risk Assessment:** Military operations often involve managing and mitigating risk under high-pressure situations. This translates directly into cybersecurity, where threat identification and risk management are critical.
 - **Leadership and Communication:** Leading a cybersecurity team or responding to a breach requires strong leadership and clear communication. Veterans, especially those in command or leadership roles, have experience making quick, high-impact decisions under pressure.

The cybersecurity landscape evolves rapidly. What I found early in my transition was that continuous learning is non-negotiable. Cybersecurity professionals must constantly update their knowledge to stay ahead of emerging threats. Enrol in courses, attend conferences, participate in forums, and stay curious about new technologies and threats.

Closing Thoughts

As a veteran myself, I understand the challenges of transitioning into a civilian career. Cybersecurity offers a dynamic and rewarding field for veterans to leverage their unique skill sets while continuing to serve a mission of protection and defense.

The demand for cybersecurity professionals is greater than ever, and veterans are uniquely equipped to meet that demand. Whether you're just starting with beginner-level certifications or leveraging your military experience for advanced roles, the cybersecurity field is rich with opportunities for growth and impact.



Major Ashish Chauhan (Retd) is the Founder and Strategic Business Officer of UniSense Advisory, a consulting firm specializing in all kinds of cybersecurity solutions. He is a distinguished veteran with over 02 decades of rich experience in business advisory, corporate risk and assurance leadership and entrepreneurship. Having in-depth knowledge of various global industry standards across cyber security, data privacy and business continuity (including ISO 27001, ISO 22301, ISO 9001, ISO 45001, EU GDPR, etc), Major Ashish has established himself as a trust worthy professional in the industry. he can be reached at ashish.chauhan@unisenseadvisory.com

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor

An advertisement for GOGETSECURE featuring a person's hands holding a glowing blue shield with a padlock icon. The background is dark with digital elements like binary code and icons. The text is in white and light blue.

 **GOGETSECURE**

“Security used to be an inconvenience sometimes, but now it’s a necessity all the time.”

- Martina Navratilova

Theme Article

IS A CAREER IN CYBERSECURITY MEANT FOR VETERANS

BY ATUL KUMAR



Military personnel thinking of transition must very clearly and thoughtfully analyse their reasons for such a change. One is not so sure of being able to come up to expectations of a civil career requirements. While monetary situation is not worrisome due to retirement funds - unless one has family responsibilities, one is apprehensive about the surety of job and salary post such transition. You must take the plunge only if you are clear what do you want to do in second career and be equipped for that role / vertical / industry with qualifications, experience and connects. Ask yourself where you want to be after five years in corporate - in which industry vertical doing what role. According to identified core competency and having obtained suitable qualifications for that would pave the way for preparation of CV / Resume. Keep in mind that your medals, battle performance reports and course grading are not relevant in civil job. Most of the officers make the mistake of writing long and armed forces-oriented experiences in the CV which is not desired. So, Role fitment is the primary task one should do before PMR / Superannuation.

To succeed in any organization, it is extremely important to be truthful to yourself. While in armed forces we do become Jack of All trades and are made to perform all kinds of jobs from operational to administrative to financial to event management. However, in heart of our hearts we do know the domain in which we are good and can excel. It is thus most important to identify that Core Competency in yourself and work towards improving your theoretical and practical knowledge as well as network in that domain. This will assist you in your career progression within armed forces as also facilitate transition to a best fit role in most suitable industry vertical / horizontal when moving to corporate world.

One field that presents an exciting opportunity is cybersecurity. With increasing cyber threats and a growing demand for skilled professionals, cybersecurity offers veterans a chance to apply their skills in a dynamic and vital sector. The cybersecurity industry is rapidly expanding due to the rising threat of cybercrime, which affects individuals, businesses, and governments alike. According to an estimate, there is expected to be 3.5 million unfilled cybersecurity jobs globally by 2025. The field's dynamic nature and continuous demand for skilled professionals make it an attractive option for veterans looking to transition into a meaningful and stable career. So, should you consider a second career in cyber security port you PMR / superannuation from armed forces? Is it meant only for "Techies" like personnel from Corps of Signals or AEL and Engineering branch or "non-techies" from supporting arms and services can also make it big in the cyber security domain? To understand and declutter your mind from all the technical mumbo jumbo read on.

What and Why Cyber Security?

Cyber or Computer Security is the protection of computing systems and the data that these systems store or access. These systems include PC's, Laptops, Smart Phones, Mobile Devices, Network Devices, Security Devices, Communication Devices and Printers etc. Cyber Security can be categorized into sub domains like Network Security, Application Security, Data Security, Operational Security, Mobile Security, Cloud Security, BCP & DR and User Education.

Nearly every industry takes cybersecurity measures to protect itself from leaks and breaches. Cybersecurity professionals may work with government organizations to safeguard military communications or with businesses to keep malicious actors from accessing financial records. Healthcare companies also use cybersecurity workers to protect their sensitive patient data. Large retailers shield customers' credit card data with cybersecurity measures as well. Similar examples of cybersecurity measures exist across every industry.

As humans have become more reliant on technology, the prevalence and severity of cybercrimes have grown. Cybercrime is an increasingly serious problem - a term which includes all the unlawful acts, wherein the computer is either the tool used in an attack or the target of an attack or used to store data related to criminal activity. In 2023, cybercrime cost the world \$8 trillion which will increase to \$10.5 trillion by 2025.

Cybersecurity intrusions have become a major problem, and cybersecurity professionals are needed to step up the defence. Only 10% of security safeguards are technical in nature and the rest 90% of safeguards rely on People i.e. each of us. Professionals in this field study breaches and malicious actors to safeguard our most sensitive information and communications. Since cybersecurity involves the protection of information and data on computers, networks and electronic devices, the cybersecurity professionals anticipate, prevent and respond to attacks on these devices.

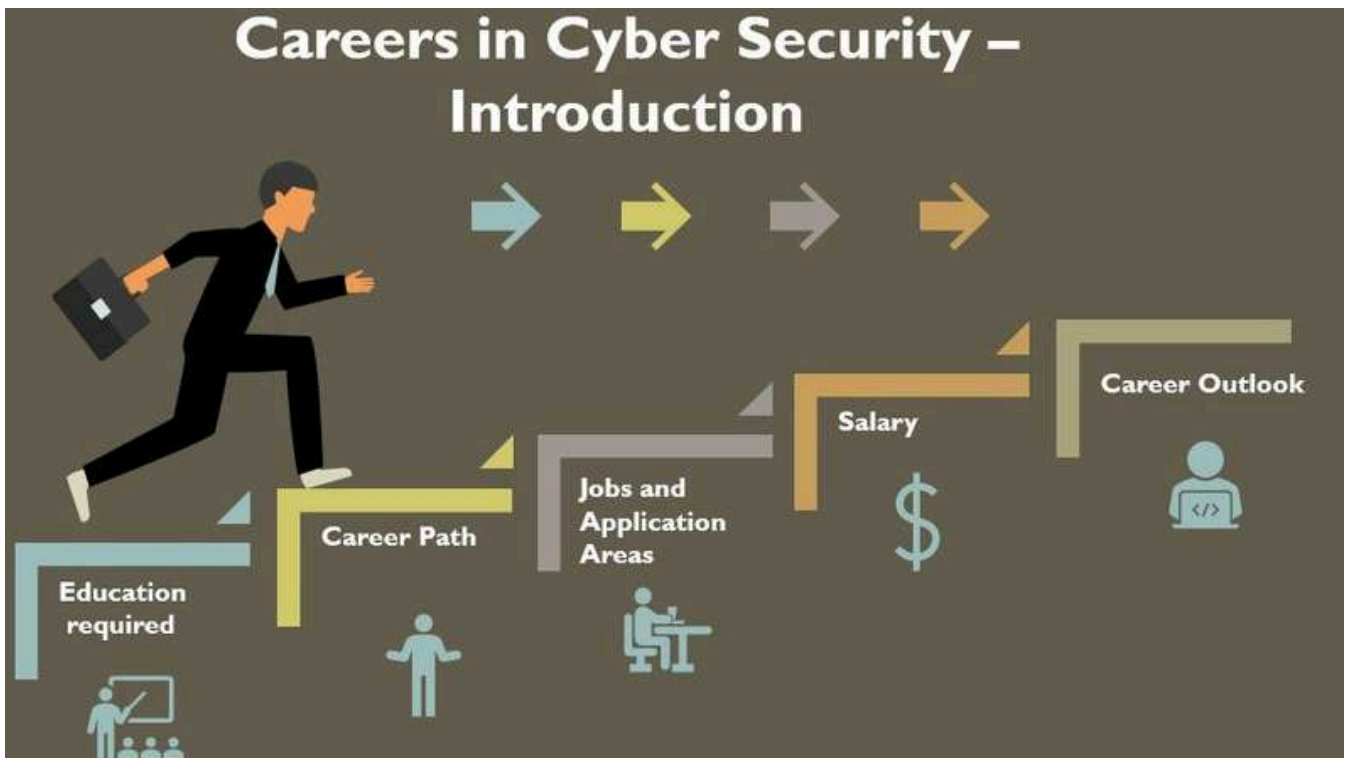


What Do Cyber Security Professionals Do?

Cybersecurity consultants fight the never-ending battle against the bad guys – malicious hackers – in what is effectively a race. At the most fundamental level, cyber security consultants make the Internet and corporate networks safer places. They plan, design, build, configure, code, run, maintain, and/or monitor security controls meant to protect data and networks from being breached.

Security consultants take actions to make it difficult for anyone to gain unauthorized access to data or network devices and to do harm. There is almost no limit to the number of ways to do so. They fall into the general categories of prevention, detection, and response. Security consultants who handle prevention may plan, build, and configure security controls, while those who handle detection and response may code and monitor. To clarify with an example a 'Security Architect' handles prevention against attacks in the future by assessing the existing security controls and design a new set of controls that would be more effective – e.g. making mandatory multi-factor authentication for all administrator accounts (i.e. needing in addition to password authentications like an OTP). Another example could be a 'Security Administrator' who works on detection by setting up security monitoring to detect suspicious attempts to access systems e.g. configuring stricter access rules on the firewall. Lastly, an example could be of an 'Incident Responder' who focuses on responding to security breaches, analysing the nature of the threat and implementing measures to prevent recurrence e.g. after a Ransomware attack understand the access provided to the attacker say through a phishing e-mail and institute measures for spam filters and organising refresher training & workshops for all employees to create awareness against phishing.

Now this may sound as very technical nature of job for a non-tech veteran. While there are essentially no 'non-tech' armed forces personnel these days with the kind of technology-based operations being undertaken in war and peace some of the roles may require education and experience in IT field while some roles can be performed by veterans with non-IT background. So, what are these roles in the field of cyber security? Let's look at them.



Spectrum of Roles in Cyber Security Domain

Typical Career Pathway in Cybersecurity is threefold – Entry Level, Mid-Level and Senior / leadership positions.

In Entry-Level roles professionals focus on monitoring networks for security breaches, responding to incidents, and performing basic threat analysis. These could be: -

- Security Operations Centre (SOC) Analyst
- Penetration Tester
- Information Security Analyst

Information Security Analyst would probably need a degree in IT / CS / Cyber Security. Information security analysts protect an organization’s computer networks, systems and databases from cyberattacks, data breaches and other threats. These professionals monitor information networks and computer infrastructure to identify vulnerabilities in digital security systems and secure sensitive information and data.

Mid-Level positions involve more responsibility, including conducting vulnerability assessments, investigating security incidents, and designing security systems. With experience, individuals can progress to more specialized roles, like: -

- Information Security Manager
- Digital Forensics Analyst
- Security Engineer

Information Security Manager is educated with degree in IT/CS/Cyber Security or has requisite certifications like CeH, CHFI or CISM. Cybersecurity / Information Security Managers are responsible for securing an organization’s computer networks and systems and protecting organizations from cyberattacks, hackers, viruses, malware and other threats. These professionals carry out security measures, update current security systems and conduct regular audits to ensure compliance with relevant regulations. Information security managers train and supervise staff and collaborate with operations managers on their organization’s security strategy.

Senior and Leadership positions require not only technical skills but also a strategic understanding of risk management, business operations, and compliance. Experienced professionals can move into senior roles such as: -

- Senior Security Consultant
- Security Architect
- Chief Information Security Officer (CISO)

Another matrix to look at the spectrum of roles in cyber security career is through the skills set needed for role fitment. These can be divided into following five types: -

- **Engineering and Architecture**

Security engineering and architecture could be a good fit if you enjoy tinkering with technology and like to take a big picture approach to cybersecurity. As a security engineer, you'll use your knowledge of threats and vulnerabilities to build and implement defence systems against a range of security concerns. You may advance to become a security architect, responsible for your organization's entire security infrastructure. Critical thinking, IT networking, system administration and risk assessment are key skills to have for this range of roles. Veterans who have experience in signals intelligence or communications can find this path particularly fitting.

- **Incident Response and Forensics**

Incident response could be a good fit if you work well under pressure and love a good mystery. Despite a company's best security efforts, security incidents still happen. The field of incident response involves the next steps after a security incident. As an incident responder, you'll monitor your company's network and work to fix vulnerabilities and minimize loss when breaches occur. Another area of incident response involves digital forensics and cybercrime. Digital forensic investigators work with law enforcement to retrieve data from digital devices and investigate cybercrimes. Key skills are attention to detail, technical writing and documentation, intrusion detection tools and forensics software. . Veterans accustomed to high-stress situations can thrive in this role, where timely and decisive action is critical.

- **Management and administration**

Management and administration could be a good fit if you're organized, an excellent communicator, and enjoy working with people. As you gain experience in cybersecurity, you may choose to advance toward a leadership position within your organization. Cybersecurity managers oversee an organization's network and computer security systems. In this role, you might manage security teams, coordinate between teams, and ensure security compliance. Typically, the highest security role in an organization is that of chief information security officer (CISO). Working in security at the executive level often means managing operations, policies, and budgets across the company's security infrastructure. Project management, risk management, leadership and collaboration are the needed key skills. Veterans with leadership experience may find this role appealing, as it involves managing projects and making strategic recommendations.



- **Consulting**

Consulting could be a good fit if you enjoy variety and want to make an impact by helping others manage their security. Companies hire security consultants to test their computer and network systems for any vulnerabilities or security risks. In this role, you get to practice cybersecurity offense and defence by testing systems for vulnerabilities and making recommendations on how to strengthen those systems. Key skills to have are penetration and vulnerability testing, threat management, operating systems and encryption.

- **Testing and hacking**

Testing and hacking could be a good fit if you want to outsmart the bad guys and get paid to (legally) hack into networks and computer systems. This field of cybersecurity goes by many names, offensive security, red team, white hat hacking, and ethical hacking among them. If you work in offensive security, you'll take a proactive approach to cybersecurity. You'll do this by playing the part of the intruder, trying to find vulnerabilities before the bad guys do. As a penetration tester, you'll seek to identify and exploit system weaknesses to help companies build more secure systems. As an ethical hacker, you can try out even more attack vectors (like social engineering) to reveal security weaknesses. Cryptography, penetration testing, computer networking and scripting are key skills for this type of role. Veterans with a background in military intelligence or electronic warfare may find their analytical skills and strategic thinking align well with penetration testing.

Veterans's Requisites for a Career in Cyber Security

Veterans possess unique qualities that align well with cybersecurity roles, such as:

1. **Discipline and Work Ethic:** The military instils a strong sense of discipline and responsibility. Cybersecurity jobs often require vigilance, perseverance, and an unwavering commitment to continuous learning, all traits commonly found in military personnel.
2. **Problem-Solving Skills:** Military roles frequently require quick thinking and problem-solving under pressure, which are essential skills in cybersecurity for incident response and threat management.
3. **Teamwork and Leadership:** The ability to work effectively in teams and lead others is a crucial part of military training. Cybersecurity also relies on teamwork, whether coordinating a defence strategy or investigating an incident.

However, before you apply for your first cybersecurity role, take some time to develop core skills, including networks and systems administration. While you don't necessarily need a degree to get a job in cybersecurity, having some form of structured training might accelerate your path toward a job. While a degree in computer science, information technology, or a related field can be beneficial, it is not always required. Practical experience and certifications can be just as valuable. You need to start preparing for a career as a security consultant by learning about Networking basics and Cybersecurity basics. An additional effort to learn coding and/or scripting and practical Hands-on experience will be good for better prospects.

Key skills needed in cybersecurity domain are: -

- **Technical Skills**

- **Networking and System Administration:** Understanding networks, operating systems, and how data flows through an organization is needed.
- **Programming:** Knowledge of coding languages such as Python, C++, or JavaScript helps in automating tasks and understanding malware behaviour.
- **Digital Forensics:** Skills in recovering and investigating data from computer systems can help identify the source and nature of an attack.

- **Non-Technical Skills**

- **Problem-Solving:** Cybersecurity requires finding creative solutions to complex problems.
- **Attention to Detail:** Identifying potential vulnerabilities often involves scrutinizing large amounts of data and configurations.
- **Communication:** The ability to explain technical concepts to non-technical stakeholders is critical, especially when discussing risk.

Certifications are an essential component of a cybersecurity career, often providing the foundational knowledge and skills necessary to get started. There are many cybersecurity certifications to choose from and you never know which a potential employer will value. There are free courses online for some certifications but the exams themselves are very expensive. Many companies will pay employees for additional training and certification. Some popular certifications not requiring IT or CS degrees are CompTIA Security, Certified Ethical Hacker (CEH), Certified Information Security Manager (CISM) and Computer Hacking Forensic Investigator (CHFI).

Look into the Crystal Ball

So, what to do if this field excites you as a career option after military service or even if you wish to pivot in your corporate career.

- Firstly, do a Self-Assessment. Assess your skills, interests, and strengths. Are you more inclined towards analysing data, ethical hacking, or strategic planning? Understanding your preferences will guide your career choice.
- Secondly, invest time in acquiring relevant education and certifications. Entry-level certifications like CompTIA Security+ provide foundational knowledge, while specialized certifications can further enhance your expertise.

- Next expand your networking. Join cybersecurity communities, attend conferences, and connect with professionals in the field. Networking provides insights into different roles, trends, and opportunities. Many veterans who have successfully transitioned into cybersecurity are willing to guide others. Mentorship programs can provide insight into career paths, help navigate certifications, and offer advice on job search strategies.
- Next gain hands-on experience through internships, projects, or volunteering. Practical exposure is invaluable in developing the skills required for specific roles.

Conclusion

For veterans, a career in cybersecurity not only offers a sense of purpose but also leverages their unique skills in a new arena. The path may require some training and certification, but with the right support and resources, veterans can successfully transition to this growing and rewarding field. Cybersecurity provides an opportunity to continue serving the nation, albeit in a different capacity—protecting against digital threats rather than physical ones. A career in cybersecurity is rewarding,

offering excellent job security, competitive salaries, and the chance to work on cutting-edge technologies. With diverse pathways ranging from technical roles to managerial positions, there is a fit for almost anyone interested in the field. Continuous learning, hands-on experience, and a proactive approach to understanding emerging threats are key to thriving in this dynamic industry.



Col (Dr) Atul Kumar, psc was commissioned in AOC in June 1988. Qualified AATO, he is an alumnus of DSSC Wellington and possesses Masters in Science, Computers and Business Management as well as Doctorate in Strategic Studies. He was awarded COAS and VCOAS Commendation Cards for contribution in the field of ERP implementation in the Army and is recipient of Brig Panna Chatterjee trophy (twice) and Brig Rodrigues Trophy. Post his army career he has worked in Deloitte India as Director Enterprise Technology for 3 years and as Principal Consultant in Boston Consulting Group for a year. He has co-chaired National Conference on Fintech and Cyber Laws at National Law University Delhi and on G20 Workshop on Cyber Security Initiatives in IMT. He was also a Panelist in Round table conference on India's preparedness for cyber security as part of G-20 Presidency in New Delhi. He is a visiting guest faculty at colleges like IIMB, IMT, PGLS, CMM, BVP, NLU and JIMS and a member of Confederation of Indo-Russian Technical Collaboration (CIRTC). Currently he is CEO of a Cyber Security company in NOIDA besides working as an Advisor Digital Transformation in NCRTC Delhi.

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor

Theme Article

The Basics of Cyber Security; and Transitioning into Cyber-Security as a second career

BY SAM ARMSTRONG KAPPALA



These statistics highlight the critical importance of cyber security in today's digital world. The increasing frequency and sophistication of cyberattacks underscore the need for robust security measures and skilled professionals to protect sensitive information and systems.

Let us review our personal practices....

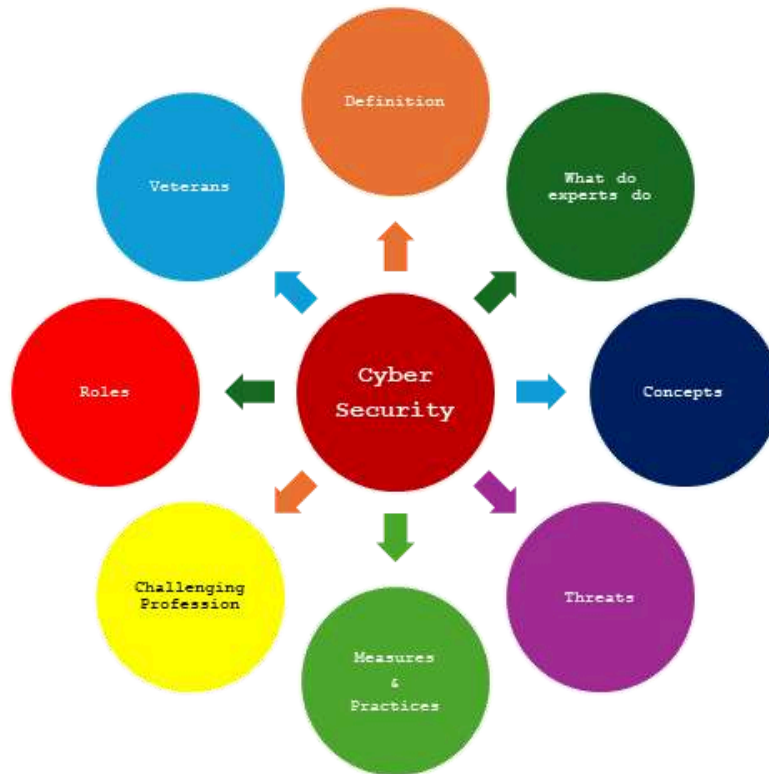
- Do you have a password for your wi-fi at home?
- Do you have password/pattern/numeric lock/fingerprint scan / facial recognition to open your mobile – albeit to safeguard your secrets and content from your spouse?
- Do you update your anti-virus regularly on your devices?

OR

- Are your passwords known to your colleagues and people around you?
- Do you keep your laptop on and open when you are not using it?
- Are your passwords easily guessable?

If the answer to any of the questions in the first set is a “YES” and/or a “NO” to the next, bingo !!!!! you unconsciously implement one/few of cybersecurity measures.

Through this write-up I would like to run through the basics of cyber-security and how it can be a career option for the second innings.



1. WHAT IS CYBER-SECURITY

Cyber security is the practice of protecting IT systems, networks, programs and applications from digital/cyberattacks. These cyberattacks are usually aimed at unauthorized accessing, changing, or destroying sensitive information, extorting money from users, or interrupting normal business processes.

2. WHAT DO CYBERSECURITY EXPERTS DO

Cybersecurity experts try to restrict the access to its authorized users only. They do so by finding weaknesses in the system’s security which the attackers could exploit and informing the user to get it rectified.

3. CYBER SECURITY CONCEPTS (cybersecurity triad) : CIA

Concept	Definition	Examples (you have an ATM card linked to your bank account)
Confidentiality	Ensuring that information is accessible only to those authorized to have access.	Only you should be able to use the ATM card at the ATM and not any unauthorised person.
Integrity	Maintaining the accuracy and completeness of data.	If your account has a balance of 50,000/, the machine should show the correct numbers and not incorrect balance.
Availability	Ensuring that authorized users have access to information and resources when needed.	You should be able to withdraw from your account and access all the services that are your card authorises AT ANY TIME OF YOUR CHOOSING.

**Ensure CIA and you will a cybersecurity expert.
However, it appears as simple as it is complicated.**

4. What are the threats to having a robust CIA. In tech terms, these are called cyberthreats. Few of them are:

Type of threat	Definition	How does it work	Effects of infection
Malware	Malicious software such as viruses, worms, and trojans designed to damage or disrupt systems.	<ul style="list-style-type: none"> · Infection · Execution · Propagation 	<ul style="list-style-type: none"> · Inability to boot · Data loss · Network disruption
Phishing	Fraudulent attempts to obtain sensitive information by disguising as a trustworthy entity.	Email phishing <ul style="list-style-type: none"> · Spoofing · Urgent Request · Link or attachment 	Email impersonates a legitimate sender, may have sense of urgency, or contain a malicious link or attachment.
		Spear phishing <ul style="list-style-type: none"> · Targeted attack · Personalised Information 	Sophisticated form of phishing targeting specific individuals or organizations. Target's personal information is gathered and shared to appear legitimate.
		Smishing <ul style="list-style-type: none"> · SMS Phishing · Short and urgent 	Phishing attack using SMS or text messages and also involves urgency.
		Vishing <ul style="list-style-type: none"> · Voice Phishing · Impersonation 	Phishing attack using voice calls or voice mails impersonating a trusted individual, agency or organization.
Ransomware	A type of attack through which the data/ systems of victim is encrypted or made inaccessible till ransom is paid.	Using malware / phishing attacks as above, exploiting vulnerabilities, public wi-fi, removable media	Files / data encryption, Ransom note Data Theft
Denial of Service	Disrupting the normal operations of a network, system, or website by overwhelming it with excessive traffic or malicious requests.	Flood attack HTTP Flood Ping Flood Slowloris attack Distributed Denial of Service	https://en.wikipedia.org/wiki/Denial-of-service_attack

5. Having seen how the attacks can happen, let us look at common cybersecurity measures and best practices.

Cybersecurity measure	Definition
Firewalls	Network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules.
Encryption	The process of converting information or data into a code to prevent unauthorized access.
Multi-factor authentication (MFA)	A security system that requires more than one method of authentication to verify the user's identity.

Best Practices for Cyber Security

- **Strong Passwords:** Complex passwords are difficult to guess and frequent change is ideal.
- **Security Software:** Antivirus and anti-malware software to be installed and maintained to protect against threats.
- **Updated Software:** Regular software updates protect against latest threats.
- **Suspicious Emails and Links:** Awareness and Avoidance of clicking on links or downloading attachments from unknown sources is a pro-active practice.
- **Regular Backup of Data:** Important data must be backed up regularly to prevent loss in case of an attack and be able to restore to nearest possible correctness of data.

6. CYBERSECURITY - A CHALLENGING PROFESSION

Cybersecurity is a challenging profession due to several factors:

- **Constant Evolution:** The digital landscape and threat actors are constantly evolving. New vulnerabilities, attack methods, and malware emerge daily, requiring cybersecurity professionals to stay up-to-date with the latest trends and technologies.
- **Complex Landscape:** Cybersecurity encompasses a wide range of technologies, protocols, and systems. Professionals must understand and manage a complex ecosystem, from networks and databases to cloud infrastructure and IoT devices.
- **High Stakes:** Cybersecurity breaches can have severe consequences, including financial losses, reputational damage, and legal implications. The pressure to prevent and mitigate attacks is immense.
- **Skill Shortage:** There is a significant global shortage of skilled cybersecurity professionals. This can lead to increased workload, stress, and difficulty in finding qualified talent.
- **Ethical Dilemmas:** Cybersecurity professionals often face ethical dilemmas, such as balancing privacy concerns with security needs or deciding how to handle sensitive data.

- **Stressful Environment:** The nature of the work can be demanding and stressful. Cybersecurity professionals may work long hours, deal with high-pressure situations, and experience burnout.

While the profession is challenging and demanding it is very rewarding for those who are passionate about protecting digital assets.

7. Top Cyber Security Roles (Col Iqbal has detailed these earlier in 2023).

- **Lead Software/Cyber Security Engineer:** Responsible for designing and implementing security measures to protect an organization's computer networks and systems
- **Chief Information Security Officer (CISO):** Oversees the organization's entire information security strategy.
- **Ethical Hacker / Penetration Tester:** Identifies vulnerabilities in systems and networks by simulating cyberattacks.
- **Information Security Analyst:** Monitors and analyzes security systems to detect and respond to security breaches.
- **Cyber Security Architect:** a strategic thinker and technical expert responsible for safeguarding an organization's digital assets.
- **InfoSec Forensic Expert (Digital Forensic Analyst / Computer Forensic Investigator):** A specialist who examines digital evidence in legal investigations. They play a crucial role in recovering, preserving, analyzing, and presenting digital evidence in a way that is admissible in court.

8. VETERANS INTO CYBERSECURITY: WHY AND HOW

As the digital landscape continues to evolve, the demand for skilled cyber security professionals has surged. For veterans, transitioning to a career in cyber security offers a unique opportunity to leverage their military experience in a new and dynamic field. As we have seen at the beginning of this article, the infosec jobs are projected to grow at 32% till 2032 and the shortage of skilled cybersecurity professionals is evident.

Let us look at why cybersecurity suits veterans' transition as a second career.

1. **High Demand and Job Security:** With the increasing frequency of cyber threats, organizations across the globe are investing heavily in cyber security. This has created a robust job market with a high demand for skilled professionals, ensuring job security and competitive salaries.
2. **Transferable Skills:** We veterans possess a range of skills that are highly transferable to cyber security roles. These include discipline, attention to detail, problem-solving abilities, and a strong understanding of security protocols. Their experience in handling classified information and understanding of threat landscapes can be particularly valuable.
3. **Mission-Oriented Mindset:** The mission-oriented mindset ingrained in us aligns well with the objectives of cyber security. Protecting an organization's digital assets requires a similar level of dedication, strategic thinking, and a proactive approach to identifying and mitigating threats.

Steps to get in to Cybersecurity roles :

- **Educational Background:** While military experience provides a strong foundation, obtaining relevant education and certifications is crucial. A degree in computer science, information technology, or a related field is often required. However specialised programs such as Certified Information Systems Security Professional (CISSP), Certified Ethical Hacker (CEH), and CompTIA Security+ are highly regarded in the industry. Importantly, as our IQ sir reiterates time and again – **ANYONE CAN TECH – but the catch is, that it requires upskilling and experience is a must.**
- **Leverage Military Networks:** Veterans can benefit from leveraging their military networks to find opportunities in cyber security. Many organizations value the unique perspective and skills that veterans bring and may have specific programs to support their transition.
- **Practical Experience:** Veterans can seek internships, volunteer opportunities, or entry-level positions to gain hands-on experience. Participating in cyber security competitions and joining professional organizations can also be beneficial.

Sustaining a Cybersecurity career :

- **Continuous Learning:** The field of cyber security is constantly evolving. Hence one should commit to continuous learning to stay updated with the latest technologies, threats, and best practices. Online courses, workshops, and attending industry conferences can help in this regard.

Support and Resources

- **Government Initiatives:** The Indian government and several state governments have launched initiatives to support veterans in their career transitions with courses in cyber security.
- **Veteran Support Organizations:** Numerous organizations provide resources and support specifically for veterans. These include mentorship programs, job placement services, and networking opportunities tailored to help veterans succeed in their new careers. The Indian government has launched various initiatives to promote cyber security education and training. Programs like the National Cyber Security Policy aim to build a skilled workforce in this domain.
- **Corporate Programs:** Many corporations have veteran hiring programs that focus on integrating veterans into their workforce. These programs often include training, mentorship, and career development opportunities in cyber security.
- **Professional Organizations:** Joining professional organizations such as the Information Systems Audit and Control Association (ISACA) and the International Information System Security Certification Consortium (ISC)² can provide networking opportunities and access to resources.

CONCLUSION

For veterans of the Indian Armed Forces, a career in cyber security offers a promising and fulfilling path. By leveraging our experience in uniform, obtaining relevant education and certifications, and utilizing available resources, we can successfully transition into this high-demand field. The skills and dedication that served us well in the forces can be equally valuable in protecting the digital frontiers of today's world.

(Cdr Bheem Reddy, IN, is offering excellent training in CyberSecurity through his start-up company at a reasonable cost. He can be contacted at +91-7058790268)

Ser No	Role	Published in ForceNet Issue	Remarks	URL
1	Cyber Security An Ideal Career Choice For veterans	Dec-22	Pg Nos 23-34	https://www.forces-network.com/_files/ugd/74ad35_2c79fe940d34c4c91415e6d982ab5d6.pdf
2	Intro to SOC Analyst	Jan-23	Pg Nos 49- 57	https://www.forces-network.com/_files/ugd/74ad35_2f1ff77293d54b0d9b20a5620891e452.pdf
3	Penetration Tester role in Cyber Security	Feb-23	Pg Nos 57- 65	https://www.forces-network.com/_files/ugd/74ad35_e87eac3907a84725baa241fc607282e5.pdf
4	Cyber Security Career Digital Forensics	Mar-23	Pg Nos 50- 58	https://www.forces-network.com/_files/ugd/74ad35_c4d1b77a074448d2aa7c87824f2045e0.pdf
5	Information Security Manager	Apr-23	Pg Nos 36-42	https://www.forces-network.com/_files/ugd/74ad35_17176d19bda3445ab9256814a0545353.pdf
6	Application Security Engineer	May-23	Pg Nos 31-38	https://www.forces-network.com/forcenetazine
7	Chief Information Security Officer (CISO)	Jun-23	Pg Nos. 75- 82	https://www.forces-network.com/_files/ugd/74ad35_4b271d048e0d42c285a7f9c834522c0a.pdf



Capt Sam Armstrong Kappala is an alumnus of Officers' Training Academy, Chennai, commissioned from SS-57th batch into the Army Air Defence. Having joined 126 Lt AD Regt (Comp), Sam spent most of his short tenure in J&K including the Siachen Glacier. Post uniformed service, he served in the banking security for seven years and currently responsible for security and risk management for Hitachi Digital (a Hitachi group company) for its offices in the Asia Pacific. With security management skills being imbibed from the Army days, numerous trainings and certifications, especially in ISO-27001 increased his interests in Risk Management. Apart from his regular chores, Sam plays active part in Business Continuity and Crisis Management Teams.

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor



SAFEGUARD BENEFIT*

**SENIOR
—FIRST—**
A PROMISE OF LOVE

AN ADDITIONAL LAYER OF PROTECTION FOR YOUR SENIORS
THAT PROVIDES **COVERAGE FOR EVEN NON-PAYABLE ITEMS.**

**Colonel R Srinivas (Retd),
Director Galaxy Associates and Business Partner Niva Bupa Health
Insurance Company.
Including Foreign Travel Insurance
Mob No :- 7400160159
Mail ID :- GAGBHAVANA@GMAIL.COM**

Survey: Members Speak

As you know ForceNet E-Zine is the monthly e-magazine of the Forces Network- the network of military veterans in the corporate. We produce a specialized theme each month; for this issue, we chose, Demystifying Physical Security Vertical.

We sourced our content from veterans who are thriving in the field of Physical Security themselves. The next few pages are dedicated to a few randomly picked veterans in their own words.

Here are the questions we asked them:

1. While in the military we do security throughout our lives. However when we hear about cyber security most of us develop cold feet saying I am non technical I do NOT know this. But in reality the concept of security remains the same only the domain changes from the physical to a virtual one. What are the concepts of physical security which are also applicable in cyber security?
2. Having worked in Cyber Security now do you think that even a non tech officer can take up a career in cyber security provided he or she does some up-skilling? Also there is a continuum of roles ranging from semi-tech, process oriented to hard core tech. What are the little technical domains that can serve as a good entry point for such officers?
3. What are the various subdomains in the Cyber Security vertical which you could recommend to transitioning military personnel as a good fit based on your exposure in the sector. Also suggest some industries?
4. What would be your advice to military personnel aspiring for a career in cyber security with regards to acquiring qualifications, certifications, skills, etc?
5. Does the salary in the cyber Security vertical also vary from industry to industry? Which typically are the high paying industries?
6. Why is cyber security is something that every industry needs to adopt. What are the 3 factors forcing even brick & mortar companies to invest in cyber security?
7. What are the three things you like about being in the Cyber Security function?
8. What are the three things you do NOT like about being in the Cyber Security function?



Unisense Advisory Ashish Chauhan

Army/Infantry/ Maratha LI, DOR:
2006 Years in Corporate: 17 years

Founder and Business Officer,
Unisense Advisory

Importance of Cyber Security?

1. Every industry is transforming to digitisation thus creating a digital self.
2. Machines even in manufacturing companies are smart, automated, remote controlled, IOT connected with internet thus susceptible to cyber-attacks.
3. With the advent of AI, the attack vector along with the impact is changing at a drastic speed.

Your Perception?

There are many common principles to both physical and cyber security, however I will highlight 4:

1. Risk Management: To identify, assess, evaluate and manage by implementing the relevant controls is foremost for both physical as well as cyber security domain.
2. Access Control: Unauthorised access is controlled by guards, gates and proximity cards in physical security. Same is applicable in cyber security to identity management using 2 factor or MFA (multi-factor authentication) protocols.
3. Surveillance: CCTV cameras for physical security to detect and respond to any incident and VAPT (vulnerability assessment and penetration testing), network monitoring etc are used in cyber security.
4. Emergency/Incident Response: In both physical security as well as cyber security, there is a need to respond effectively to any physical or cyber incident.

Cyber Security: Corporate versus Military?

Being from the non-tech background, I could chart a career for myself hence I believe any officer can build his/her career in this field:

1. One needs to identify his/her strengths and interests like if one wants to get into audit or one wants to be in the management. There are different set of certifications for each career line.
2. For non-tech or little tech person - audit and compliance is the easiest route. One can get oneself familiarized with many standards like ISO27001, ISO22301 etc. to start with.

Recommended Sub-domains?

For Non-Tech:

1. Risk Management
2. Compliance Management
3. Audit and Assessment
4. Privacy and Data Protection (to an extent)

For Tech:

1. Network Security
2. Cloud Security
3. Endpoint Security
4. Data Protection
5. Penetration Testing
6. Threat Hunting (Red Teaming)

Any Advice?

1. Start with relevant certification like CISSP, CISA, CISM, CRISC, CGEIT, CIPP etc
2. Go for a formal degree like Masters in Cyber Security, there are many masters programme available
3. Keep attending various forums, seminars, conferences to update oneself with the latest trends and upskill oneself accordingly
4. Take paid subscription of LinkedIn Learning, and keep completing relevant certifications.
5. Register in FutureSkill Prime by NASSCOM and enjoy many free courses.

Salary Variations?

Salary is dependent on many factors thus not restricted only to industry, however the more critical a sector the more budget is allocated to safeguard it.

3 things you like?

1. Helm of Affairs gives one an opportunity to know the organisation as a whole.
2. Consequence of data breach is huge, so safeguarding the infrastructure gives a different job satisfaction.
3. Loads of learning - as the tech changes so does the threat landscape and so is your learning curve.

3 things you don't like?

1. Always on your toes: You are the last line of defense
2. Very stressful: If you can't manage it, it's not your cup of tea
3. Administrative Challenges: Like management time and budget - since it is still considered a cost factor, it is a challenge for every CISO.

Additional Comments

Cybersecurity is very futuristic, scalable and promising given the changes in the technology space, evolving threats and improving regulatory frameworks and since everyone is moving to the digital space this career brings challenging yet rewarding future.



Lt Cdr Gaurav Saini

Navy, DOR: 2021

Years in Corporate: 3

Information Security Manager,
American Express

Your Perception?

1. Defence in Depth
2. Multilayered Security
3. Setting up a desired state of security
4. Continuous monitoring and alert system
5. Periodic audits to ascertain the desired state of security.
6. Principle of zero trust (if you trust, then verify again)
7. Never ignore the insider threat.

Recommended Sub-domains?

1. Governance Risk and Compliance is one domain where non techies can venture smoothly.
2. Other subdomains are also there but need little technical exposure though not unachievable.
3. Almost every industry is having this domain as one of the main operational wing, be it technological, telecom, Banking, FMCG, professional services etc.

Cyber Security: Corporate versus Military?

1. Yes, non techie can venture into this domain very comfortably as I have some team members who are even from law background and doing cyber security. 2. Your passion and will to something does the job. 3. Some skills can be acquired but they are not at all a road blocker.

Any Advice?

1. Reading and knowing things are important.
2. We have to convey the interviewer that we can really generate the revenue in the company by carrying out the work they are doing.
3. This will only happen when we study and get the required knowledge. Lot of easy resources are available online and I can also help in the same.

3 things you like?

1. A feeling of being in security function like armed forces career.
2. A sense of accomplishment when I contribute to secure ecosystem of my current industry.
- 3 Nice growth and leadership opportunities in this sector.

3 things you don't like?

Nothing as such

Importance of Cyber Security?

1. Security is important for every industry if they want to keep doing business and earning revenue.
2. Cyberattacks now a days are encompassing every industry and rather than losing revenue due to such attacks, it's better to invest a part of that revenue to safeguard such industries.

3 factors:

1. Security is important for uninterrupted business operations.
2. Security increases the customer trust in any industry.
3. Security ensure regulatory compliances and obviate any fines due to that.

Salary Variation?

1. Salary is generally good across the verticals in every industry as cyber security is now a requirement for everyone.
2. However, some niche skills are being paid nicely.



Cdr Vinayak Srimal

Navy, DOR: 2023

Years in Corporate:

1

SENIOR VICE PRESIDENT, INFORMATION
RISK MANAGEMENT, KOTAK MAHINDRA
BANK

Your Perception?

The 3 pillars: Confidentiality, Integrity and Availability of information assets remain common to both fields

Recommended Sub-domains?

Across the board, depending on skillset and experience...however, choose your verticals wisely and look to build in that for the long haul.

Any Advice?

1. Hands-on learning trumps certifications; it is respected in the industry.
2. ISO27001 as a foundational course and CISSP as an advanced certification would give adequate exposure

3 things you like?

1. The responsibility of doing the right thing.
2. No one is an expert as yet!
3. The pay

Cyber Security: Corporate versus Military?

1. Upskilling is a continuous requirement in cyber; its not a one-time effort. At a foundational level, understanding of a computer architecture and networks is crucial. because it gives an idea of how things can be broken.
2. Entry level roles related to these domains viz. network security and endpoint security could be explored

Salary Variation?

Yes it does, based on the industry and role...time and space also matter!

Importance of Cyber-Security?

In today's world, every company is an IT company..a digital presence in operations is a must. Since IT cannot do without security, hence the demand is across the board.

3 things you don't like?

1. Things move when sh*t hits the roof.
2. Do more with less.
3. Busy weekends.

Additional Comments?

Learning to code in Linux, Windows powershell opened a new dimension for me and gave me additional confidence...an exposure with IW teams was invaluable!

COURSE REUNION T-SHIRTS

Create memories for life...

- Individual Delivery
- Free Design Options
- Exclusive Defence Discounts

iLogo.in

**A VETERAN
ENTERPRISE**



Gp Capt Nikhil Sc (Retd)

www.iLogo.in

[8369833275](tel:8369833275)

sales@iLogo.in

[022 67498749](tel:02267498749)

Star of Forces Network

A Forces Network Star is a member of the Forces Network who has gone on to achieve glory in the his/her corporate/civilian avatar. The aim of this series is not just to celebrate our successes from the veteran community, which unfortunately we do not do enough, but also to inspire others. The ultimate goal is to set up a virtuous self-sustaining cycle of inspiration leading to more successes in turn inspiring many more.

IN INTERACTION WITH IQBAL SINGH

Col KPM Das is from the 53 course NDA and was commissioned in the Corps of Signal in Dec 78. Post having a successful career in the Army including commanding a regiment, he switched to the corporate. Starting with Persistent Systems in Pune as a Technical Manager, then Aztecsoft/Mindtree in Bangalore where he took charge of Global Operations reporting onto the Chairman/CEO. Post which he was approached by Cisco to consider a role in the APJC Public Sector Segment as a Consulting Architect. Later, in Cisco, he set up the India Cybersecurity Office and established compliance, secure supply chain structures and processes and information security frameworks. Presently he nurtures & mentors two startups in cybersecurity space. He is also a Fellow with Takshashila Institution



IQ: Please tell us something about your background prior to joining the NDA and Army, and your subsequent Army career. Please share any significant achievements.

Das: I came from a background where family members were mostly in military or civil services. Options in seventies were limited for a high school student- it was either Engineering or Medical. During my final year at school, I had a passion for sciences and successful entrance attempts for IIT, REC (now NIT) and NDA followed. Made a choice to pick NDA and follow a military career and was fortunate to be commissioned into the Corps of Signals.

I did well in all courses, served in Divisional Signal Regiments and Brigade Signal Companies for most of my career. I topped the degree course and thus got to do my masters in computer science from IISc. I also did the Staff Course and followed by a very satisfying tenure in MO Directorate. A stint in Angola with UN was a fond memory as well.

Two milestones which I cherish and I am proud of- commanding a Regiment in Op Parakram and being the lead of the first handheld rugged military computer anywhere in the world.

IQ: You had such an illustrious and a glorious career in the Army. Then, what was the motivation for taking Pre Mature Retirement?

Das: Computers had just come in early eighties and again opportunities during the courses guided me to develop an interest in and immerse myself in software. From Commodore desktops to Apple IIs, from PS DOS to Windows it was quite a journey. I wrote the first desktop BASIC application in 1982 and never looked back.

Army has been a great enabler supporting me even as I went through the rites of passage for an officer- I commanded a Divisional Signal Regiment in Op Parakram 2002 and eventually got nominated for the Higher Command Course HC-32. *This was a pivotal moment, where I took a deep breath and looked afresh at the career ahead.* I realized there was this unfulfilled passion and it was time to focus on technology and this required moving away from a military career. This was a decision taken with little notice and possibly I left behind another set of opportunities in the military.

IQ: Give us an understanding about your current role and what you are presently engaged in. Also please share in chronological order the roles and companies in your corporate career also include your key learnings in each role?

Das: Presently, I am not in formal employment any more. I now nurture and mentor two startups in cybersecurity space, one in the cloud posture management product segment and another in risk and consulting services segment. The motivation is to transfer my experience and learning to the emerging and exponentially growing cybersecurity eco-system.

I am also a Fellow with Takshashila Institution where I research and guide in geopolitical and military aspects of technology, cybersecurity, supply chain and informatization.

I began my career with a software product engineering services company Persistent Systems in Pune as a Technical Manager. It was a fulfilling experience. Coming straight out of command of a unit, it was a catharsis of sorts. The company initially offered me a role in operations but I had my eyes set on technology and software development. I joined in a hands-on role and that brought in immense learnings in software engineering and in managing the product life cycles. Later, I also managed a product developed for a Japanese retail bank. Delivering to the exacting and unforgiving expectations of the customers was an experience which stood me in good stead later.

I then moved to Aztecsoft/Mindtree in Bangalore where I set up the Web Technologies BU with P and L responsibilities. Given the 360 degree nature of management exposure, I was schooled in running a profit centre. I worked with customers largely drawn from US and Europe at a time when industries and businesses had to necessarily have a web front end to manage customers.

Post acquisition, the leadership asked me to take charge of Global Operations reporting onto the Chairman/CEO and that role pushed my learning envelope to the extremes. This time around it was squeeze efficiencies within a globally widely dispersed centres and within the Indian software export zones. I ran a tight ship and it was satisfying to deliver on expected operational and bottom-line parameters. We also won the Great Places to Work award having brought in an inside-out approach to engaging employees.

In 2009, I was approached by Cisco to consider a role in the APJC Public Sector Segment as a Consulting Architect. That was quite a change and against the grain of my career path. I pivoted to this role which demanded a lot of engagements across countries and building Cisco's brand and position as the first partner of choice in networking, security and data centers. Later, in Cisco, I set up the India Cybersecurity Office and established compliance, secure supply chain structures and processes and information security frameworks.

In a nutshell, my career was built on a foundation of technology and later in cybersecurity with a deep product engineering exposure

IQ: How did you prepare yourself for the Military to Corporate transition? Is transitioning from the military to a tech career more difficult than a non-tech career in your view?

Das: A few serendipitous events towards the later half of my military career catalysed my readiness for a tech career. I was chosen to lead a small team of Sigs plus Infantry officers to build a handheld platform for infantry in CI Operations. At that time in 2002, it was the first military PDA based on embedded Linux, open source mini-GIS and a mini-C3I wrapper. Hardened for use, it was called SATHI : https://defenceforumindia.com/attachments/esl_sathi_brochure-pdf.20561/ This experience in product and software development gave me the confidence to transition to a tech career.

I would not make comparisons between transitioning experiences in tech versus non tech careers. Each has their own challenges and opportunities. That said, many of the military skills map directly into the corporate space and are called transferable skills. That gives us a head start during transition; a few certifications and understanding of global standards and processes and we are good to go.

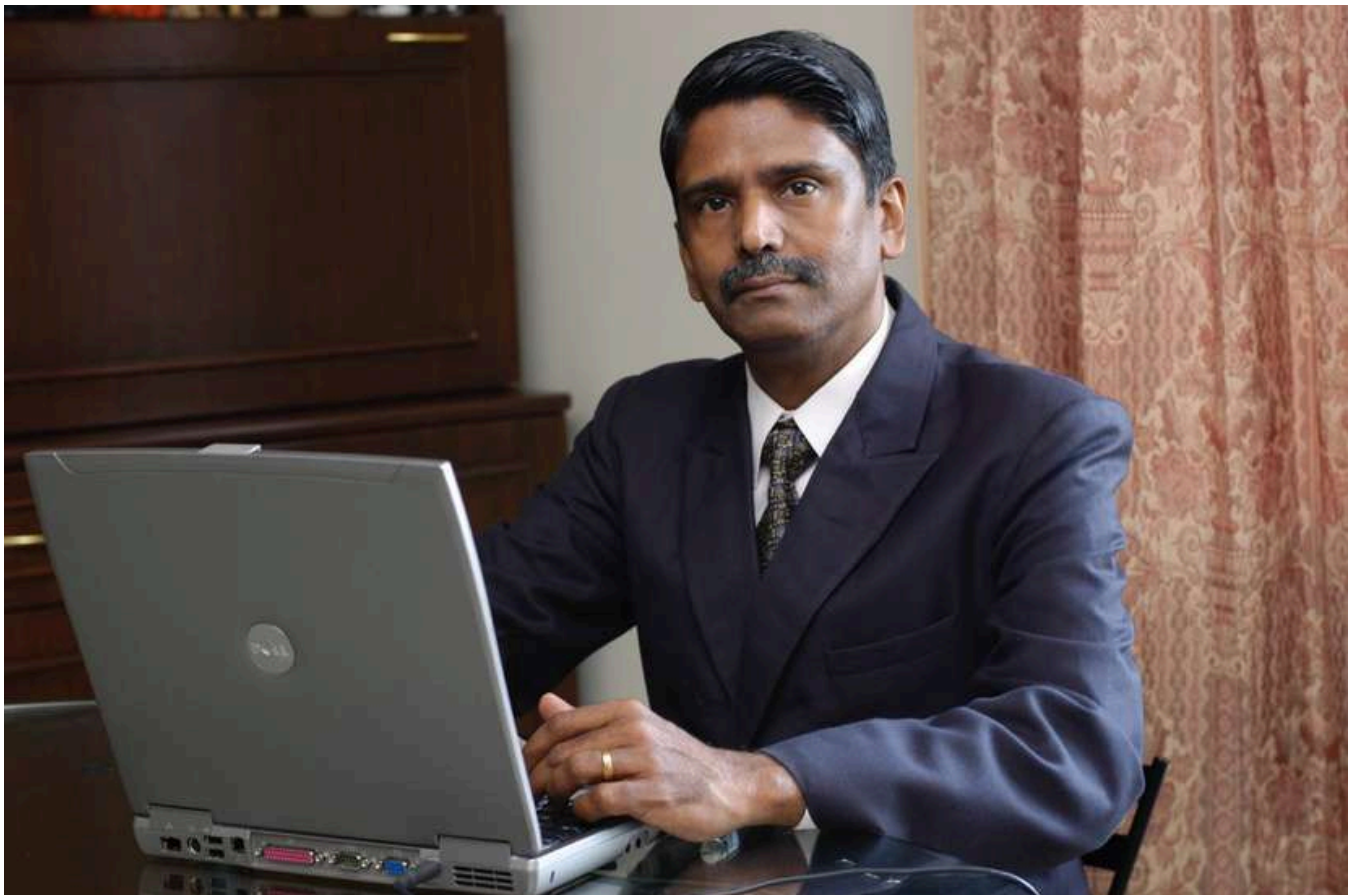
In a tech career transition, it needs a little more rigour. You need hands on skills and a bit of on the job experience. However, given the changing tech cycles and mature learning methodologies, **it really does not matter whether you are from a technical service or infantry/artillery/others**. There are learning pathways to take any officer into a tech career. **Let not background hold anyone back**. This is from experience- my best delivery manager was a former infantry officer!

IQ: Has the Transition become more challenging now than what it was when you joined the corporate?

Das: Yes and No.

Yes, in terms of challenges of expectations from industry in the form of a steep learning curve, adopting agile and modern workplace practices etc. Today the portfolio of skills and experience is a lot more complex and demands more investments of time, effort and cost. You need to be seen as a hands-on contributor. Plain vanilla management skills are not enough. Also, twenty years earlier we were seen as stereotypes and best-fit for facilities management and legacy security roles. That has changed. The fact that the compensation between the military person and the corporate employee was huge. That has changed and getting a parity in compensation itself is a challenge.

No, in the sense that available opportunities are a thousand times more in the job market. Also, access to internet has been a game changer. You can be in units and still continue to invest an hour to learn the ropes in the latest skills and technologies. You now have the power and reach to communicate to CEOs and industry leaders in a pre-transition-conversations.



In his corporate Avatar

IQ: What were the challenges faced during your Transition? How did you overcome the challenges?

Das: To me, the biggest challenge was in getting out of military service. I was nominated for the HC Course and many seniors up the chain of command found the decision-to-leave as foolish and against the run of play.

The other challenge was in finding a job. I was determined to write code in my new career and I got no interview calls when they realized that I was in my forties. Instead, some of them readily offered me other roles in operations and security, many of them senior. So I began at the bottom rung but with the satisfaction of a hands-on role.

IQ: In your experience what are the common pitfalls for most service officers while switching to the civilian world. What would you advise on this subject to transitioning officers?

Das: That is a great question. In my mind, there are four that I could list.

One, clarity in the motivation to make the change. That is the first thing I ask. If it is compensation or an inclination to ease up on the pace of work, I see them as not enough.

Two, not looking at expectations from the change correctly. The mix between role/company/location/compensation/career-pathway/learning-opportunities factors has to be right. For a short service officer compensation is also a priority given no fallback pension in addition to a role where he or she can look at a pathway to future leadership. For an officer transitioning prematurely, I would think it is role and location. And so on. This has to be given a thought. Making an early mistake in making the correct mix of these factors can prove costly later.

Three, going into the transition under prepared. A clear runway towards skill development, networking and organising your story and resume with clarity is necessary.

Lack of a Mentor: A mentor at this stage can make a positive difference.

IQ: While you came from a strong technical background ie Corps of Signals, ME from IISc Bangalore did you have to learn some technology related subjects? How did you do so?

Das: Oh yes!! Degrees like ME in Computer Science help but get out of date soon. One has to learn all the time. In fact, most learning models today prioritise self-learning and certifications over others. I learnt Java and PHP in my year one- those were commonplace twenty years ago. For a technical person, learning is sine qua non on a daily basis. Else, you get out of reckoning for the company, for your customers and for the teams you work with.

IQ: If you were to Transition from the military to the corporate today with the benefit of all the insights and wisdom that you have gained in the corporate today what would you have done differently?

Das: Looking back and drawing lessons is always a challenge. I guess if I were to pick just one path which I could go back on and choose another, it would be about international exposure. I had a choice to move into sales teams working in the Bay Area and I let it pass. **Lesson- let not location or culture be a barrier.**

IQ: Any important lessons you learnt while switching jobs and companies in your corporate career? Any advice for transitioning military personnel on this front?

Das: I just switched one job in twenty one years (other changes were through acquisitions)- I went from leading a large set of teams with over 3000 engineers to an individual contributor role. That switch , against the grain of common practice, is something I do not regret. I could make a larger impact across multiple geographies as an expert and specialist.

IQ: How important is it to understand your own passion and expertise and then to work towards upskilling in that domain so as to have a better innings in the corporate? How does one identify one's passion?

Das; It is important. In fact, that should ideally be the prime driver for any role you seek. It is always a choice between spreading yourself horizontally versus going deep in one area while still being versatile. I chose the latter. Both in military service and later I stayed in touch with contemporary trends in tech.

IQ: You have had a long stint in the corporate. To be successful what traits from the military must be give up and what must we imbibe?

Das: We must give up inclinations towards a Command & Control way of working and build more collaborative skills. Be the odd one in the room breaking group-think even while in service.

Most other traits are transferable and corporate leaders immensely value military people for their self-discipline, communication, process and compliance way at work, execution orientation and most of all good cheer and optimism.

IQ: Today with the democratization of learning is it possible for a military officer coming from a non tech background (ie Infantry, Armd, etc) to make a career in the tech industry? How would you advise them to go about this? Let's say if someone wants to join the cyber security vertical.

Das: Absolutely. I have answered this in Question 4. The very notion of silos among arms and services is **a drag to progress. Nothing holds you back except that legacy.** However, the change in orientation requires a certain planned pathway. Get yourself a mentor who walked that path before. Plan out the path. And then mark out the skills and experiences needed. Often, for an infantry or tank officer experiences are scarce. Plan on internships.

Fortunately, cybersecurity is one such space for all. For those aspiring for a career in cybersecurity, many options exist. I would encourage the technical lot to focus on software development, deep malware engineering and core infrastructure engineering. For others there are roles in risk and governance, processes and cybersecurity operations, and audit. In fact cybersecurity roles are a mix and match and as you go along you can pivot and add more skills towards leadership as a CISO/CIO/CTO



With his classmates

IQ: The one regret in your life?

Das: Wish I could be thirty years younger and transitioning today. No better time!!

IQ: Tell us about your family. What role did your parents play in shaping your value system. Also share the role played by your family including spouse in your successful Transition and subsequent civil career?

Das: I come from a family of military members. The Indo-Pak war of 1971 was a milestone in my teenage years. We had two members from the family who were fighting the war. One returned with a Vir Chakra and the other got killed during a counter-bombardment a day after the cease-fire on 17 Dec 71. I remember lining up along with many town school-children along the central street in Calicut to welcome my relative and gallantry award winner, who was received with fanfare on a caparisoned elephant. The seeds were sown to be a soldier first.

My wife has been extremely supportive- especially when I had to walk away from a point where I said no to a HC nomination in 2003. We recast our family priorities together, all through my career.



A Family Pic



Lt Col Iqbal Singh (ret'd) is an infantry officer who started his career with the Garhwal Rifles in Dec 1987. He is currently a senior technology executive with Google based at Gurgaon, India. He is firmly of the belief that tech is an enabler and your friend. He is the Founder of Forces Network – the Network of the military veterans in the corporate. He believes that there are no barriers: all the barriers exist only in one's mind. It was with that firm conviction that Iqbal started the now famous ABCT (Any Body Can Tech) Program in Forces Network in 2019. Under this program non-tech officers were taken to cloud certification level. Over 40 participants got certified from Microsoft in cloud computing under this program. He is convinced that military personnel can easily transition to tech roles with some upskilling.

Please provide your invaluable opinion/feedback on this Interview, by clicking/tapping [HERE](#) - Editor

AB KIDS LIFE COACH
CARVING DIAMONDS | CREATING LEADERS

Parenting Woes

OUR UPCOMING WEBINAR

3 SECRETS to Your Child's Success

Key Takeaways:

- ▶ Biggest Mistake Most Parents Make
- ▶ Formula for Parenting for success
- ▶ The magical Secret to get quick and amazing result

Lalit Panwar > **Amit Batra** 1 hr · 🌐

Hi Everyone.... attended the Amit Batra's webinar on Kids Coaching today and found it extremely useful and powerful session. Shall recommend parents of all kids from 1 yr to 18 yrs to attend and gain the useful insights right from foundation to communication. Great Job Amit....carry on the good work.

Rajiv Ghosh > **Amit Batra** 1 hr · 🌐

Attended a session on parenting by AB, it was quite insightful. Concepts like mentoring your child, setting rules, delegating responsibilities, respecting your child's opinion did invoke my interest and we will definitely implement the same in my daughter's upbringing. Loved the way he explained how right parenting creates an environment which will help the child grow in a positive direction. I highly recommend all parents to attend his webinar.



If you are facing any of the issues with your child
SCAN THE CODE BELOW

JOIN OUR FREE WEBINAR



Contact us @ (Whatsapp msg only)



<https://wa.link/q28897>



<https://abkidslifecoach.in/forcesnetwork>



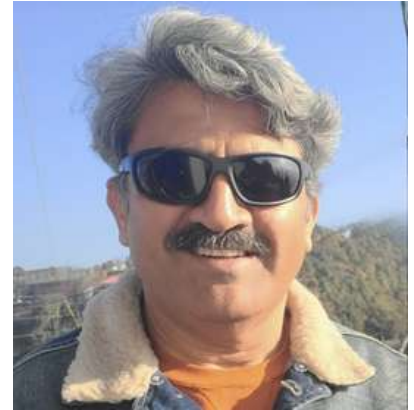
Connect@abkidslifecoach.com

Author of the Month

Sunil Kotnala

IN INTERACTION WITH IQBAL SINGH

Col Sunil Kotnala is a 3rd generation Army officer and was commissioned into 5th Battalion The Garhwal Rifles Regiment. After serving close to 3 decades in the Army he sought Pre - mature retirement to pursue his craving for writing and acting in the glitzy world of Bollywood. He now resides in Dehradun and is a full-time author. He has now stepped into active politics by joining the Uttarakhand Kranti Dal, a regional party and is the General Secretary. He has also started a small farming and home stay venture in Chamba, Tehri Garhwal.



IQ: Please tell me a little bit about yourself, your background, your childhood and education before you joined the Army?

Sunil: Youngest of four siblings I was born in a military family. My father was commissioned in 6/5 GR and due to command surplus opted to command 5 Garh Rif and was nominated to raise 12 Garh Rif prior to the Indo-Pak conflict of 1971. My grandfather was with the BEG and was awarded the OBE and Sardar Bahadur after the WWII. Although my father moved all over the country on postings he kept the family stable at Delhi. I started my schooling from the erstwhile Defence Services Public School, Maulana Azad Road Hostel, New Delhi which is now known as Army Public School, Dhaula Kaun. After my primary schooling I shifted to Kendriya Vidyalaya to take on any move out of Delhi. I was a talented sportsman and represented Kendriya Vidhyala Sangathan in Basketball at the SGFI meet and later was part was of the Junior India Team also. I represented J&K in the 1978 SGFI meet. I shifted to KV, Srinagar when my father took over as the Centre Commandant, JAKLI Center in 1977 where I did my 9th and 10th class. I completed my Senior Secondary Schooling from KV No1 Jalandhar Cantt and was picked up by the DAV College Jalandhar for my outstanding performance in sports and Extra curricular activities i.e. Dramatics. This is where the creativity got wings and I got recognition as an actor on stage. "Best actor" All India Inter university and Doordarshan, Jalandhar. But standing at the crossroads of future life and profession the military genes proved stronger and more pragmatic and got the better of me. In the Army I played for the Services Cricket team and represented Central Command in Basketball.

IQ: Was your joining the Army a calling or a continuation of family tradition?

Sunil: Joining the Army seemed the most natural progression for me. At the time of choosing a profession I had 2 choices; the Army or the Film industry. Therefore, it was both; a calling and a continuation of the family tradition



IQ: Did you do any kind of creative, fictional or non-fictional or even professional writing while in the Army? Tell us about that.

Sunil: Of course, I did. I wrote and directed plays/skits in the unit for various occasions including Raising days, Dusshera and ladies meets for senior officer's lady wives. During AWWA events I compered and directed their shows. I have written extensively for the CIJW magazine PRATIVIDROHI. My books are predominantly military experience-based fiction either inspired or based on real incidents/operations.

In 1994 I wrote a concept paper; *My Dream Sheet for the MS Branch* which was based on the fact that officers posted in the MS branch decide about an officer's career without even asking his choice/ opinion, which leaves them dissatisfied and the satisfaction level percentage of the Indian Army officers remains low. For Example; two Majors have to be posted to Cat A establishments as instructors. One to IMA and the other to OTA. Officer A belongs to Chennai and would want to go to OTA for obvious reasons and similarly Officer B who belongs to Uttarakhand wants to go to IMA but the officer in the MS branch knows nothing of this and does not bother to call either of them, so A goes to IMA and B goes to OTA. As far as the MS branch is concerned, they have done a great job but the satisfaction level of the officers is zero. This paper talked about how to let the officer's dream about his future keeping his career profile in mind. This was accepted by the then MS Lt Gen Yuvraj Mehta and has since been implemented in some way.

IQ: You were doing well in the Army and then you decide to take Premature retirement. What was the motivation for that? Was it an easy decision- what factors were weighing in your mind? Why did you relocate to Mumbai?

Sunil: Doing well in the Army is a very deceptive term. If I may use a simlie; you maybe think you are a thorough-bred stallion all 364 days of a year but on the 365th day your boss may tell you that you are a mule. Doing well is entirely what others think of you. Well that aside it is a great oragnisation to serve in. To tell you the truth I would have left the army way back in 1994 when I had at least 2 offers from Bollywood but my wife restrained me from doing so which now in hindsight was a good decision as I got to experience the Indian Army more in-depth and to command one of the finest units of the Indian Army.

Once I finished my command the action in my life waned away and the sheen of army life faded. The desk job got on me and the craving for creativity and maybe glamour started clawing me. I was pushing forty and I was aware that any delay in leaving the Army now will hamper my chances to even get a corporate job; which I would need to survive in Mumbai. Any further delay may get me in a comfort zone and I may then not want to leave the Army. It was not a difficult decision to make as leaving the Army was always in my sub conscious but yes it was difficult for people in my family and regiment to digest. My mother was the only one who supported my decision and told me that she was confident that I would do well in the outside world no matter what I decided to do. This gave me immense confidence I took the plunge. Before I left I made sure that I follow the Infantry teaching of 'One foot on the ground.' Thanks to Maj Narayan Kurup of 4 Garh Rif who had also left and was nicely embedded in the corporate sector who got me a good job in a security agency in Mumbai.

IQ: Tell us about your first book. How did that happen ? Also tell us what is the book about? Why did you chose this topic to write upon?

Sunil: My first book is The Holy Warriors and the tagline is, "You fight your Jihad and we will fight to defend our motherland. Let us see whose war is holier; yours' or ours."

I believe there can be no higher service than to defend your Mother (Land). This book was in my mind since my tenure with the unit in Kashmir. I thought that the terrorist also believes and feels that their cause is justified as much as we do, so what is that differentiates us from them. So, whose cause is more pious? Ours, because we fight for our motherland irrespective of our caste, creed, colour and sex. It is from here that the word Holy Warrior took birth. We are undoubtedly the **Holy Warriors**. It took me 15 years to write and get it published. Frankly, it took 3 years to write and 12 years to gather the courage to get it published. Thanks to Mr Pranay Gupte an outstanding author of international repute who was staying in the Leela Hotel, Mumbai where I was working later to have read the manuscript and encouraged me to go to a publisher. He said, 'If you don't go to a publisher how will he publish it.' In the book he wrote the foreword which I am re producing below.

Why Write? Why Not?

Foreword by PRANAY GUPTA

There isn't just one Sunil Kotnala, there are several. There's the tall, sturdily built man who distinguished himself in the Indian military. There's the man who produces documentaries. There's the fellow who acts in plays. One could go on. And now there's the Colonel Sunil Kotnala who's written an exceptionally enthralling novel...

That he's written such a thriller comes as no surprise to me. The man is a natural storyteller. Even the briefest conversation with him would reveal that. In fact, I'd be surprised if anyone would be satisfied with merely a short chat with him. Each conversation with him has a beginning, a middle, and an end – an indication of a mind that's neatly organized and one that's able to communicate succinctly.

It's a mind that is all absorbing. Sunil has keen powers of observation and synthesis: nothing escapes him. Those are important assets when it comes to writing, but particularly fiction. Sunil can reconstruct scenes from memory, or he can create new ones from his vast imagination. Happily for his readers, all his skills converge in this novel.

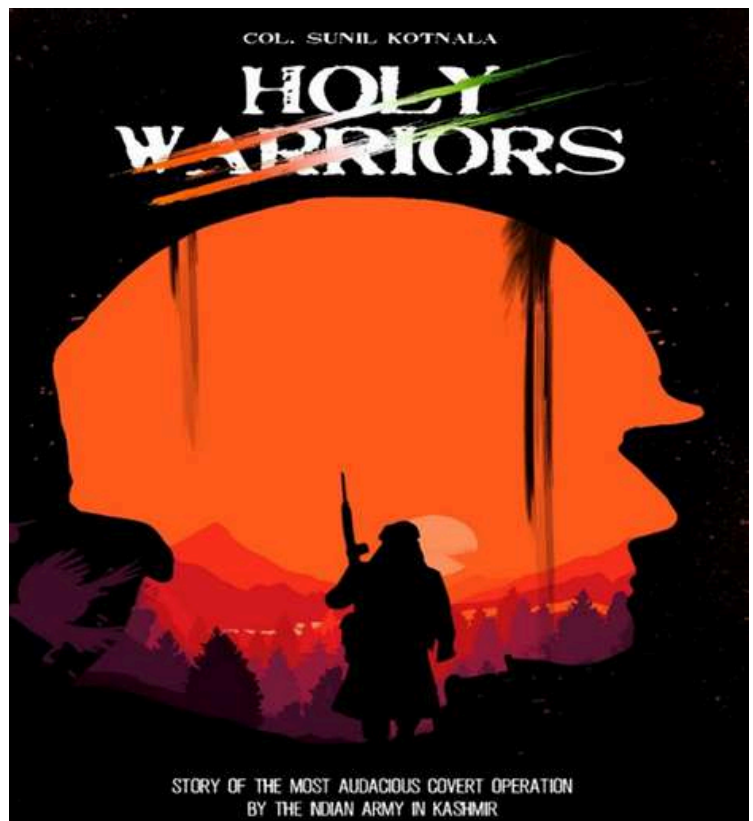
It is a timely work of fiction, revolving around happenings in Kashmir, one of the most volatile regions in the world where ideology, religion and ethnicity are constantly in confrontation.

Sunil deciphers the geopolitics of Kashmir in a way that doesn't seem academic. After all, this is a novel – even though I am certain that it will become assigned-reading in school and university classrooms.

It entertains, but it also chills. Sunil depicts the daily cruelties that characterize war zones, even when bullets and bombs don't always go off continuously. Sunil shows us the impact of conflict on everyday people who have no recourse other than to accept their fate silently. He also shows us how some of those people choose to become terrorists. He paints a deadly scenario of futility, spiritual despair and moral degradation.

I realize that this is meant to be a foreword, and not a book review. But having read Sunil's manuscript, I'm still shaking. You will, too.

I also predict that you will want to read the novel a second time, and a third. That's because it's nuanced, it's filled with subtleties and surprises. And then you will want Sunil to deliver his next novel. He's young enough to build a library of his own books, both fiction and nonfiction. I just wonder how he finds the time for all that.

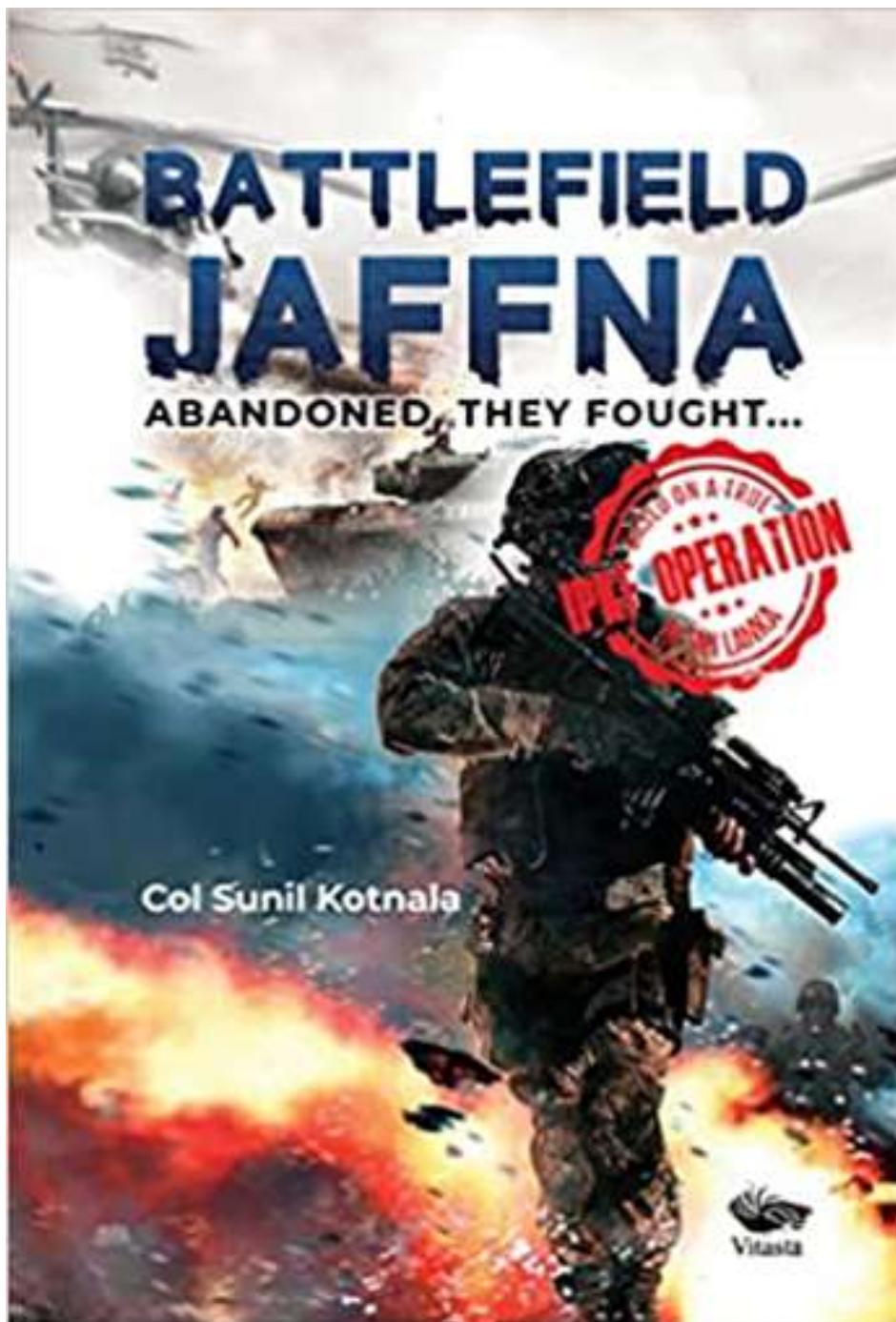


My First Book

IQ: Keen to know about your second and third books. What prompted you to write on those topics? Also briefly mentions what the book is about?

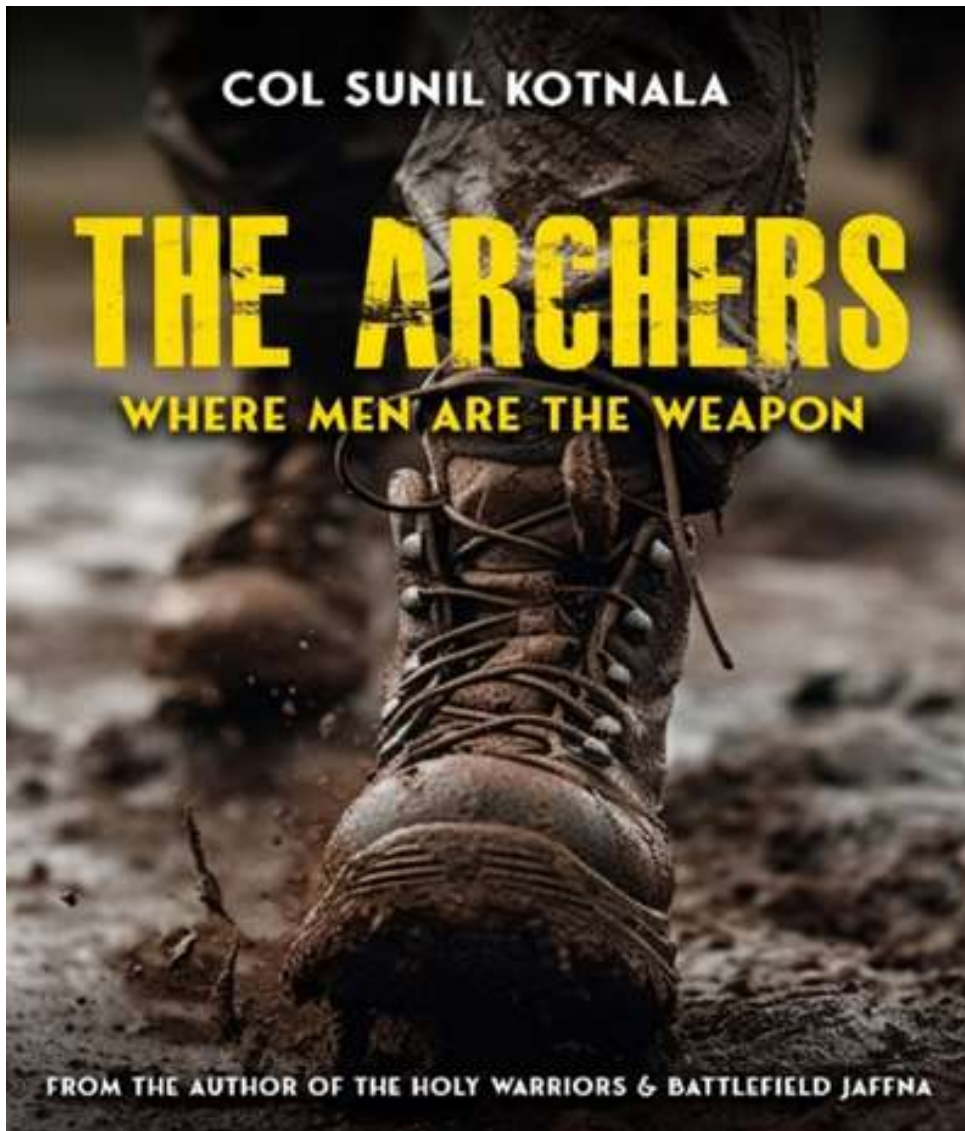
Sunil: Like all other things in life, 'First time is the most difficult one,' once you cross that landmark and depending on the experience you either never do it (Negative experience) or want to do it more and more (Positive experience). Luckily, I had a great time with my publisher and this encouraged me to write on all the story concepts that I had written.

The motivation to write, 'Battlefield Jaffna', came from an India Today cover story by Shekhar Gupta in 1987. It was always in my sub conscious.



My 4th Book

'The Archers,' my 3rd book is purely fiction of course based on personal experiences. It is about a highly covert group handpicked by the Indian Army that operates clandestinely to eliminate ANEs. The protagonist is a Major who is immensely independent and flamboyant but professionally one of the best. His team consists of 'the best of the best' and are the weapons of the organisation. My Commanding Officer in the Garhwal Scouts; which later I also commanded now runs a publishing house by the name of 'Sabre & Quill' wanted to publish Battle field Jaffna but due to some reasons and mainly my fault it did not materialize. So, he took on The Archers which he liked because of the concept of a special operations team and the beginning.



My 3rd Book

IQ: Your book **Battlefield Jaffna: Abandoned, They Fought** seems like a fascinating story to tell. It is a story that needs to be told and sadly very few know about it in the country. Why do you think you felt impelled on writing upon such an important though neglected subject? Is it a factual account of part fiction? How did you conduct research for this book?

Sunil: As I have mentioned earlier this story was in my mind since I had read about it and I was surprised that nowhere in the Army whether in school of instructions or during presentations did, I ever even hear a whisper about it. The operation was treated

treated as a bad memory which was never to be recalled. I was appalled. Why were we treating our comrade so shabbily and with disrespect? It was sad. I started my research and it took me 5 years to write it. I was lucky that my father had served with Gen Deepinder Singh the OFC and Southern Army Commander during Op Pawan and he welcomed me at his home with open arms and candidly narrated every detail through his amazing narrative skills and memory. I extensively interviewed Maj Gen Sheonan Singh, the erstwhile company commander of 10 Para, Capt Ranjit Singh Bhadauriya, 10 Para, Col Sethi, CO 13 SikhLi, Gp Capt Sonpar and their Air Force pilots who were part of the operations.

The story of the operation is true to the last word as told to me by the officers; Army and Air Force and the men, Sepoy Hawa Singh the lone survivor of the operation whom I met. Yes, to make it palatable and readable certain incidents and conversations are fictitious or to say the best my military mind could conceive. It was India's Black Hawk Down as many journalists wrote about it but I thought it was an unfair comparison. Our operation was a failure of the top hierarchy who neither had the vision or a workable plan. It was sheer complacency, bravado and 'Rambones' that led our men to a suicidal mission. It was not a Rag Tag mercenaries that we were fighting against but men and women who were highly motivated for their cause of 'Tamil Eelam' and unfortunately trained by our finest. The entire country and the world ought to know that we went in with grossly inadequate intelligence input and ill prepared in both equipment & weapons. Troops were inducted into high intensity operations without any preparation and the operation went topsy turvy from the word Go. An operation which the commanders thought would take 10 to 12 hours took 23 days to be completed that too without achieving the aim of the mission of eradicating the top brass of LTTE.



The owner of Leela Hotels and Ventures; Late Capt CP Krishnan Nair and Executive House Keeper Ms Kakroo.



With Star Aamir Khan at the Leela Hotel

IQ: What is your writing or the creative process? Do you make a list of points then create a draft and then refine it or do you have long sittings to pen the book? Is there a specific routine you follow while writing a book?

Sunil: I am a writer with no formal education in writing, which is by design and not by default. I did not want to be influenced by the Grammer of creative writing because it kills the originality and the style of the writer. I must maintain my uniqueness and essence. Therefore, I write without any notes or draft. It's all in my mind; each scene, every character and the flow of the story. I just reproduce it on paper sometimes sitting long sessions and sometimes only a few minutes depending on my writing mood. Lately I have learnt that to follow a routine to write is also good as it does get me into the mood or at least gives me time to refine what I have written.

I am an early riser and am up by 4 AM. My most creative time is 5 to 7 AM although I do try to write 5 to 6 hours each day.



With the legendary Naseerudin Shah, discussing a concept. A film that he and Pankaj Kapoor agreed to do but couldn't materialise.

IQ: How was the experience of being based in Mumbai and writing there for the entertainment industry?

Sunil: Mumbai was fantastic in all aspects. I loved the fast and furious life there. Every single man and woman there are ambitious, competitive, and totally professional. To give you an example during any shoot of a scene of a film say a song at least 150 to 200 people are on the set. All these people come from different parts of the country specialising in their trade. It is chaotic when the camera is not rolling, but one command of the director, 'silence, lights sound camera rolling and action', and it must be seen to be believed how things move in total sync thereafter. Totally professional. Nothing of the sort that we hear about the film industry. I remember being on a shoot of a film where a super star was doing the lead role. It was a 12-hour shift and the complete unit of about 600 was ready at the call time – 8 AM. The super star was late due to some reasons and arrived only at 5 PM. The producer was in tears as one day of shoot was costing him over 2 Cr. But the super star was all prepared and gave all shots okay in first take in 2 hours and Pack Up was called. That is the level of professionalism.

IQ: You have also entered political life. Tell us about that and the motivation behind that?

Sunil: 'I have done it for my country and now I must for my state,' पहले देश के लिए अब प्रदेश के लिए। Seeing the state of affairs in the state of Uttarakhand I thought that if people like us do not enter politics then this vacuum will be filled by such people who are in power now and then we should not blame them. We must be the difference. Politics is not dirty by itself but it is the people who make it so, if the good ones come in it will become good, clean and we can give the people a corruption free governance.

IQ: Tell us about your family. How do they take it when you are busy writing, reading and researching your books?

Sunil: I am lucky that both my kids are settled and live abroad. Initially when they were young I did not write much at home. I used to discuss the concept with them and they would give me some useful inputs which did help me immensely in writing. The Holy Warriors first draft was written at a post known as Jatti Gali near TMG in winters sitting in the FRP with 6 to 7 feet snow all around and the oil Bukhari at its maximum.



Col Kotnala with his family

IQ: What are your future plans regarding writing?

Sunil: I have just completed the first draft of my 4th book and it should be with a publisher by December '24. It's a Dark Comedy based in the hills of Garhwal. I have many more stories to tell and write and I plan to keep writing.

IQ: Do you think that writing can be a good vocation for veterans? Why do you feel so? Can anyone write or it needs a special talent?

Sunil: I believe that NO ONE has seen life and characters of people as closely that we have seen. In the face of certain death all the masks that we wear in our life vanish and our true character in all its nakedness can be seen. We have gone through this many a times. We have been in sh*t situations and have either come out victorious or vanquished either way it has taught us many lessons which make great reading for people who will or will not ever be there. Therefore, military veterans must write it may be books, articles, short stories, poems whatever but they must tell the world what it is to be a soldier a profession that is nobler than all.

IQ: How can our readers keen to pick up a copy of your book do so?

Sunil: My books are on Amazon, Flipkart etc.

<https://www.amazon.in/Holy-Warriors-Col-Sunil-Kotnala/dp/9352011201>

<https://www.amazon.in/Archers-Col-Sunil-Kotnala/dp/BOCNJPPRSZ>

<https://www.amazon.in/Battlefield-Jaffna-Abandoned-They-Fought/dp/9390961483>



Lt Col Iqbal Singh (retd) is an infantry officer who started his career with the Garhwal Rifles in Dec 1987. He is currently a senior technology executive with Google based at Gurgaon, India. He is firmly of the belief that tech is an enabler and your friend. He is the Founder of Forces Network – the Network of the military veterans in the corporate. He believes that there are no barriers: all the barriers exist only in one's mind. It was with that firm conviction that Iqbal started the now famous ABCT (Any Body Can Tech) Program in Forces Network in 2019. Under this program non-tech officers were taken to cloud certification level. Over 40 participants got certified from Microsoft in cloud computing under this program. He is convinced that military personnel can easily transition to tech roles with some upskilling.

Please provide your invaluable opinion/feedback on this Interview, by clicking/tapping [HERE](#) - Editor

Stars On The Horizon

Children of Defence Officers have the capability to excel in various fields, owing to their extensive exposure resulting from frequent transfers and change of stations. They possess very high adaptability skills, and immense potential as individuals. In this series we plan to showcase the achievements of such children of the members of Forces Network who are on the path to carve a niche for themselves through hard work, grit and determination, so as to provide adequate motivation to the others.

IN INTERACTION WITH UDAY SHRIWAS

Ms Ariya Nair was born to Capt. Ravi Nair & Mrs. Sulekha Nair in Pune. She pursued a Bachelor's degree in Biotechnology from Modern College of Arts, Science and Commerce, Pune, and an MBA in Pharma Biotech, specializing in Marketing, from the Department of Management Sciences, Savitribai Phule Pune University (PUMBA). She is a consultant at a healthcare analytics and consulting MNC, IQVIA and also a passionate certified career coach with 6 years of experience empowering teenagers and professionals. Driven by a commitment to transformative growth for millennials, she is now expanding her expertise into life coaching, guiding individuals to unlock their potential and achieve profound personal and professional transformation.



Uday: Please tell us about your childhood and the life you spent in an Army environment. What's the best thing that Army life teaches you?

Ariya: Growing up in a unique blend of army and civilian life has profoundly shaped my identity. When my father completed his tenure in the army, I was just 1 year old, which meant I didn't experience the traditional army life upbringing that many of my peers with army backgrounds did. Instead, I was raised in an environment that balanced the values of military discipline with the experiences of civilian life.

One of the most significant contributions of my exposure to army life has been the understanding of how to carry oneself with confidence—how to walk, talk, maintain positive body language and follow the etiquettes. Hearing experiences from my peers with army backgrounds gave me a sense of belonging, revealing how welcoming and homely the environment can be. This duality has enabled me to connect effortlessly with people from diverse backgrounds. The poise that comes from an armed forces upbringing, combined with the principles of persistence, discipline, and adaptability, has been instrumental in my personal development. Observing the resilience and commitment of my family and their army friends has instilled in me a strong work ethic and the ability to adapt to various situations.

These values shape my approach to life, encouraging me to savor the present.



My parents and I

Uday: What has been your childhood dream and any specific moments from your early childhood which left an imprint?

Ariya: Throughout my childhood, I dreamed of many paths—being a dancer, a fashion designer, a doctor or even a psychologist. At first glance, one might think I was just a confused child with too many aspirations. However, these dreams have woven together to form a rich tapestry of experiences that have shaped who I am today.

The hobby of dancing taught me to regulate my emotions and express myself through movement, helping me develop a strong sense of body language. This foundation laid the groundwork for understanding the nuances of communication. Simultaneously, my fascination with fashion allowed me to explore how styles are uniquely crafted for different individuals. Through this journey, I discovered my own sense of style—something many overlook, yet it plays a crucial role in defining one's identity.

As I grew older, my childhood dream of becoming a doctor evolved into a deeper passion for life sciences. This shift opened up a world of exploration, allowing me to seek answers to my questions about the healthcare field. I find immense joy in learning about advancements in this industry and the innovations that continually reshape our understanding of health.

In my quieter moments as a child, I was a keen observer of those around me. This natural inclination eventually blossomed into strong people skills and public speaking abilities. My fascination with understanding others' lives became invaluable in my journey as a career and life coach, enriching my capacity to guide and support individuals on their paths.

Today, I not only help students navigate their career prospects but also work with millennials who are seeking their passion, feeling lost, or redefining themselves. I am dedicated to providing the motivation and support they need to discover their true potential and pursue fulfilling paths.

In the end, my diverse childhood aspirations have played a crucial role in my development, molding me into the passionate person I am today—dedicated to guiding others on their journeys.

Uday: As you started your college life what's been your approach (preparation and research) to get closer to your dreams?

Ariya: As I embarked on my college journey, my approach to getting closer to my dreams centered on self-awareness and understanding my passions. Pursuing a BSc in Biotechnology, followed by an MBA, and now working in healthcare analytics while gaining experience in coaching, has all been part of a deliberate path.



With Dad at Deolali, Nashik

In school, I discovered my love for science, particularly biology, which led me to choose the PCB stream at Fergusson College. Although medicine was the conventional route for many students in this field, I made it a point to engage with professionals from microbiology and other life sciences to explore whether that was truly my calling. I secured admission to Modern College, Pune for Biotechnology and was also considering civil engineering, having been eligible to apply.

I vividly remember the day my parents and I visited the engineering college to fill out the admission form. I felt uncertain about choosing engineering over biotechnology. In that moment, my father suggested I take 20 minutes to make my final decision while they walked around the campus. I've realized that having a deadline helps me process my thoughts more clearly. When my parents returned, I was able to articulate my reasons for wanting to pursue biotechnology. That was the first time I truly felt I was taking ownership of my life, and my parents fully supported my decision.

For postgraduate studies, initially prepared for MSc entrance exams but soon realized I needed to assess my strengths and goals to determine the right path. After reflecting on my skills and aspirations, I came to the conclusion that MBA was the right choice.

To those who think an MBA is solely about academics, I would emphasize that it's equally about extracurricular activities and real-life experiences that prepare you to be a resourceful professional. My involvement in the placement committee marked the beginning of my realization that I could be a life coach.

The key takeaway here is the importance of self-awareness. It's essential to understand who you are, what you desire and where you see yourself in the next five years. In college, you might feel certain about your aspirations or you might not, but setting short actionable goals and gaining a deeper understanding of yourself will guide you toward discovering your true calling.

Uday: It is evident that you decided to follow a certain path in your career? Any reasons?

Ariya: Let me break down my passion for healthcare and coaching. Every day in the healthcare industry presents a new learning opportunity, and contributing—however small—to advancements in this field brings me immense joy. It's fulfilling to pursue a career I've been drawn to since childhood, allowing me to align my work with my lifelong interests. Being in the healthcare industry also made me more aware of mental wellbeing and how important it is to prioritise your health.



Travel

This is where my interest for life Coaching began and it has played a pivotal role in my personal and professional growth. It has enabled me to channel my emotions and make decisions in a structured manner. Coaching not only helps me improve myself but also empowers me to guide others in their development.

Life coaching is a broad area that encompasses career guidance, personal transformation, health, mindfulness, and business, among other aspects.

By pursuing career and transformation coaching, I envision empowering individuals to identify their passions and facilitate transformations in their perspectives on life. This journey of helping others discover their true selves is incredibly fulfilling.

Uday: Would you like to talk about mentors and teachers who have guided you through your journey? And why do you think mentors or teachers are really important in our life?

Ariya: I have been fortunate to have three significant mentors in my life.

My mother has instilled in me values of empathy, situation analysis, care, and strength. From her, I have evolved and learned a great deal about the psychological and emotional aspects of human behavior. She has taught me the importance of active listening and understanding others' perspectives, which has deepened my connections with people.

My father's sheer determination, personality, communication skills, networking abilities, resourcefulness, persistence, and practical nature have supported me at every phase of life. His ability to face challenges head-on and his unwavering belief in hard work have taught me the importance of resilience. He has shown me how to navigate obstacles with confidence and creativity, inspiring me to approach my own goals with the same tenacity and optimism.

Then there's my godmother, Sarla Aunty. She has been not only my English and French teacher but also my life coach. Her wealth of knowledge about life has been invaluable, and I am deeply grateful for the lessons she has imparted.

Mentors play a crucial role in our development, guiding us through challenges and helping us unlock our potential. Their insights, support, and encouragement shape our perspectives and empower us to strive for our goals. I am truly grateful for the invaluable impact my mentors have had on my life.



Career coaching at a school to motivate under privileged kids to pursue further education

Uday: What is your larger goal in life, and how are you preparing for it?

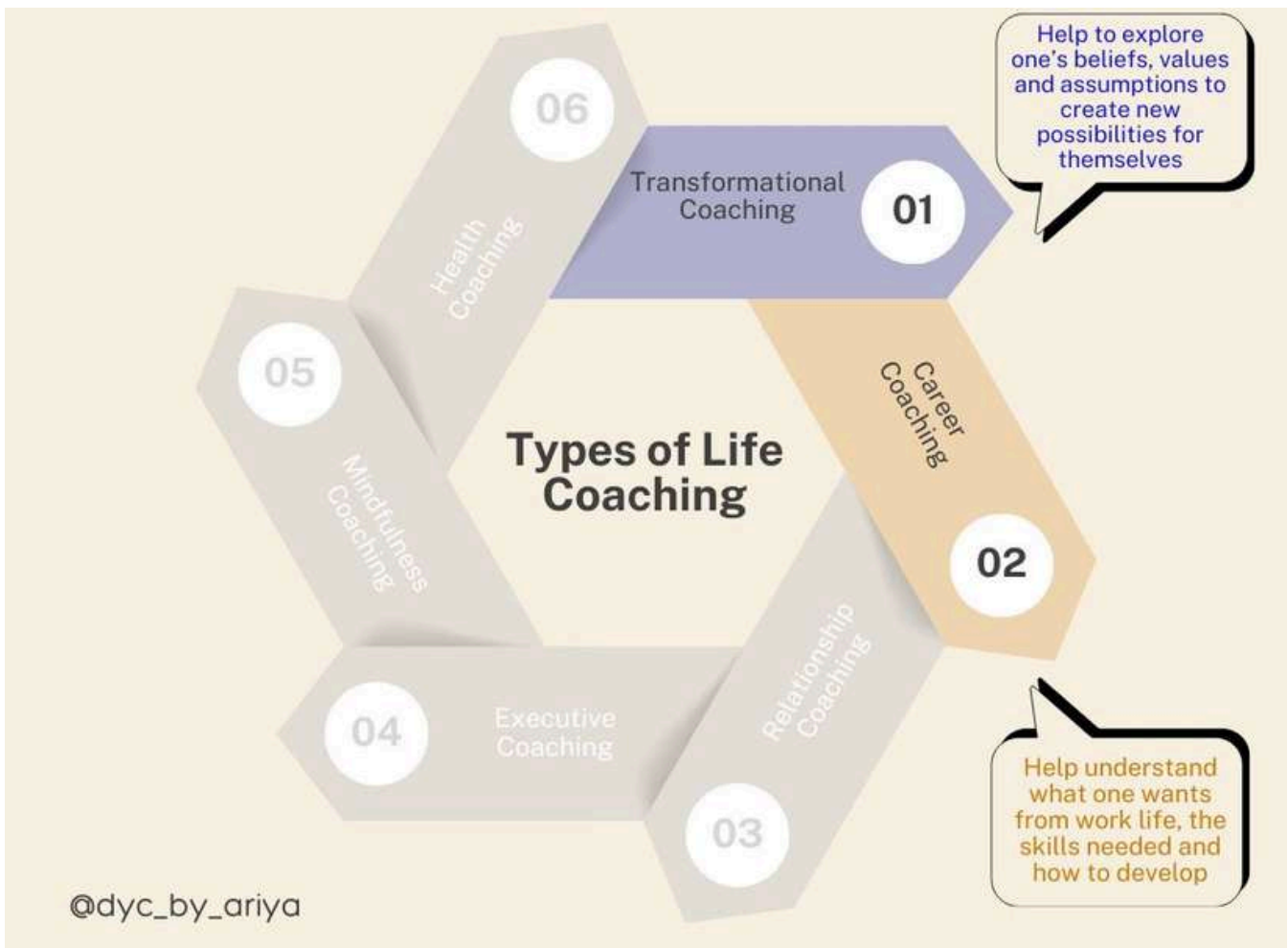
Aiya: Today, many millennials feel stuck in various aspects of life—whether at work, where they find themselves in a limbo between junior and senior roles; in relationships, where expressing emotions or bridging communication gaps can be challenging; or as parents, overwhelmed by their responsibilities.

As a life coach, my primary goal is to empower individuals to uncover their passions and achieve meaningful growth. I believe in the transformative power of persistence, both in my own journey and in guiding my clients. By helping individuals navigate their challenges with confidence, I aim to create a supportive environment where millennials can explore their aspirations and overcome obstacles.

Uday: There is a huge potential, especially in fauji kids. What would be your message for them?

Ariya: As fauji kids, we possess unique strengths that can significantly contribute to personal and professional growth. The discipline and resilience instilled in from an early age equip the kids to tackle challenges effectively.

Adaptability helps to thrive in diverse environments, while strong interpersonal skills enable to connect with people easily. To leverage this potential, fauji kids must focus on continuous learning, networking, and engaging in extracurricular activities to enhance leadership qualities. By setting clear goals and seeking mentorship and channelize these experiences into meaningful opportunities for growth and success.



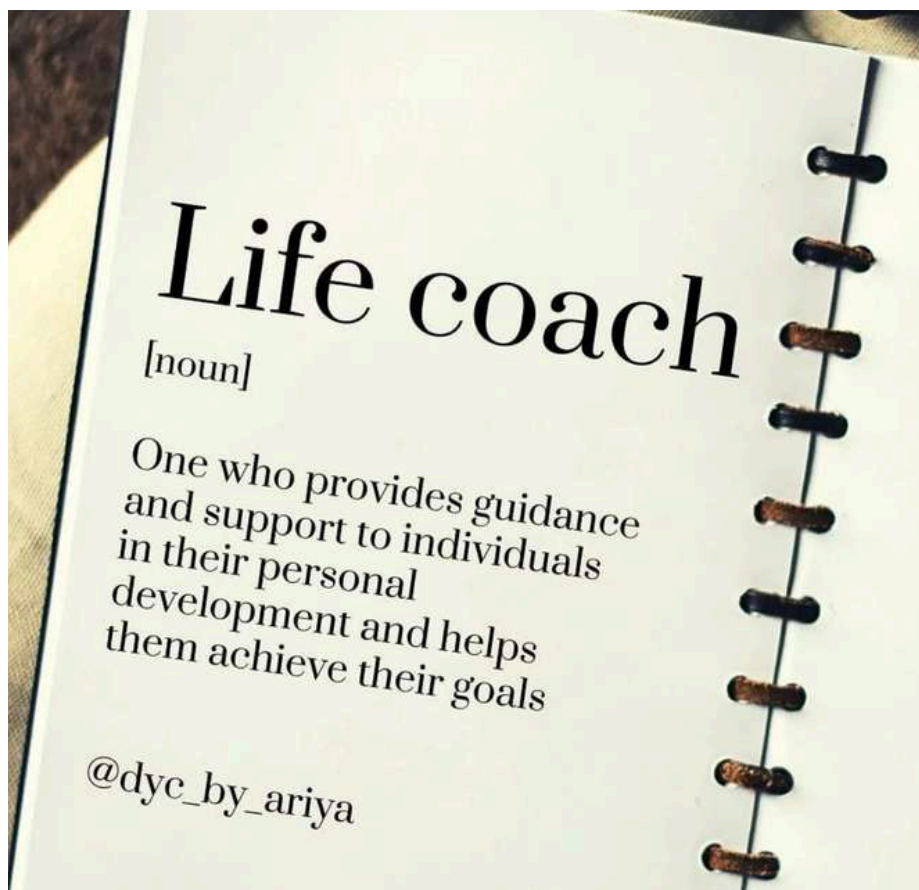
Types of life coaching and my specialty

Uday: Any subjects which you are passionate about and people need to be sensitised about them?

Ariya: In today's fast-paced world, it's crucial for us to prioritize ourselves- self-love is something most of us do not pursue.

We often juggle countless responsibilities—work, family, and social obligations—leaving little room for self-care. However, neglecting our own needs can lead to burnout and emotional exhaustion. When we prioritize our well-being, we cultivate resilience, clarity, and joy. Taking time for ourselves allows us to recharge and reconnect with our

passions, ultimately enhancing our ability to support others. By recognizing our worth and dedicating time to our own growth, we not only nurture our own spirits but also become more effective, compassionate individuals in our relationships and communities.



Uday: Most important -what keeps you going? A Bit about your Family. Your hobbies and what You love the most about your Work?

Ariya: Dreaming big, setting clear goals, and staying consistent have been instrumental in helping me reach where I am today. I am incredibly fortunate that my parents and my husband not only love and support me but also challenge me to critically evaluate my decisions. Their constructive feedback ensures that I'm confident in my life choices. Presenting a case study to them helps me navigate the various examinations life throws my way, providing clarity and focus.

Beyond my professional pursuits, I am passionate about dancing—I'm a trained Bharatanatyam dancer. I also enjoy expressing myself through shayari and love to travel, exploring new cultures and experiences.



The newly married couple- Dr. Sandeep Nambiar and Ariya Nair



Capt Uday K Shriwas was commissioned into the Corps of Signals, and served in various theaters during his service for five years, including in a newly raised RR Battalion. Thereafter he has worked with many renowned Companies, like Kingfisher Airlines, IFB Home Appliances, JK Cement, and Yes Bank Ltd. He enjoys working in the field of Marketing, Business Development, Strategy. He also has keen interest in the field of Personal Branding. He is presently working as Regional Head - Honour First (Defence Vertical) IDFC FIRST Bank

Please provide your invaluable opinion/feedback on this Interview, by clicking/tapping [HERE](#) - Editor

Author of the Month

Dharamdatt Goel

IN INTERACTION WITH UDAY SHRIWAS

About the Author

Lt Col (Dr)Dharamdatt Goel (Battle Casualty & War Wounded Soldier) – A Motivational Speaker and Soft Skills Trainer, an accomplished motivational speaker and soft skills trainer, he hails from Mumbai and has done his schooling from Panchgani. He completed his post-graduation in Psychology from the Dept of Applied Psychology, Mumbai University and went on to obtain a Ph.D. in Psychology. He also pursued his B.Ed to train the troops, and further went on to acquire a Master's degree in Personnel Management from Pune University. Before his distinguished military career, Lt. Col. DD Goel served as a lecturer of Psychology at SNDT University in Mumbai and as a Teaching Assistant in the Department of Applied Psychology at Mumbai University. His extensive experience in academia provided him with a deep understanding of human behaviour, soft skills, and personality development. Lt. Col. DD's military journey showcases his resilience. As a wounded Soldier he overcame tremendous Physical challenges to inspire others. After his casualty, he has participated in various adventure sports, including paragliding, bullet expeditions, half marathons, long-distance swimming, Skiing and Kite surfing. Lt. Col. DD Goel holds the esteemed position of Limca Book of Records in Paragliding. His dedication and determination has earned him the Chief of Army Commendation medal. Known for his talks, Lt. Col. DD Goel has been invited to speak at prestigious events, including TEDx , conferences and gatherings throughout the Indian Army. He addresses a wide range of topics on behavioural aspects, soft skills, mental health, emotional development, self-esteem, and personality development. Lt. Col. DD's has conducted motivational Sessions for renowned organizations. Furthermore, Lt. Col. DD has two decades of experience in the Army conducting training sessions on behavioural dynamics, change management, perception management, confidence building, cognitive enhancement, and more. His expertise contributes to resilience training. With a strong focus on empowering individuals in both their personality and professional lives, being a trained psychologist from DIPR & SSB Bhopal, Lt. Col. DD Goel has been instrumental in guiding aspirants seeking to clear the Services Selection Board (SSB) and join the armed forces. In addition to his speaking engagements, Lt. Col. DD Goel is also a published author. His book, **"When People Doubted My Ability to Walk, I Decided to Fly,"** published by Pentagon Press, showcases his inspirational journey. The book was released by the former Chief of the Army Staff, later Chief of Defence Staff, General Bipin Rawat, in May 2019. It has since been translated into Braille language, in Marathi titled **"Pagum Laghtaye Girim"** and in Hindi " **Udaan* hauslon Ki** " which was recently presented to the President of India.

Uday: Please let us know something about your background prior to joining the Armed Forces?

DD: Before I joined the Armed Forces, my journey was that of a typical young Indian filled with a sense of purpose and dedication towards making my life fruitful. I was a college dropout for almost two years, that time I was a Dhabawaala running my own Dhaba on a highway side in Bhilad Vapi road where I was a cook, dishwasher, Waiter and Manager, Later, when I pursued my studies, after my Postgraduation in Social Psychology, I became a lecturer of Psychology at SNTD University Mumbai and Teaching Assistant at Department of Psychology at Mumbai University . After I resigned my lecturers job, I appeared for many corporate interviews, in between I got the call letter for SSB and I cleared to Join the IMA .

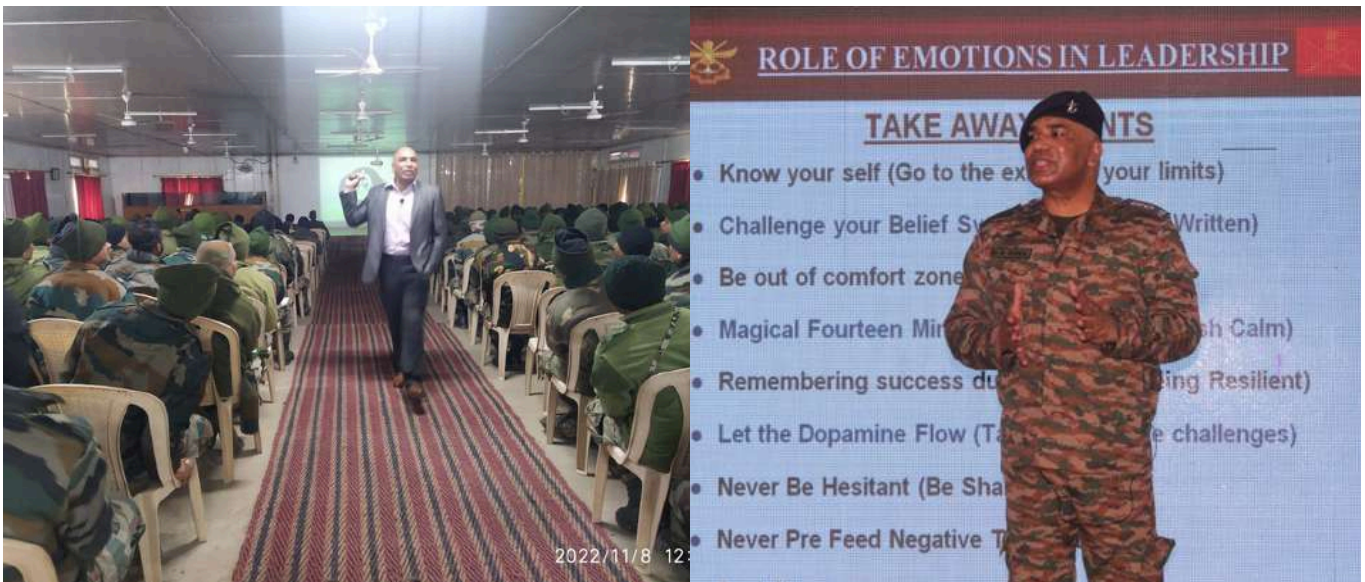
Uday: Tell us about your military career. What were the experiences that defined you, and what were important life lessons that the military taught you?

DD: My military career was one marked by adventure, challenges, and a deep sense of duty. After completing my training, I was posted in various capacities that gave me the opportunity to serve the country during critical moments. However, the most defining moment of my career was during *OPERATION PARAKRAM*, where I was severely injured and lost my left leg below the knee during one Operation. This moment, while physically debilitating, transformed my outlook on life. The Armed Forces taught me invaluable lessons in resilience, courage, and camaraderie. Even after the injury, my journey didn't stop. The military instilled in me the importance of never giving up, no matter how insurmountable the obstacles seem. I embraced adventure sports—paragliding (later making it to the Limca Book of Records), half marathons, skiing, Motorcycle Expeditions, Kitesurfing—on my prosthetic leg, showing others that limitations are only in the mind. This experience not only defined my personal and professional journey but also led me to inspire others through my book, *"When People Doubted My Ability to Walk, I Decided to Fly!"* Which was released by CDS Gen Bipin Rawat



Uday: Please give us details about what you are presently engaged in your professional role and where are you based out of?

DD: After retiring from active service, I transitioned into a new phase of life where I continue to motivate and inspire others. I have taken on several roles as a speaker, author, and mentor. My autobiography, *"When People Doubted My Ability to Walk, I Decided to Fly!"* has inspired many, and I recently translated it into Braille language, Marathi titled **Pangum Laghtaye Girim** and in Hindi under the title *"Udaan Hauslon Ki,"* to ensure it reaches a wider audience, particularly within the Armed Forces. The hindi book was presented to the Honourable Preident of India on 09 Sep 2024. The royalties from the book go towards the war-wounded fund of Indian Army. I regularly participate in motivational talks, marathons, and other adventure activities to spread the message of resilience and positivity. I am currently based in Lonawala, working as Chief Trainer for **Della DATA resorts** where I conduct training activities for the Corporates and FITs visiting DATA . I also travel extensively across the country, working closely with veterans, youth, and various organizations.



Uday: How did being in the forces helped you to write?

DD: Being in the Indian Army was an incredible source of motivation and support when it came to writing my book. The Army, despite its structured and disciplined environment, always encourages its officers to explore their passions beyond their duties. I found that amidst my demanding routine, I could still carve out time to pen down my thoughts and experiences. The Army's environment allowed me to reflect deeply on my journey, and that reflection translated naturally into words. The process of seeking permission from Headquarters to proceed with publishing was smooth and supportive, showcasing the Army's commitment to personal growth. One of the most gratifying moments was when I had sent my manuscript for the book's release, and the then Chief of Army Staff, General Bipin Rawat, who later became our first Chief of Defence Staff (CDS), personally read it. His encouragement and magnanimous gesture to release the book not only honored me but also made that moment truly historic. His belief in my story and its message was profoundly inspiring and validated all the effort that went into writing it.



Uday: What is your message to all those people who plan to write a book but never really take up the effort to do so?

DD: My message is simple: if you have a story, an idea, or any thoughts in your mind that you want to pen down, just start writing. Don't overthink the process or wait for the perfect moment. Begin with free association - write whatever comes to your mind. It doesn't have to be perfect right away. day,



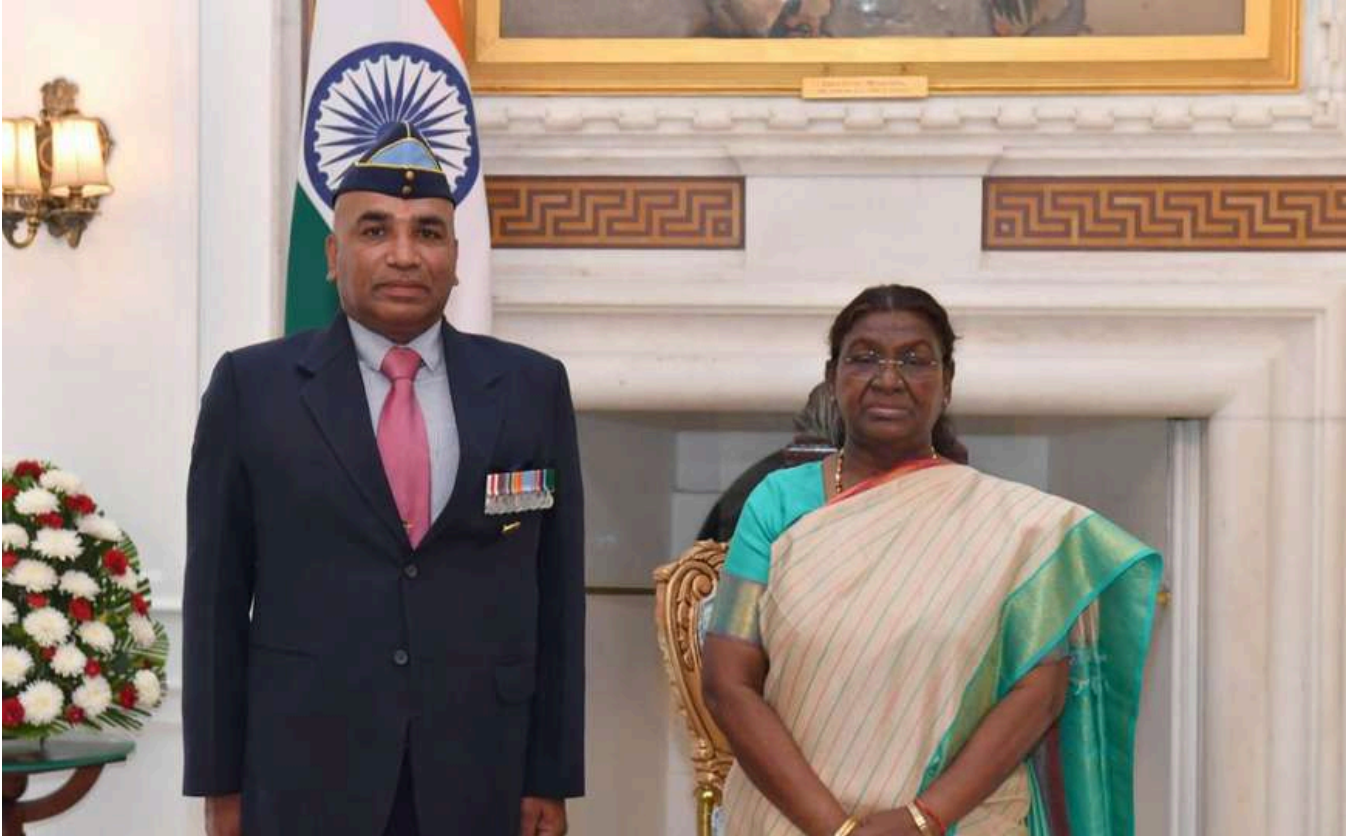
or even two. Take your time - weeks, months, or even a year - but keep writing. Consistency is key. Once you see that your thoughts are starting to take shape, your interest will naturally grow, and you'll begin to see the light at the end of the tunnel. The more you write, the clearer your vision will become, and eventually, you'll find yourself nearing completion. In my case, it took me one year to write my book. I didn't wait for flowery words or the perfect sentences - I simply wrote what was in my heart and mind. I divided it into chapters, gave each chapter a title, and let the story flow. By the end, it became so engaging that people would finish it in one sitting, eagerly waiting to see what happened next in the following chapter. So, my advice is - don't hesitate. Start writing today. Your story is unique, and the world needs to hear it!

**Uday: What inspired you to start writing?**

DD: Writing was never my cup of tea, and it all began with a rather interesting story. I was entirely into adventure sports and military activities, not the literary world. Over time, several articles about me and my achievements were published in newspapers, and I would display them under the glass on my office table, facing the visitor's side. This was my subtle way of sharing my journey with those who dropped by when I wasn't around. One fine day, Mr Rajan Arya, the publisher from Pentagon Press visited our establishment to meet someone. He was sent to my office to wait for a bit. Since I wasn't there at that moment, he ended up reading all those articles about me. When I returned, he enthusiastically insisted that I write a book about my experiences and narrate my journey to the world. At first, I politely declined, saying that writing wasn't my forte. But the publisher kept pursuing me for years, urging me to share my story. It wasn't until one day that he called and said, "Just jot down your experiences on sticky notes and throw them in a bag. When I meet you, I'll make a book out of it." His determination left me feeling a little embarrassed—I hadn't given a second thought to the idea of writing, yet here he was, so thoughtful and concerned about preserving my journey.

That was the turning point. Something clicked inside, and I finally felt the calling from within. I started penning down my experiences. It took me precisely one year to complete the book, get the necessary permissions, and release it. The rest is history. The book, titled "When People Doubted My Ability to Walk, I Decided to Fly", has sold more than 15,000 copies to date. What I never could have dreamed of is how much love and support the book would receive. Readers went out of their way to translate it into Braille, Marathi, and Hindi, and now, I'm honored to say that I recently presented

the first Hindi copy to the President of India. Further translations in Konkani and Gujarati are also on the way. This journey taught me one key lesson: consistency and optimism are everything. You may not see yourself as a writer or a storyteller at first, but when you're consistent, driven by purpose, and believe in what you're doing, anything is possible. This whole experience has inspired me to continue writing. My upcoming book, The Magic of "So What", will be out soon in a few months. I can't wait to share it with the world!



Capt Uday K Shriwas was commissioned into the Corps of Signals, and served in various theaters during his service for five years, including in a newly raised RR Battalion. Thereafter he has worked with many renowned Companies, like Kingfisher Airlines, IFB Home Appliances, JK Cement, and Yes Bank Ltd. He enjoys working in the field of Marketing, Business Development, Strategy. He also has keen interest in the field of Personal Branding. He is presently working as Regional Head - Honour First (Defence Vertical) IDFC FIRST Bank

Please provide your invaluable opinion/feedback on this Interview, by clicking/tapping [HERE](#) - Editor

Moment In Time

We have started with a Photography section “**Moment in Time**” to provide an outlet for creative side of our esteemed members. The rules for submission are as under:-

1. Forces Network members, spouses and their wards can submit images for publication.
2. No Nudity or Porn.
3. No mention of Mil establishments or unit identity or tac numbers or tail numbers.
4. It's a photography section so no images of various get togethers and social functions will be published.
5. The longer side of image should be 2048 pixels.
6. Maximum 5 images will be published every month. The images must be submitted by 20th of every month.
7. Mention your Instagram ID.

8. **While submitting the following details be submitted along with the suitable**

Title:-

- a. Aperture
- b. Shutter speed
- c. ISO
- d. Camera used
- e. Lens
- f. Focal length.
- g. In case of a mobile click, the same may please be mentioned.

All Photos may please be sent to forcesnetworkz@gmail.com by 20th of every month.



© Praveen Kumar

**Orange-Bellied Leafbird Male @Jim Corbett, Uttarakhand -
Canon EOS 700D, Aperture : f/6.3, SS- 1/800, ISO - 320, FL - 552mm
By Lt Col Praveen Kumar**



Indian White-Eye clicked at Jim Corbett, Uttarakhand. - Birds help in Cross Pollination; you can see the pollens on the forehead.

Canon EOS 700D, Aperture : f/5.6, SS- 1/500, ISO - 250, FL - 329mm .

By Lt Col Praveen Kumar



Kingfishers found in India-

Nikon 7500D, Aperture : 4.5 - 5.6, SS- 320 -400, ISO - 250-600, FL - 300 to 400mm

By Wg Cdr Puthur Devassy Joju - @joeymiltonpix



Bird Flower

By Col Bhupinder S Rai



In the City of Gods, Varanasi-

By Col Bhupinder S Rai



**WISHING YOU A
SPARKLING & PROSPEROUS**



**HAPPY
DIWALI**

RUDIAR  LUXE
Custom Diamond Jewellery

94991 84881 / 9321 8393 66
www.rudiarlux.com

Knowledge Bytes

The Deepfake Dilemma: Navigating Corporate and Personal Cybersecurity Threats

BY RUPA MITTAPALLI

Movies have long fascinated audiences with the idea of impersonation and identity manipulation, often relying on high-tech disguises and clever deception to drive their plots. Think of films like *Face/Off* (1997), where two men physically swap faces to infiltrate each other's lives, or the *Mission: Impossible* series, where hyper-realistic masks and



voice modulators allow characters to impersonate key figures to achieve their goals. These cinematic tools allowed protagonists (and antagonists) to outsmart their foes by posing as someone else.

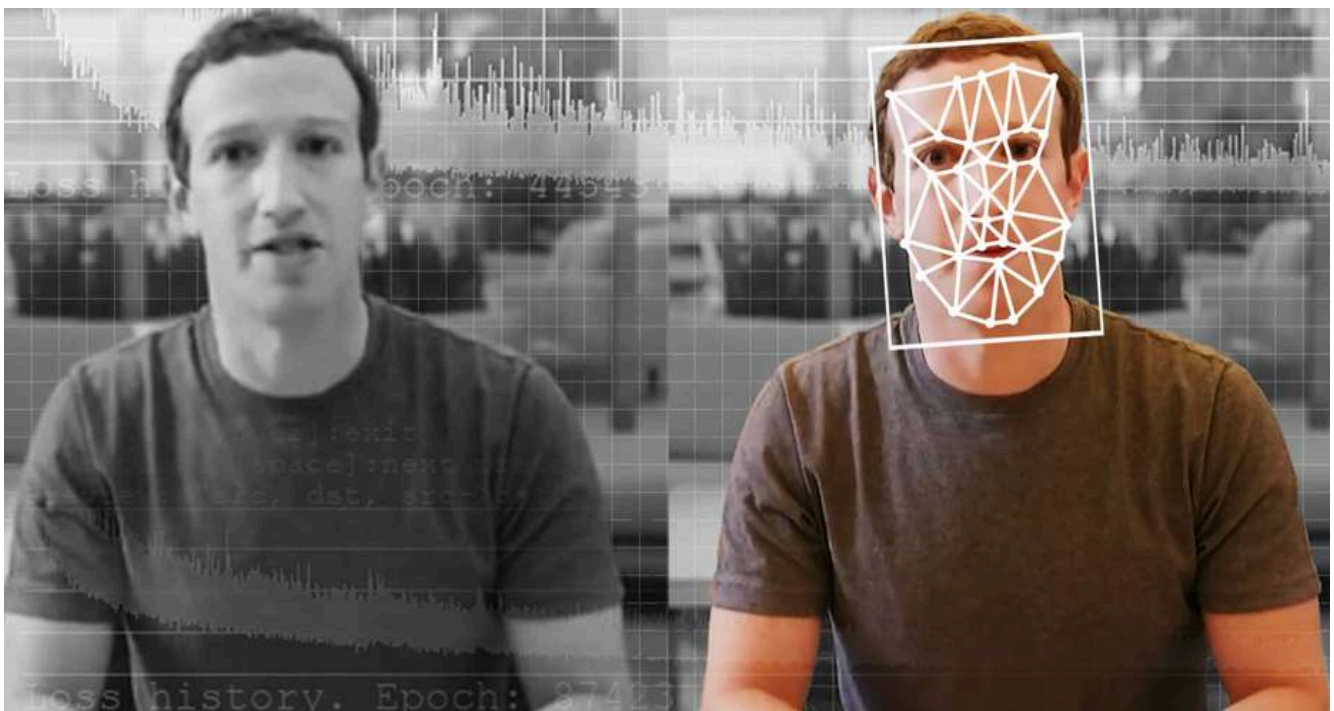
What once seemed like the stuff of fiction has become a very real threat in the digital world today. **Welcome to the era of deepfakes**—a cutting-edge technology that uses AI to create disturbingly realistic images, videos, and voices that can easily deceive even the most discerning eye. Unlike the limitations of makeup or physical disguise seen in Hollywood, deepfakes transcend geographical boundaries and allow anyone to become anyone else at the click of a button.

What does Deepfake do?

Deepfakes rely on Generative Adversarial Networks (GANs) to generate fake content, such as videos, audio, or images, that mimic real individuals. GANs involve two neural networks—the generator and the discriminator—working in tandem. The generator creates fake content, while the discriminator evaluates it. As the two networks compete, the generator gets better at creating more convincing fakes.

What makes deepfakes particularly dangerous is their ability to manipulate voice, appearance, and even behavior of real individuals with startling precision. A well-made deepfake can trick people into believing that a CEO is issuing an order, a public figure is making controversial statements, or an individual is participating in activities he/she has never been involved in. The technology has been used for everything from harmless pranks to corporate fraud and political disinformation.

In 2023-2024, the rise in deepfake incidents has forced us to confront the potential for abuse. Let's explore two key scenarios—one targeting corporate environments and the other affecting personal reputations.



Scenario 1: Corporate Espionage via Deepfake Video Call

The Attack

Imagine a multinational tech company on the verge of a significant merger. During a high-stakes video conference, where sensitive financial details are being discussed, the CEO appears on the call to share important instructions. What no one realizes is that the CEO in the meeting is actually a deepfake, skillfully manipulated to give fraudulent directives.

In this scenario, the deepfake CEO authorizes a major transaction, which redirects funds to a fraudulent account. The attackers, having gained access to sensitive corporate information, sabotage the merger and profit from stolen data. By the time the real CEO is made aware, it's too late—the damage is done, and the company faces reputational and financial losses.

Prevention using GenAI

- **Real-time Deepfake Detection:** AI-powered systems equipped with GenAI can analyze video feeds in real-time. By detecting subtle inconsistencies in lip movement, facial expressions, and voice modulation, these systems could have flagged the deepfake CEO before the damage occurred.

- **AI-Driven Identity Verification:** Integrating biometric verification into video conferencing tools can ensure that participants are authenticated before sensitive discussions take place. This includes using voiceprint analysis and facial recognition, ensuring only authorized individuals are present.

Post-Attack Forensics

- **GenAI Forensic Tools:** After the fact, GenAI technology can be used to forensically analyze the deepfake video, identifying the specific digital manipulations that were made. This can aid in tracing the attackers and building a case for legal action.

Scenario 2: Personal Attack via Deepfake Video

The Attack

Now consider the case of a well-known public figure who is targeted by a malicious deepfake video. The video appears to show them engaging in illegal activity, which is quickly circulated on social media platforms. Despite the victim's insistence that the video is fake, the damage is almost instant. Media outlets pick up the story, and public opinion turns against them. The individual faces not only professional fallout but personal strain as their reputation is severely tarnished.

Even though the video is eventually proven to be fake through forensic analysis, the damage to the victim's career, relationships, and personal life is often irreversible.

Mitigate using GenAI

- **Proactive Threat Detection:** GenAI-powered systems can continuously monitor social media and other platforms for suspicious content. Using AI, these tools can scan for manipulated videos or content that shows signs of tampering before it spreads, allowing for early intervention.

- **Enhanced Content Verification:** Platforms like YouTube, Facebook, or Instagram can integrate GenAI-based content verification systems. These systems would check uploaded videos against verified data to detect fakes and block them before they go viral.

Restoring Reputations

- **Forensic AI Tools:** When an attack like this occurs, GenAI forensic tools can quickly verify the authenticity of the video and help generate legally admissible evidence to show how the deepfake was created, giving victims a way to defend their reputation.

Conclusion: A New Era of Deception

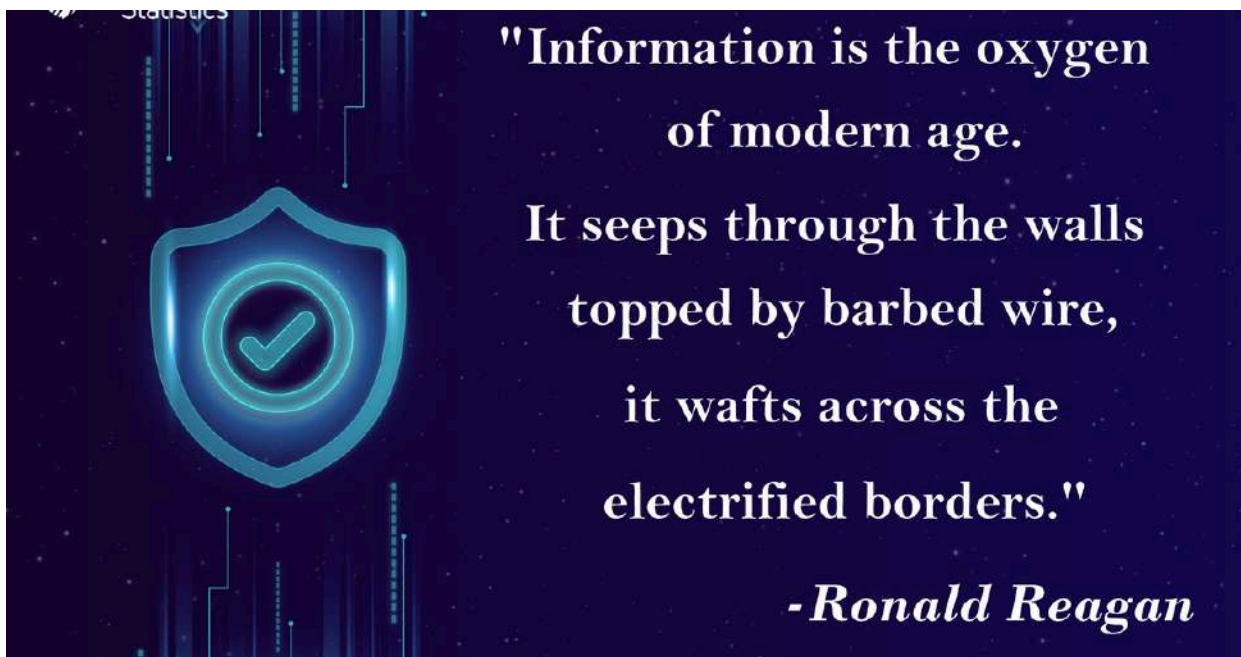
Deepfakes are a modern twist on age-old tactics of impersonation and fraud, but they are far more dangerous due to their digital nature. These AI-generated attacks have the potential to disrupt businesses, damage reputations, and undermine trust in media and communications.

However, by leveraging GenAI as a tool for detection, authentication, and forensic analysis, we can protect ourselves from this rising threat. Just as in the movies, where technology was used to impersonate and deceive, we now have the tools to fight back—if we act fast, stay vigilant, and deploy AI to safeguard our future.



Capt. Rupa Mittapalli, PMP, CISM, is a results-driven military veteran with over 20+ years of experience in Cybersecurity(IT & OT), and infrastructure, specializing in risk management, compliance, and strategic leadership. Currently a Regional Delivery Leader in Cybersecurity at IBM, she brings global expertise across diverse sectors, including IT, telecom, oil & gas, and services.

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor



Knowledge Bytes

Ageing Gracefully

BY DINESH DUTT SHARMA

'Age is an issue of mind over matter. If you don't mind, it doesn't matter'

Mark Twain.

Age has often been referred to as the number of seasons one has seen; the new year's one has ushered in or the number of cakes one has cut—effectively it is just a number and a number which is all in the mind. Older and younger is a relative concept. For a five-year-old, 30 years is ancient and for a person who has crossed 50, 30 seems pretty young. Yet most people fear aging because society has built a hype about it being no less than a demon which is heralded with dentures, bifocals, hearing aids, walking canes, arthritis, Alzheimer's, macular degeneration and what not. In reality it is simply and inevitable biological cycle which revolves irrevocably.

- **Accepting the Truth:**

Whatever may happen in the far-off future, the one certainty with which no responsible scientist can disagree is that there is at present no medicine or magic potion which can combat aging, nor is there likely to be one soon, if ever. Some of our most experienced bio-gerontologists are convinced that no aging gene will ever be found... hence, in Sherwin B. Miland's words, 'the better we use our years, the greater will be the rewards of individuality and accrued wisdom.'

- **Preparing oneself:**

Change is integral to life and accepting this fact helps you to age gracefully. When small things continue to bring joy and yet you see harmony in conflict, you know that you have grown old, but wisely so. When you courageously challenge norms and speak your mind with conviction, you realize that years have added strength to your voice. The key to successful aging is acceptance of the changes that are taking place in the body and the mind. Experts agree that aging gracefully is not always easy but attitude matters a lot. Aging in itself is not the problem but what you think and feel about the aging process definitely is. It is true that the clock keeps ticking, whether you like it or not. Therefore, denial is not going to get you anywhere.

Anticipating the changes that come with aging could help you from being overwhelmed when it does happen. Preparing oneself psychologically for what is yet to come is an art in itself. There is a positive side to aging- it also means you are wiser and are more experienced.

Since we cannot stop or reverse it, we need to learn to age gracefully. Aging gracefully doesn't necessarily have to refer to looks or appearance, but rather the attitude people have as they go through the various stages of life.

- **The Physical Aspect of Aging:**

Your face is marked with lines of life, put there by love and laughter, suffering and tears. It's beautiful. — Lynsay Sands

Profound words indeed! The maturity that comes with this revelation enables you to accept your wrinkles and strands of grey hair with a new found belief in who you are –older but wiser. Unfortunately, our society is obsessed with anti-aging formulas and elixirs of eternal youth in spite of the fact that time and again empirical evidence has proven that physical beauty is skin deep.

We need to accept that the physical signs of aging will make themselves felt. More importantly we need to accept that lines and wrinkles are not a curse or something to be ashamed of. They are the evidence of experience and a life well lived. So one does not need to run to the surgeon and exchange the souvenirs of beautiful experiences for a shot of plastic. Nor do doses of Botox ever make up for the beauty which radiates from within. It is best not to interfere with nature and let it take its own course. Hormonal treatment and invasive surgery may appear attractive measures but are short term pacifiers and are potential risks later on.

However, this doesn't simply mean you have to wear your wrinkles with pride; instead, you can and must do whatever is necessary to stride into your older years with confidence. It means taking steps to make your outside appearance match the way you feel on the inside.

We hear about going 'gracefully grey' and see people around who look awesome with their naturally grey tresses but being graceful about your age does not necessarily mean flaunting your greys. It also does not indicate that beauty aids become taboo. If you feel that dark hair suits you more than grey...go ahead and colour it. After all it's your body temple and you have every right to make it look beautiful. As long as it is not a statement to defy your age; rather an expression of pride that you take in your appearance, go ahead and indulge in it.

- **Accepting Biological Limitations:**

It is an irrefutable fact that the passage of years takes its toll on your body's agility and flexibility. So please don't assume that you can dance the salsa all through the night and wake up the next morning as fresh as a daisy—the way you did when you were just twenty. And don't try to run up that flight of stairs, two at a time. You don't need to prove to anyone that you can do what you could a decade back....least of all to yourself. Remember, what matters most of all is your happiness and not your physical prowess.

- **Strengthening Relationships:**

The most important fact which is usually ignored is that with the passing years we need to take a fresh look at our relationships and social connections. Maturing gracefully brings harmony in relationships because you are less judgmental and readily accept divergent views. It is important to give time to our contemporaries and space to the younger generation whom we have always guided and protected. We need to let them grow out and find their own place in the sky. Most importantly, we need to accept that their horizon will expand and they will spread their wings. But the new relations they weave are not replacements to existing ones but extensions. The new bonds will never be threats to the older ones.

The gentle serenity of our age should enrich all our social and interpersonal interactions--- be it with colleagues, contemporaries or even our household staff. It is our behaviour which will define the respect and dignity which is accorded to us.

- **Making the Most of It:**

With age comes a wealth of experiences. We can actually revel in our abundance of knowledge and dip into it to share with others and guide the younger generation. The old order will change, giving place to new, so whether it is our personal, professional or social life, it is inevitable that the younger lot will overtake us. That is the law of Nature. Instead of resenting the fact that we no longer occupy center-stage, it should be our endeavour to guide and facilitate their growth. The onus is on us to groom the younger lot so that they can carry on the traditions and values of the past, create a glorious present and lay the foundation for the future.

So let us enjoy each new milestone that this journey called 'life' unfolds and revel in every new dimension it adds to our persona because that is what aging is all about.



Colonel Dinesh Dutt Sharma (Retd), a Post Graduate in Geography from Bareilly College Bareilly and an alumnus of Military School Dhaulpur and Chail Shimla Hills. Commissioned in 1985 in Army Service Corps from IMA Dehradun, Qualified in Hospital Management (CHM) and in Finance Management and Audit Sensitization from CAG's International Institute of Noida. The officer had served in Ministry of Defence (Directorate of Standardization). He Commanded Composite Food Laboratory Jammu, had been Col Transport HQ 16 Corps J&K, Col Supply & Transport HQ U B Area Bareilly & Director Recruiting, Army Recruiting Office Muzaffarpur-Bihar, Deputy Group Commander and Chief Administrative Officer, NCC Group HQ Bhopal (MP) and NCC Group HQ Agra (UP). Finally superannuated as Director Administration, Coordination & Automation) Adjutants General Branch. Discipline and Vigilance Directorate (ADG D&V), Integrated Headquarters of Ministry of Defence (ARMY). DHQ-PO New Delhi with 36 years of experience. Performed the duties as Officer-In-Charge Ex-Servicemen Contributory Health Scheme (ECHS) Polyclinics at Greater Noida and Noida from April 2022 to 31 Aug 2024. Presently performing the duties as Deputy General Manager (DGM) Uttarakhand Purv Sainik Kalyan Nigam Ltd (UPNL) Govt of Uttarakhand. Dehradun (UK) India

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor

SecurityLinkIndia

www.securitylinkindia.com ISO 9001-2015 CERTIFIED

(India's Leading Monthly Magazine & e-News Portal on Security, Safety & Fire)

PRINT & DIGITAL

India's Leading & Awarded Media Platform for Security (Physical, Homeland and Cyber) & Fire Safety

The Best Reach to the Indian Market

SecurityLinkIndia
(Print & Online)

✓ Total Readership: 100000+

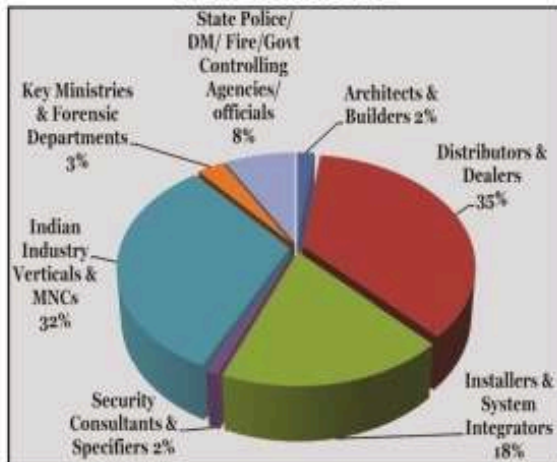
e-Newsportal: www.securitylinkindia.com

✓ Average Monthly Traffic: 400000+

✓ Average Unique Visits: 60000+

✓ E-mail Blasts: 35000+

READERS PROFILE



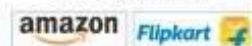
Offering
New Year Discount
on Advertisement &
Annual Subscription
Flat 30%

Exciting opportunity for the promotion of your products and services through advertisements and advertorials

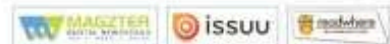
Find us at:-

- <https://www.facebook.com/SecurLinkIndia/>
- <https://twitter.com/SecurityLinkIND>
- <https://www.linkedin.com/in/securitylink-india/>

Recognized by



Online distribution through



Reach us at:

info@securitylinkindia.com; editor@securitylinkindia.com

Knowledge Bytes

If Karma Balances Everything Then Why Bad People Prosper And Good People Suffer !!!

BY TARUN PRATAP SINGH

1. The Misunderstood Nature of Karma - The concept of Karma often seems delusional, incomplete, or something we struggle to fully explain. Many times, we observe that good people suffer while those who are perceived as bad seem to prosper. For a long time, even I used to think the same. However, after understanding the mechanism and the complete system of Karma, I was able to comprehend it much better.

Before I begin to explain the entire concept and mechanism, let me share an anecdote with you.

Once, a young major was posted to the Army Headquarters. Even though seeing a major in Army Headquarters is rare, due to his job profile and past service performances, he was selected for a particular job. During his initial days, as he was adjusting to his new place and learning the work, he ended up staying late one night in the office.

On that same day, as he was wrapping up and preparing to leave the office, he noticed a very senior general standing in front of a shredder, clearly confused. The general was looking at the machine, left and right, trying to switch it on, shaking it again and again, but somehow, he couldn't make it work.

The young major approached him and said, "Sir, may I help you with this?" The general replied, "Oh yes, young man, you know, with this old age, I am handicapped when it comes to technology. In our times, everything was done on typewriters, pen and pencil—none of these sophisticated machines. But these days, everything is done by machines. Sometimes I feel I've grown too old for this." The major smiled and said, "No worries, sir, I'll help you." The general handed him a document, and without much trouble, the major realized that there was a button at the rear of the machine that was switched off. That's why it wasn't operating. He switched it on, and the shredder started functioning smoothly. Once the machine started moving and making noise, the general said, "Ah, that was the problem. Thank you, son, thank you so much."

The major, having fixed the shredder, took the document from the general and put it into the machine. The shredder started working as intended. Then the general said, *"Thank you so much, son. Actually, this is a top-secret document handed over to me personally by the Chief of Army Staff. He didn't trust anyone else with it. Since we have served together in the past, he trusted me. This document needs two copies: one for the Prime Minister and one to remain with the Chief of Army Staff. Please make two copies of it using this photocopy machine."* The major was left in shock.

This was just an anecdote, but in truth, many of us are often like that general. We stand in front of a shredders expecting it to work like a photocopy machine. In the same way, since we don't fully understand the concept of Karma, we often get different outcomes than expected. And because we don't grasp how Karma truly works; we end up blaming it for not functioning properly.

This article aims to explain various aspects of Karma, so you can better understand how it truly operates.

2. The Many Levels of Karma: More Than Just Physical Actions - Karma is neither a complex mechanism nor a philosophy—it's simple. Karma means actions. We all learnt in science that every action has an opposite and equal reaction, but in the realm of energy work and spirituality, every action might not have an "equal and opposite" reaction, but there will always be a reaction. The universe doesn't want Karma to exist—it constantly seeks to balance Karma, which is why we are born and why we die.

If you explore spiritual texts, you will come across the concept that the human physical body is called the "gross body" or "grossest body." This is because it is an accumulation of Karma. If a soul has no Karma left to resolve, that soul won't need to take another human birth. Spiritual texts describe life as a journey to balance previous Karmas and generate good ones.

Here's an analogy: Think of this world as a casino. To enter the casino, you need to buy tokens, much like how we need Karma to enter this world. Good or bad doesn't matter—if you have Karma, you are here. The rule of this "casino" to leave is that, you have to shed all your tokens here. Karma is like those tokens, and as long as we are living, we have unresolved Karmas to balance out. No one on this Earth is living a life free of Karmic debts.

Now, another misconception is that Karma only happens at the physical level. People often say, “That person never uttered a harsh word; he was so humble. But still suffered from mishap.” See Karma means actions, and actions aren’t just limited to the physical level. Karma can be created on mental, emotional, and energetic levels too.

Let me explain further. You would have heard in movies that imagining a crime isn’t a crime itself. But in the spiritual realm, thinking about a crime is even more severe than committing the crime physically. This is because humans have subtle bodies—mental, emotional, and energetic bodies. If Karma is created on these levels, it can manifest into a larger karmic debt than physical actions alone.

So, if you are mentally, emotionally, or energetically creating negative Karma, be mindful—it will still have repercussions. Karma is simple: every action, no matter the level, will have a response. For instance, if you speak kindly to people but mentally or emotionally harbour negative thoughts about them, you will experience stress, anxiety, and other psychological issues.

This is why forgiveness is one of the most powerful therapies in the world. Techniques like Ho'oponopono revolve around this concept. Most people are unaware that Karma also operates on mental, emotional, and energetic levels. Try it out—if you repeatedly commit negative mental actions, you will face the consequences or vice versa.

As an energy healer and practitioner of various energy healing modalities, I have seen how quickly mental and emotional Karmas affect the energies of the human system. As experiments we have even tested out by saying bad words on mental and emotional levels and checked the energy of our systems during workshops to validate this. I still remember when one of my seniors wanted to test the efficacy of this particular thing and I told him to write ill and good word on 4 pieces of paper. And when I scanned, I was able to find out the good paper and bad paper. Because those papers had different energies in them.

So, always remember that Karma is not just about physical actions—it’s also about what happens mentally, emotionally, and energetically.

3. Intention: The Driving Force Behind Karma - Now, another crucial aspect that people often overlook is the role of intention. Karma is indeed Karma, but there's an account holder for it, and that account holder is Intention.

To explain this, consider this analogy: if Karma is a vehicle, Intention is the driver. You might have a powerful, sophisticated vehicle, but if the driver isn't clear on where to go, the vehicle will inevitably reach the wrong destination. Similarly, even if you're performing Karma that you consider "right" from your own context, but if your intentions are misaligned, that Karma will not manifest positively.

Let me explain this concept from a Fauji (military) point of view. There were two officers, Person A and Person B, both of whom took command. They shared one common trait: they were both highly disciplined and strict about their physical routines. They placed a great emphasis on physical standards, always striving for excellence and demanding the same from their troops.

Upon assuming command, both officers made it clear that no one in their regiment would be allowed to fall below the required physical standards. As a result, their respective regiments saw significant improvements in physical fitness within a short time. Both units raised their bars, and the soldiers embraced the higher physical expectations. The outcome was the same—both regiments excelled physically.

However, despite the identical outcomes and actions, the Karma accumulated by both officers was different. Let me share how !

Person A, during his early years of service, realized that many veterans—whether they were JCOs, jawans, or officers—suffered from physical ailments after leaving the Army. Many of them, unfortunately, passed away within a short period after retirement. Why? Because they neglected their physical health while they were in service. This observation left a lasting impact on Person A, who began to value physical fitness deeply. He developed a strong belief that when he will take command, he would raise the physical standards in his unit and ensure that everyone understands the importance of maintaining their health. His intention was to protect his soldiers' long-term well-being.

On the other hand, Person B had a different story. He was physically weak during his early service and often failed in many tasks, leading to humiliation. This experience embittered him, and he carried a grudge. He decided that when his time to command will come, he would ensure that his soldiers would never sit aram se (with ease). He believed the only way to control people was to keep them constantly engaged in physical tasks and to make them endure physical hardship. His intention was rooted in making others suffer as he had.

Now, while both officers raised the physical standards in their units, do you think the Karma they accumulated was the same? No, it wasn't. On the surface, their actions may appear identical, but their intentions were entirely different. Person A's Karma would be positive because his intention was to promote the long-term health of his soldiers, while Person B's Karma would be negative due to his desire to impose suffering on others.

This is the power of intention. Even though actions and results in the physical world may be judged based on right, wrong, good, or bad, however Karma operates differently. If your intention behind creating Karma is wrong, you will never reap the positive outcomes of your actions.

If your intentions are not right, even if your actions appear justified to you in a certain scenario, Karma will eventually correct the imbalance. Your intentions must align with the right perspective, or Karma will take care of it.

4. Right vs. Wrong: A Matter of Subjectivity, Correct vs. Incorrect: A Universal Truth - Now, let's talk about the concept of right and wrong. When we discuss right and wrong, it becomes a highly subjective matter. Anything viewed from the lens of right and wrong can never truly be justified, because it will always be influenced by personal perspectives. The human mind is so prone to distortions that it creates scenarios based on individual attributes, making it hard to have a universal understanding of what is "right" or "wrong."

What we need to focus on instead is grading situations as correct or incorrect. When I say correct and incorrect, I refer to actions that are objective in nature. These are not influenced by subjective views but are instead universally understood in light of all those involved.

Let's now take the example of Bhishma Pitamah. According to the texts, he never did anything wrong in his life, even in his past lives. He was always considered a righteous person. Yet, at the end of his life, he died on a bed of arrows, enduring immense agony. Why? Because, when it was necessary to intervene and stop the injustice occurring, he remained silent (Draupati's Cheerharan). And he did so intentionally.

While it's not explicitly written in the texts, Bhishma Pitamah's own perspective played a role in his decision. As a loyal part of the Kauravas, he believed that going against his allies or the people he supported would be wrong. His actions were guided by his perception of what was "right" at that moment. However, Karma doesn't operate based on right or wrong. Karma functions on the principles of correct and incorrect. When the time came for him to face the consequences of his actions, the universe responded in the form of his suffering on the bed of arrows.

Karma doesn't evaluate actions through the subjective lens of right and wrong because, in our individual perceptions, what seems right to us may seem wrong to someone else. Even Chanakya has stated, "There is nothing good or bad. If you take good out of something, it becomes bad. If you take bad out of something, it becomes good."

Right and wrong are always subjective, varying based on personal stories and points of view. What may be right in your own story could easily be perceived as wrong in someone else's. That's why, whenever you perform any action or Karma, you should always judge it based on whether it is correct or incorrect.

Never evaluate your actions based solely on your subjective perception of right and wrong. Adopt an objective viewpoint when making decisions, because when Karma comes back to you, the universe will judge your actions based on correctness, not your personal perception of right and wrong.

5. The Non-Linear Nature of Time in Karma - Now, let's talk about the timeline. I've explained this concept in one of my previous articles, How Astrological Prediction Can Fail and You Can Win. However, I'll summarize it briefly here.

Any event that happens in our life is driven by four primary elements: time, space, intention, and energy. The first element, time, is not linear, nor is it universal. If you delve into scientific fields such as quantum physics, celestial studies, or astronomy, you will find that time doesn't flow in a straight line. In

astrology, the concept of Dasha supports the idea that time functions differently for each individual.

For instance, a person who is sitting with their love will perceive time differently compared to someone going through hardship. Time, in its essence, is subjective to the experience and circumstances of the individual. This variance in perception is how time works for each of us. So, when you observe that good people seem to suffer while bad people appear to prosper, it's important to understand that time functions differently for each person.

What you may interpret as someone prospering despite their wrongdoings is actually a result of the difference in your timelines. You might be working off some old Karma while that person is in the process of creating new bad Karma. Both of your timelines have simply crossed paths in this moment, allowing you to witness the disparity.

When you understand that your soul has been traveling through lifetimes for thousands of years, facing challenges along the way, you begin to grasp the larger picture of why certain problems exist in your life today.

6. Reaping and Sowing Karma: A Call for Constant Self-Improvement - So, I hope you now understand the essence of Karma. The whole point of grasping the concept of Karma is to realize one simple truth: no one in life is exempt from problems. It's impossible to live a life without challenges. The nature and areas of problems may differ, but difficulties will always exist. The reason is simple - we all are reaping / gathering karmas.

Personally, I believe in one principle above all: we should constantly work on improving ourselves. This is the only way we can reduce and resolve our Karma. At the same time, we should focus on sowing the seeds of good Karma for the future. According to many spiritual texts, we are living in Kalyug, which has a unique characteristic. Unlike in Satyug, where people who committed wrongdoings in one life would suffer in a completely different birth, Kalyug brings a more immediate reaping of Karma. If you commit an action today, you will likely face its consequences in this very life. At most, you may experience it in the next birth, but Karma will not stretch across multiple lifetimes.

7. Method To Dissolve Karma - The best method to create a better life for ourselves begins with identifying which aspect of our life is most affected. Once you can gauge which area of your life is facing the most challenges, you can start focusing on it. This could be any area—health, relationships, finances, manifestation of desires, or spirituality.

If you truly want to understand time and Karma more deeply, I recommend my article *How Astrological Prediction Can Fail and You Can Win*, where I explain in detail the four elements of events happening in our lives. But for now, from a layman's perspective, I'll guide you through a process that can help you resolve your Karma and create a better life.

The first step is to home in on the area that's most affected. Once you identify the troubled area, the next step is asking the right questions. Asking the right question is crucial because, in my experience, many people ask the wrong questions and, consequently, don't receive the answers they need. The wrong question will always lead you to the wrong answer, which will never clear your path.

For example, if your roof is leaking and you keep asking, "Why I am suffering from a leaking roof?" over and over again, you won't find a solution. Instead, the first question you should ask is, "How can I fix this problem?" Once you've solved that, you can ask, "Why did this leakage start?" This approach will lead to better answers. However, if you get stuck in a cycle of asking, "Why me? Why am I suffering from a leaking roof?" you'll only become a victim instead of finding the solution. This question will not help you move forward.

So, the first step is to ask the right question. If there's a problem in your life, understand that there's some Karma requiring resolution. Once you identify the aspect of life being affected, begin asking, "How can I get rid of it?" If you consistently ask this question, the universe will answer. The universe is very simple.

Let me give you an example. If I ask you why one magnet attracts another magnet, you might say it's because of the concept of magnetism and the interaction between the North and South Poles. But the core reason is much simpler: one magnet resonates with an energy that the other magnet understands, which causes them to attract. The same concept applies to the universe. If you resonate with a specific energy, the universe will understand that energy and respond with the necessary actions.

So, if there's an area in your life that's badly affected, no matter which aspect, begin by asking the right question. The first question should always focus on finding the solution. If you keep asking for the right solution, the universe will deliver it. And once you receive the solution, the universe will also deliver the why behind it. When you understand both the how and the why, the problem will disappear as if into thin air.

Conclusion - As we journey through life, may we all find the wisdom to resolve our Karmas with grace and clarity. Let us constantly seek the right questions, allowing the universe to guide us toward the solutions we need. May we be blessed with the strength to improve ourselves every day and embrace the lessons life offers with humility and courage.

I wish you all good health, boundless happiness, and spiritual growth. May your relationships flourish, your desires manifest with ease, and your path to abundance be illuminated. May the universe shower you with prosperity, peace, and love, allowing you to live the best version of your life. May we all walk this journey together, reaping the rewards of our positive Karmas and creating a future filled with joy and fulfilment.

Blessings to each of you on this beautiful journey of life.



Maj Tarun Pratap Singh

Founder Sanidhya

Energy Coach & Spiritual Guide

Qualified Teacher from Diana Cooper

School of White Light (UK, Britain)

Certified Oracle Card Reader

Astrologer

Numerologist

Vaastu Expert

Please provide your invaluable opinion/feedback on this Article, by clicking/tapping [HERE](#) - Editor



LOOKING FORWARD FOR THE FORCES NETWORK GATHERINGS ACROSS THE GLOBE;

Incase you do, don't forget to share the photos along with Names

Do you desire to be a Member of this awesome Group, which is not restricted by National boundaries?

Forces Network is a 'Closed Group'. It is open only to the Commissioned Officers of the Indian Army, Air Force and Navy.

One can join only after being referred or sponsored by an existing Member of the Group.

For more information and details, visit: <https://www.forces-network.com/>

