

FORCENET

E-ZINE

Magazine for military veterans in the corporate
November 2022, Volume IV, Issue 11

CYBER SECURITY



**FORCES
NETWORK**

THE NETWORK THAT WORKS

FOCUS | PASSION | IMPACT

SCAN ME



FORCENET

From the Editor

Dear Readers,

From Google Pay to Amazon shopping to online classes to WhatsApp, a common man's life today is full of internet or the virtual world. The cyber world gets us a host of benefits but there are downsides as well like cybercrime and cyber hacking. This is definitely a challenge but can also be viewed as an opportunity, especially for veterans. Veterans are a natural fit in cyber security post some upskilling. This is the reason that we have chosen **"Cyber Security"** as the theme for this month's magazine.

India's Internet usage stands at 14.1GB/Month with the internet usage base crossing 830Mn mark as per Economic survey 2022. Covid and subsequent Work from Home (WFH) ensured that the usage of internet increased more for people at home, as also the number of attacks by ransomware and viruses. With 18 Million cyber-attacks and 2,00,000 threats a day in the first quarter of 2022 alone the threat landscape is staggering. There is need for a strong cyber security, this has been felt by governments, big corporates, small businesses to retail users.

Cyber Security is the protection of internet connected systems including hardware, software and data from cyber-attacks. Cyber security can be of several types like network security, cloud security, mobile, IoT, application etc. The sector is fast growing with low unemployment, the compensation is also good in addition there is a huge opportunity to grow.

Forces Network has been propagating for more than 3 years now that Cyber Security as a career is a very good option for veterans. Forces Network has conducted several training webinars on this subject as well in the past. Many of our members are already doing exceptionally well in this field - look around and you will find that a large number of CISOs are veterans.

In this Issue our Founder Col IQ has penned an article which explains why veterans must look at cyber security as a career seriously. Several upskilling pathways have also been shared in this article. Even if you feel you are non-tech or working in a non tech organisation Cyber Security not something that can be ignored any longer. Even non-tech people can make a career in it with some upskilling effort.

Happy Reading – this Edition could be life changing for some.

Jai Hind



Yours CyberMan,
Capt Rajesh Nair

13th Raising Day

November 1st, 2022

Thank You All



We are celebrating the **13 glorious years** of Hum Fauji Initiatives and celebrating the auspicious element of **Trayodashi** as we complete 13 years of being the exclusive '**prosperity managers for armed forces officers**'.



Number 13 portrays focus, independence, creativity and a secure foundation. It always completes the full cycle of life. There are 13 cycles of the moon, 13 weeks each of the four seasons we have, the teenage years start at 13.

We bring to you 13 Great Offers this year, starting November 2022.

Stay Tuned and subscribe here, www.humfauji.in

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



Hum Fauji Financial Services Private Limited

Visit at : 2nd Floor, Bimal Plaza, Sector 11, Dwarka, New Delhi - 110075

+91-9999053522 , +91-9999838923 (SMS & WhatsApp)

www.humfauji.in

By the Faujis. For the Faujis.

EXCLUSIVE
INVITE



studio pepperfry

Hazratganj, Lucknow

Saluting The Defence Forces

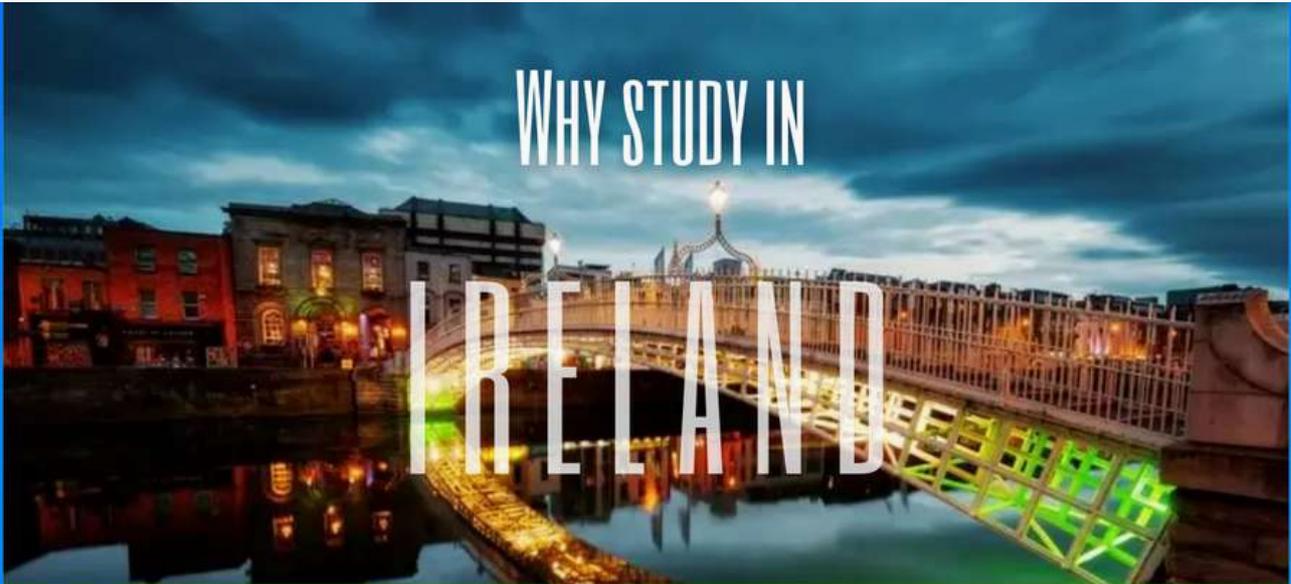
Contact Now

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

studio pepperfry

Sapru Marg, Hazratganj, Lucknow

☎ 9305216506



World-class education ... Steeped in history
 Education is in the DNA of Ireland
 Second largest exporter of software in the world
 Second highest GDP per Capita in the world after Luxembourg
 Highly ranking universities ... globally

WHY US?

We help students to study medicine in Europe
 We are specialists for Critical Skill Work Visa and Post Studies Visa
 We support students to integrate with European countries

Our students are a part of a vibrant community currently enrolled in the following universities/colleges:



A student recruiter with a difference!

HEPTA CONTINO INC | WWW.HEPTACONTINO.COM
 +353 8949 14324 / +91 72176 26824 | HEPTAINFORMATION@GMAIL.COM



CYBER SECURITY AS A SECOND CAREER

Convergence of Security and Cybersecurity Fields

Get hands-on cybersecurity training from ISAC for a second career in the cybersecurity field. Checkout this roadmap that ISAC offers for retired armed forces personnel to transition into the corporate world.

Foundation

Cyber Crime Intervention Officer (CCIO)

Basics of Information Security (ICBIS)

Cyber Psychology (ICCP)

Intermediate

Penetration Testing (ICPT)

Bug Bounty Researcher (ICBBR)

SOC Analyst (ICSA)

Specialist

Forensics Investigator (ICFI)

Reverse Engineering (ICRE)

Malware Analysis (ICMA)

Techno Managerial

Privacy and Data Protection Officer (CPDPO)

Cybersecurity Governance Professional (ICCSG)

National Cybersecurity Scholar (NCSSP)



The CCIO course was real eye opener on the various connotations in cybercrimes which can affect anyone. It gave tremendous knowledge in various aspects of cybercrimes and how as an individual I can help the society affected by cybercrimes in a better way. The guidance provided by Mr Sreeshankar and Gp Capt P A Naidu was immense during the course

Wg Cdr K Venugopal (Retd)



The ICBIS course has been excellent. Couldn't have asked for more. Murugappan sir as an instructor has been the best instructor I have been fortunate to be associated with. The course content is curated well. The interactive methodology was indeed very useful. Thank you for everything !!

Col Sanjay, Indian Army

About Us

Information Sharing and Analysis Center is India's leading cyber security non-profit foundation and a Partner with Ministry of Education, Government of India, AICTE, CERT-IN & KDEM.



Contact Us:

+91 8317344662

support@isacindia.org

www.isacindia.org

RAXA ACADEMY
Centre of Excellence for Higher Learning in
Security & Safety
Training Today for Securing Tomorrow

RAXA Academy is an ISO 29993:2017 and ISO 45001:2018 certified training institution of Raxa Security Services Ltd, an ISO 9001:2015 and ISO 18788:2015 certified GMR Group company. The Academy is spread across 100 acres amidst sprawling meadows, the best-in-class training and administrative infrastructure and has been designed aesthetically with modern amenities to cater to the needs of trainees seeking an invigorating and rejuvenating training experience here. We offer the following courses for transitioning officers/ personnel from the forces.

Advanced Security Management Course is designed to cover the security management, security risk assessment, physical and electronic security as well as the emerging technology in security management, cyber security, health & safety and crisis, emergency & incident management, Intelligence, Investigation and legal aspects of security.

Intended outcomes:

- Understand concept of Security Risk Management
- Update knowledge on Physical Security & Cyber security
- Acquiring skills in Security Management & Security Technology Systems Fundamentals
- Understanding Security Intelligence Management and Security Investigation Management.
- Attaining awareness on Emergency and Crisis Management & Conflict Management
- Knowledge of the legal aspects related to security.
- Skills to Conduct a Security Survey /Audit and Discussion of Case Study on Security
- Understanding Managing health and safety at the Workplace

Ex Servicemen Corporate Security Management Programme is designed to groom the personnel who intend to join security domain. Curriculum is designed on the POA (ASIS Protection of Assets manual) which is recognized as the "Gold Standard" for the security professional worldwide with additional inputs on security and safety matching the need of the hour. Successful completion of the course will provide the participants with fundamental competencies in security field.

Intended outcomes:

- Understand the concept of Security Management.
- Acquiring knowledge and skills in security operations & management of a security unit
- Acquiring skills in Risk assessment and Management.
- Understanding Security Technology Systems.
- Proficiency regarding material and information security.
- Attaining awareness on Emergency and Crisis Management & Conflict Management
- Knowledge of the legal aspects related to security.
- Proficiency in firefighting and safety.

Drone pilot Training and Industrial Level Training is intended to impart DGCA approved Drone pilot training to aspirants. The advanced programmes in Industrial level training will provide expertise in survey mapping, agricultural uses of drones. The emerging market for Drone as a service is expected to grow at a rapid rate and we aim to capture the market for our candidates.

Intended outcomes

- Different types of Drones & illustration of Fundamentals of flight (Aerodynamics).
- DGCA Safety Regulations & safety guidelines, ATC procedures & Radio Telephony, Weather and meteorology
- Designs of drones and power systems, Controllers, Transmitters, Receivers & Flight controllers.
- Payload considerations like: Cameras, Gimbals & usage in drone flying/ maintenance.
- Understanding Ground Control Stations (GCS) & FPV.
- Drone flight simulator and simulator training.
- Understanding GIS data Formats, Design and Quality, Acquaint with Geospatial and environmental Analysis.

IOSH Managing Safely® is one of the most popular health and safety certificates in the world. It's designed to bring the delegates up to speed on their health and safety responsibilities and help them develop the practical skills to manage risk on a day-to-day basis. This level of safety competence will lead to international recognition for the individual as well as the organization to which they belong. Being an Approved Training Provider of IOSH (Training Provider # 4644), Raxa Academy is happy to offer the 22 hours flexible and highly interactive training package for individuals and corporates.

For Registration and further details on the course and schedule, please contact:

Mr. Yadu Menon - GradIOSH, Manager;	Mob- +91 9391333183;	Email: yadu.menon@gmrgroup.in
Mr. GGK Nair, AGM;	Mob- +91 7093261904;	Email: Gopalakrishnan.NairG@gmrgroup.in
Mr. Muni Prasad, BD Executive;	Mob: +91 8019888907;	Email: Muni.Prasad@gmrgroup.in



[CLICK HERE FOR REGISTRATION](#)



Are you looking for?



Returns!



Active Monitoring



Liquidity All Throughout



Diversified All Weather Portfolio



Tactical Asset Allocation

Personalised Financial Solutions



 S-15, Manish Global Mall,
Sector-22, Dwarka, New Delhi-110077

 info@finvision.in

 +91-7508055826
+91-9654341212



The Winning Edge

Mentoring For Success

CONTACT US FOR

- 1 **RIMC Coaching**
- 2 **Sainik School**
- 3 **Military School Coaching**
- 4 **SSB Coaching**
- 5 **NDA/CDS Coaching**
- 6 **ASIS Certifications (CPP,PCI,PSP,APP)**
- 7 **United Nations Placement Guidance**

CONTACT US AT



+91 8279908864
+91 7999356350



thewinningedge.career@gmail.com



571D Garhi Cantt (Near RIMC)
Dehradun



AUTHORIZED TRAINING PARTNER OF PMI®



SIX DAYS OF **LIVE** PMP®



ONLINE BOOTCAMP



GAUTHAM SUDAKAR

PMP®, PMI-ACP®
PMI Approved PMP® Trainer
& Mentor at EDUHUBSPOT



- DELIVERABLES**
- PMI® Approved 35 Contact Hours**
- PMP® Exam Simulator**
- 1170+ Practice Questions**
- 67+ Chapter Videos & Podcasts**
- 1200+ Chapter Slides**
- 210+ Real PMP® Questions by PMI®**

Sat 12 NOV	Sun 13 NOV	Sat 19 NOV
-------------------------	-------------------------	-------------------------

DAY 1 DAY 2 DAY 3

Sun 20 NOV	Sat 03 DEC	Sun 04 DEC
-------------------------	-------------------------	-------------------------

DAY 4 DAY 5 DAY 6

5.30PM - 1AM(IST)



~~Rs. 30,000~~
Rs. 21,000
To Avail Your 30% Discount
Email to Soumya Ghatak
@

✉ SOURMYA.GHATAK@EDUHUBSPOT.COM



🔍 WWW.EDUHUBSPOT.COM

📞 +1(833)338-7768
✉ services@eduhubspot.com

74065 81681
www.nyatigroup.com



KUCH FARZ HAMARA BHI SWABHIMAN

Kuch Farz Hamara Bhi

SWABHIMAN

An **EXCLUSIVE HOUSING INITIATIVE** for **DEFENCE PERSONNEL** by Nyati


PREFERENTIAL PRICING


NO FLOOR RISE


ASSURED 24 MONTHS RENTAL*

INTRODUCING



ONGOING PROJECTS IN PUNE

EVOLVE
MAGARPATTA

ELYSIA
KHARADI

ELAN
WAGHOLI

EXUBERANCE
UNDRI

ERA
DHANORI

 6th FLOOR, NYATI UNITREE, NEAR GUNJAN THEATRE, NAGAR ROAD, YERAWADA, PUNE - 411006, INDIA.



Disclaimer: The information on this advertisement is provided "as is" without any warranties, express or implied, including but not limited to the implied warranties for a particular purpose, or non-infringement. Nyati Group makes no representation or warranty that the information contained on this site will be timely or error free. Nyati Group has not reviewed all the sites that may be linked to its site and does not endorse and is not responsible for the content of a 3rd site pages or any other sites linked to these sites. Your linking to each site is at your own risk.

MOUNTAINS CALLING PEACE FOR YOUR BODY AND SOUL



PRICE
**2.5
crore**
ONWARDS

**The
Dak
Bungalow**

Expertise of an
ex Armed Forces Officer and MDI Alumni

CAPT VIPUL CHOUDHARY

MDI, GURGAON CLASS OF 2008

OLIVE GREEN
CONSULTANT

7840080900 | vchoudhary@olivegreenrealty.com

LUTYENS HABITAT

LEASING WORKSPACES & HOMES FOR 15 YEARS

How COVID-19 has Transformed the Corporate Real Estate Ecosystem:

- 25% Workforce to permanently Work From Home
- Resulting in Reduced Office Space Requirement
- Resulting to Higher Vacancy/ Availability of Office Spaces
- Resulting in Reduction in Rental Rates to the tune of 20%
- Resulting In New Interior Concepts With Floating Desk

SO, SHOULDN'T YOU SHIFT POST COVID?

&

Save Upto 40% Rent!!

Use the Covid-19 slowdown to your Advantage

Maj Dhir Singh

☎ 9999007829

✉ dhir@lutyenshabitat.com

LUTYENS HABITAT

LUTYENS HABITAT PVT. LTD.

Sector 27, Golf Course Road,
Gurugram, NCR.



This festive season, gift
your family

FINANCIAL FREEDOM

Invest right and safeguard
your investments to meet
your financial goals,
recession or not



Reach out to Fauji Wealth to learn
more...

 9354266573

 www.faujiwealth.in

 support@faujiwealth.in

 Vardhman Bahnoff Plaza, Sector 12,
Dwarka, New Delhi



Choose the **right health plan**
before making **vacation plans.**

#ZindagiKoClaimKarLe



**Director of Galaxy Associates
Business Partner with
Niva BupaHealth Insurance
COL.R. SRINIVAS(Retd)
7400160159**



Pain and Spine HOSPITAL

"A Unit of Surange Healthcare North India Pvt. Ltd"



=FIRST IN INDIA= **CHRONIC PAINS** **SPINE AND JOINTS**

HOSPITAL WITH END-TO-END SOLUTION



+91-7028195111 | SECTOR -19, DWARKA | www.ipscindia.com

Contents

From the Editor	2
Star of Forces Network: Maj Sanjeev T	18 - 22
Cyber Security An Ideal Career choice for Veterans: Col Iqbal Singh	23 - 34
General Humour : Col Amit Dalvi	34
Rising Star - Shining Bright: Vansh Luthra	35 - 36
Moment In Time	37 - 40
Know the Price of a Cyber Attack: Col Iqbal Singh	41 - 46
Solar Power: An Insight II: Capt Rajesh Nair	47 - 57
The vortex – A true story of History’s Deadliest Storm, an Unspeakable war, and liberation: Col Arun Hariharan	59 - 62

[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/clicking on them.

For the ease of providing a 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. The facts and opinions appearing in the articles thus do not reflect the views of Forces Network, and Forces Network does not assume any responsibility or liability for the same.

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 UDAY SHRIWAS

Maj Sanjeev T born in Kerala and grew up all over India had served for 13 plus years in the Army post getting commissioned in 14 JAT. Post Army its been 18 years in the Corporate world. During his tenure in the Army which included tenure as the Ceremonial Battalion in Rashtrapati Bhavan and been GSO 2(MIS) in Corps HQ. He had the opportunity to roll out LAN across the Corps zone from the Corps HQ to Bde HQ. A techie work done by an Infantry Officer. He has worked with many MNC in his corporate carrer. Currently he heads the Corporate Real Estate (CRE) vertical for Legato Health Technologies LLP (APAC) based out of Hyderabad.



Uday: Please tell us something about your background prior to joining the Army, and your subsequent Army career?

Sanjeev: I am a son of an Army officer and grew up in cantonments, Had six different schools and did my graduation from Nagpur University. I was commissioned in Jat Regt in Aug 1990 and served for 13 years. During my service I had served in Punjab at the height of militancy in 1990 and 91, like every Infantry officer served in North East and the Valley. My best two tenures being the ceremonial Battalion in Rashtrapati Bhavan (RB) and GSO-2 -MIS in Corps HQ. The Rashtrapati Bhavan tenure was great as it gave me an opportunity to meet visiting Heads of State. I have had the privilege of meeting Nelson Mandela.



With President of India 1994

Uday: Give us an understanding about your role and what you are presently engaged in?

Sanjeev: I am the Director for CRE (Corporate Real Estate) for Legato Health Technology, which is GCC (Global Capability Center) of \$140Billion US based Health care company.

Uday: How did you prepare yourself for the military to corporate transition?

Sanjeev: I did not. I became a Cat C and decided to leave the Army after serving for 13 years. I was fortunate, as my wife was working and thus took the risk of leaving the Army. Looking back, I would have done things differently. I learnt the skillset on the job.

Uday: What were the challenges faced during your transition? How did you overcome the challenges?

Sanjeev: There were challenges, however Army teaches you Flexibility and Adaptability. This was my mantra to survive in the civil street along with willingness to learn.

Uday: How has been your experience in the corporate domain so far?

Sanjeev: I have had a great run in the Corporate world. The only thing that matters is performance.



With Team in Office

Uday: Academy Training teaches us a lot and it prepares us for our future life. What has been your biggest take away which has been really a big lesson even as you take up challenges in corporate life?

Sanjeev: The biggest lesson for me was "Never give up" and "short cuts do not work".

Uday: How important is it to understand your own expertise and then to work towards upskilling in that domain so as to have a Better Outing in corporate?

Sanjeev: As soldiers we have certain skills, like ability to get to the root of the issue, simplify complex issues, ability to work hard and work in a team. Upskilling and domain skills are paramount once you join any Industry. Without the domain skills, one is like duck out of water.

Uday: There must have been great lessons during this tremendous journey after hanging the spurs. Can you share a few from your experience?

Sanjeev: My lessons from my experiences is, "Never hesitate to ask for help" and do not be afraid to say "I do not know"

Uday: Wisdom is the ultimate for a Leader? Do you agree ? And how you would like to define a Leader ,what Values drive you as a Leader?

Sanjeev: My definition of a Leader is one with the ability to listen. My value system is Integrity and Honesty in everything that I do.

Uday: The VUCA world is a huge learning experience for all of us. Could you please share how much the present world situation has impacted your professional world? And what is your insight and suggestions to our readers?

Sanjeev: We are living in a complex world but that is not something we can control or influence. Thus, do not waste time worrying about issues beyond our area of influence. My focus is on the work that I do and manage the challenges that is coming my way and always look beyond the horizon.

Uday: We all have had great mentors and coaches in our Lives? Would you like to talk about them from your Journey in Fauj and in Corporate?

Sanjeev: I had Two great mentors one in the Army and one in Corporate.

In Army, my Commanding officer when we were in valley. He told us the following lines: "*All your success is your and all your failure is mine*" This were not empty words. When we got success, he gave credit to the officers involved but when we had a big challenge and something went wrong in an operation, he just said "*I am responsible*". I am sure lots of CO in his place would have put all the blame on the officer.

In the Corporate my mentor told me; you do not have to fix all the problems. Asking for help is a right thing to do and not a sign of incompetence.

Uday: Do you have any other hobbies or interests, which you pursue passionately? And how?

Sanjeev: My wife and I have over the last few years been associated with a NGO who works for orphans. We help them with advice and some volunteer work. I am also keen to help fellow soldiers. I have over the last few years purchased painting by soldiers who are paraplegic for my organization and showcased their talent. The paintings are from Pune Paraplegic center, Kirkee. All the money we paid for the painting went to the soldiers. I am amazed but their ability to bounce back to life.



My wife with the NGO

Uday: Top 5 Qualities that you feel are very important for excelling in the corporate world?

Sanjeev:

1. Flexibility
2. Adaptability
3. Do not hesitate to ask for help.
4. Keep learning and keep upskilling
5. Do not bring your Rank to the Corporate world.

Uday: One question that you think every officer should ask himself/ herself while preparing for his/her career after Fauj?

Sanjeev: Do a honest self-assessment about your skill.

Uday: Your views on the role played by Family, Friends and Well-Wishers in the Transition and in future assignments?

Sanjeev: I left Army because my wife was working and like a good Inf man, I had one leg on the ground. My first job was courtesy a fellow Army Officer. Thus, it has been my endeavor to help others in uniform. Most Civilian/Corporate world do not care about us, thus we need to help each other.

Uday: Thank you for your time and for sharing your experience with us.



My wife Nandini and son Utkarsh



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

Cyber Security An Ideal Career Choice For Veterans

BY IQBAL SINGH

Introduction

While each career is a lifetime learning and investment and most people rarely switch industries or sectors in the civilian workplace the military veterans have a steep ask of switching careers midway through their lives. This is by no means an easy endeavour. In addition enhancing the degree of challenge is the fact that these jobs are competitive and veterans need to compete with their civilian counterparts to find suitable jobs. Hence, as I have always maintained that a successful Military to Corporate (M2C) Transition is a challenged that must never be underrated.



Military Veterans are a Natural Fit in Cyber Security

The Challenges of Transition For Veterans

While the military trains people to be generalists the industry places a premium on specialists. This is a significant barrier to cross for veterans. In addition is the fact that almost all veterans come with experience and are thus what the industry calls “lateral hires”. Almost no company generally likes to hire laterally in large numbers as they would prefer to grow talent internally within their organizations providing career progression to their existing employees.

The second challenge is the lack of industry experience when competing with your civilian counterparts for jobs. This is a tough nut crack. So, a veteran with a string of industry certifications under his belt also may face this barrier.

Veterans too come with aspirations of a high growth and financially rewarding career. These aspirations are difficult to fulfill in traditional or old industries vs new age sectors. But, the new age industries demand cutting -edge and in-demand technological skills which most veterans may not be equipped with by virtue of their military service alone.

The Importance of Career Strategy

While it is important to align one's career choice with one's passion and aptitude it is also equally critical to choose one's industry or sectors carefully. Just to illustrate the point the same role (eg a Chief Security Officer) in a manufacturing company vis-à-vis a new age/ tech company may have quite different compensation structures, the latter being financially more lucrative.

The issue of getting hired laterally has already been highlighted. The only industries who hire laterally in large numbers are the ones experiencing explosive growth and talent/ skills shortages. These skills are generally the high in-demand skills and keep changing dynamically.

In addition while veterans may have a disadvantage of deep domain industry skills there are several transferable skills that the military teaches that are prized by the corporates. Hence, the importance of having a suitable career strategy for veterans assumes significant importance. As far as possible veterans should try to choose a job role/ industry that largely matches with their aptitude they must also try to target the roles in high growth sectors wherein their transferable skills can give them a leg up in the hiring process.

Keeping all the above in mind if we try to select a suitable sector for veterans today Cyber Security would come up on the top of charts for most veterans. While some may say that this requires a lot of technical skills but the fact remains that if one plans well in advance this is easily doable with some preparation and mentoring.

Why Cyber Security is a Good Match For Veterans

The first reason is that veterans already have a security-first mindset which is not common in the civvie street. In addition, several of the concepts of cyber security have been borrowed from the military. Concepts like fort mentality, Defence in Depth, Zero Trust model, etc are intuitively understood by veterans. What do cyber security professionals do? Cybersecurity professionals protect computers, networks, digital assets, and information against unauthorized access. In a broad sense, any device connected to the internet/ networks could be exposed to a cyberattack and therefore needs to be protected. As a veteran, pursuing a career in cybersecurity lets you continue your mission of protecting citizens, critical assets and defending your country. The only difference is that the context changes slightly instead of the physical battlefield we have a digital battlefield. **That's all!**

Many of the skills necessary for the military are also important in cybersecurity, such as situational awareness, willingness to learn on the job, ability to quickly process information, bias for action, time-sensitive challenges, process orientation, alertness and quick reaction time. The following factors also help veterans a good match for the cyber security domain.

- Experience working in high-stress environments
- Mission mode style work ethic
- Leadership skills and experience
- Problem-solving abilities
- Disciplined attitude
- Experience handling time-constrained assignments
- Understanding of the significance of defending and protection
- Ability to communicate quickly and efficiently
- Loyal, dedicated, and a self-driven attitude
- Have been trained to combat an adversary

Add to all this the below facts about the cyber security industry.

- **Explosive Growth.** With digitization, remote working and exponential increase in cyber hacking and cyber crimes the sector is already facing exponential growth. The onset of 5G and IOT (Internet of Things) will further exacerbate this trend even further.
- **Demand Exceeds Supply.** The latest numbers from Cyberseek indicate nearly 600,000 cybersecurity job openings exist in the U.S. alone, and the CISOs complain they can't find enough good people to fill the available jobs. The talent shortage is for real even in India and most other countries across the world. This is an excellent sector to target for veterans to offset the disadvantage of lateral hires. Also in addition since the sector faces acute talent shortage the employers would be happy to look at candidates with certifications even if they maybe lacking in industry experience.

- **Wide Spectrum of Roles.** Unlike what most people think cyber security does NOT comprise of only technical roles that involve coding but a broad spectrum of roles ranging from non-technical, semi-technical, process, audit, compliance, operations, engineering and highly technical roles. Veterans can easily find a fit across this wide spectrum to match their talents and aptitude.
- **High Salaries.** Since this is a new age sector and the demand outstrips supply the salaries are quite attractive. This trend is likely to continue in the foreseeable future.

Roles In Cyber Security



Cyber Security has a Large Number of Roles Available to Choose From

Cybersecurity Skills

Some of the common skills required in cyber security are:

- Programming and coding skills
- Data management
- Mobile device and application security
- Security incident handling
- Analytical skills
- Communication skills
- Networking skills
- Security Incident Handling & Response
- Applications and Systems
- A diverse IT background

There is a very broad spectrum of roles available in cyber security. Some of the prominent roles are as listed below:

- Security Analyst
- Security Engineer
- Security Architect
- Security Administrator
- Security Software Developer
- Cryptographer
- Chief Information Security Officer
- Security Consultant

Let's take a brief look at these roles.

Security Analyst

Analyzing the vulnerabilities in the software, hardware, and networks and recommending solutions and best practices is what a security analyst does. Tests for compliance with security policies and procedures can assist in creating and implementing security solutions.

Roles and Responsibilities:

- Monitoring security access.
- Performing internal and external security audits.
- Analyzing security breaches.
- Updating the company's incident response and disaster recovery plans.
- Verifying the security of third-party vendors.

Security Engineer

Security Engineer performs security monitoring and forensic analysis to detect security incidents and mount an incident response. They utilize new technologies and processes to enhance security capabilities and implement improvements.

Roles and Responsibilities:

- Developing security standards and practices.
- Creating new ways to solve existing security issues.
- Conducting penetration testing.
- Developing automation scripts to handle incidents.
- Watching out for irregular system behavior.
- Supervising changes in software, hardware, and user needs.
- Helping plan an organization's information security strategy.
- Educating staff members on information security through training.
- Recommending modifications in legal, technical, and regulatory areas.

Security Architect

Security Architect designs security systems and heads a security design team building a new security system.

Roles and Responsibilities:

- Reviewing current system security and implementing enhancements.
- Conducting regular system tests.
- Developing project timelines.
- Establishing disaster recovery procedures.
- Promptly responding to all security incidents

Security Administrator

The Security Administrator manages the organization-wide security systems and takes on some of the tasks of the security analyst in a smaller organization.

Roles and Responsibilities:

- Defending systems against unauthorized access.
- Monitoring unusual activity.
- Configuring and supporting security tools.
- Implementing network security policies and corporate data safeguards.
- Developing and updating disaster recovery protocols.

Security Software Developer

Security software developer implements security into applications software and develops software to monitor and analyze traffic, intrusion detection, virus/spyware/malware detection, anti-virus software, and so on.

Roles and Responsibilities:

- Implementing, testing, and operating advanced software security techniques.
- Performing ongoing security testing and code review to improve software security.
- Troubleshooting issues that arise.

Cryptographer

A cryptographer works as a researcher to develop strong algorithms to secure information or to build secure software.

Roles and Responsibilities:

- Identifying any weakness in existing cryptography systems.
- Testing cryptology theories in practice.
- Implementing highly encrypted solutions for your organization.
- On-going development of encryption technology, training, and enhancement of IT security.

Chief Information Security Officer (CISO)

CISO is a high-level management position responsible for hands-on technical work and maintaining the entire information security staff.

Roles and Responsibilities:

- Security operations
- Data loss and fraud prevention
- Security architecture
- Program management
- Investigations and forensics
- Governance

Security Consultant

A security consultant is responsible for protecting computers, networks, software, data, and/or information systems against viruses, worms, spyware, malware, intrusion detection, unauthorized access, and denial-of-service attacks.

Roles and Responsibilities:

- Testing for potential security threats.
- Identifying possible security threats.
- Designing and maintaining security protocols to cover all possible security threats.
- Coordinating a team of security specialists and assigning tasks.
- Meeting with clients to discuss security measures.
- Running risk assessment.
- Compiling reports on the test results.
- Suggesting improvements to existing security systems

Pathways To Upskilling

While a career in cyber security can be extremely rewarding it does call for some upskilling by veterans. There could be two major pathways. One is via the college degree route and the other one via industry certifications



Military Veterans Can Crack Cyber Security Jobs With Some Upskilling Effort

College Degree Routes

One can undertake a Bachelor of Science in Cyber Security or a Master of Science in Cyber Security or related majors. Nowadays many of these courses are available in an 100 % online mode. One can also earn degrees from reputed universities. Many of these courses are also available via the MOOCs (Massive Open Online Courses) on platforms like Simplilearn, UpGrad, Great Lakes Learning and even some universities.

Some of the examples of these courses is as listed below:

Course Name	Institution	Link
MS in Cyber Security from UC Berkeley	Berkeley School of Information	https://ischoolonline.berkeley.edu/requestinfo/cyber-spz-atf/?experimentid=20783712294&lsrc=fortunecplsite&utm_source=fortunecplsite&email_id=null&utm_medium=strategic_partnership&utm_campaign=onlinerankingscyber&l=onlinerankingscyber
Syracuse University M.S. in Cybersecurity Online (15 months)		https://onlinegrad.syracuse.edu/requestinfo/mscy-spz-atf/?experimentid=20971461423&lsrc=fortunecplsite&utm_source=fortunecplsite&utm_campaign=onlinerankingscyber&l=onlinerankingscyber&c=instream&utm_content=instream&utm_medium=strategic_partnership
M.S. in Cybersecurity Yeshiva University, Katz, NY	Yeshiva University, Katz, NY	https://go.yu.edu/katz/programs/graduate/cybersecurity?utm_term=cyber%20security%20masters%20programs%20online&utm_campaign=CYB+%7C+Katz+%7C+Search+%7C+Dom&utm_source=adwords&utm_medium=ppc&hsa_acc=4399719919&hsa_cam=14758994617&hsa_grp=128393108140&hsa_a

Course Name	Institution	Link
Advanced Certificate Programme in Cyber Security from IIIT, Bangalore (6 months)	UpGrad	https://www.upgrad.com/cyber-security-certification-pgc-iiitb/
PG Programme in Cyber Security (6 Months)	Great Learning	https://www.mygreatlearning.com/online-cyber-security-course

Industry Certifications Route

Cyber Security Certifications



Some Prominent Cyber Security Certifications

This is a shorter pathway though maybe more intense. One point to note is that there are several agencies/ organizations that conduct various cyber/ info security related certifications. Some of them are listed below.

- ISACA: <https://www.isaca.org/>
- (ISC)2: <https://www.isc2.org/>
- EC-Council: <https://www.eccouncil.org/>

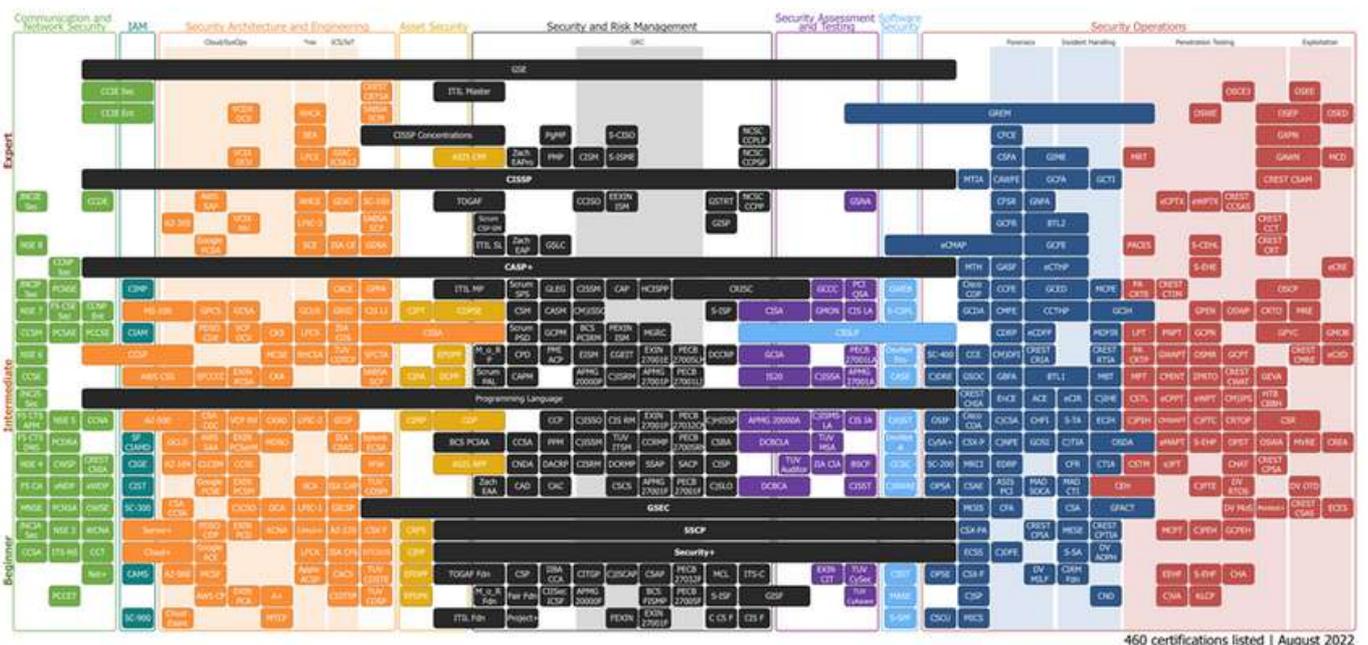
- CompTIA: <https://www.comptia.org/resources/cybersecurity>
- GIAC: <https://www.giac.org/>
- BCS: <https://www.bcs.org/qualifications-and-certifications/certifications-for-professionals/information-security-and-ccp-assured-service-certifications/>

As already stated the entire gamut of Cyber Security includes a spectrum of fields ranging from non-technical, semi-technical, process, audit, compliance to deeply technical.

Broadly there are 8 verticals. It is suggested that you may choose one vertical and then start from the Beginner level certifications and subsequently graduate towards the Intermediate and Expert levels.

1. Communication and Network Security.
2. IAM- Identity & Access Management.
3. Security Architecture and Engineering.
4. Asset Security.
5. Security and Risk Management.
6. Security Assessment and Testing.
7. Software Security.
8. Security Operations.

Under these 8 verticals there are a plethora of an ever-increasing number of certifications. Currently there are around 460 certifications available. It can be viewed at Security Certifications Roadmap. A snapshot of the same is as shown below.



Security Certifications Roadmap

10 Cybersecurity Certifications to Boost Your Career in 2022

While that is a lot of certifications to help you narrow down your choice I am listing down the top 10 certifications in cyber security in 2022 as per Tech Target. In building this list of top 10 cybersecurity certifications, Tech Target talked to a broad range of people in the security industry. They heard from course providers and consultants, such as Cybrary and CyberVista; talked to a professor from University of Maryland Global Campus; sought advice from security providers, such as Cisco and Fortinet; and contacted leading trade groups and certification providers, such as CSA, CompTIA, EC-Council, ISACA, (ISC)2, ISSA International, Global Knowledge and Offensive Security.

The list starts off with basic, entry-level and management track certifications, then moves on to the offensive security certifications for hands-on penetration testers and certified ethical hackers. It concludes with a list of 10 top vendor-specific certifications. Security professionals typically need a mix of all three types of certifications: management training, hands-on and vendor/product-specific knowledge.



Top 10 Cyber Security Certifications in 2022 (Source Techtarget)

CompTIA Security+;

(ISC)2 Certified Information Systems Security Professional (CISSP);

(ISC)2 Certified Cloud Security Professional (CCSP);

ISACA Certified Information Security Manager (CISM);

EC-Council Certified Ethical Hacker (CEH);

EC-Council CEH (Practical);

CompTIA PenTest+;

Offensive Security Certified Professional (OSCP);

Cloud Security Alliance (CSA) Certificate of Cloud Security Knowledge (CCSK); and

Vendor-specific security certifications.

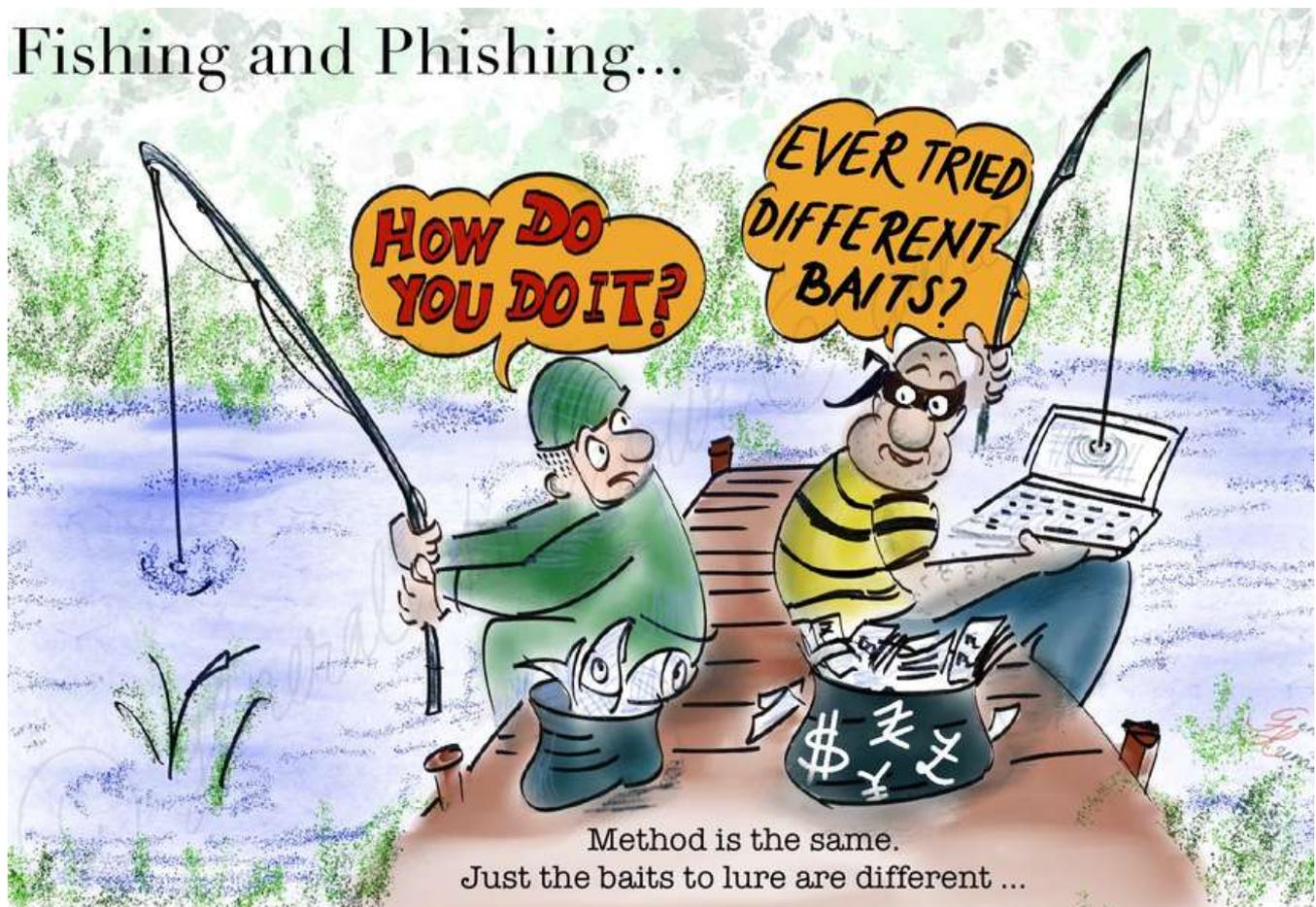
Conclusion

While that may seem like a lot of information and be a little overwhelming – it is an honest endeavour to summarize the vast field of cyber security and present it in a concise, easy to understand and comprehensive manner. Many veterans may get a little confused as to where to start from. In case they are not very technical it may be advisable to start from the lesser technical areas of info security, Governance, Risk and Compliance (GRC) and Risk Management. Having gained some technical knowledge and experience one can always switch to other / more tech intensive areas such as Software Security, IAM, Digital Forensics, Penetration testing , etc in case that interests oneself.

What is important is to get started on the journey – greater clarity would emerge once you are on the journey. Have faith in your abilities – remember we as humans have a tendency to always under-estimate human potential. We all can do much more than we think we can. This is even more true for military veterans.

So what are you waiting for? Get Started!

Fishing and Phishing...



Amit Dalvi

Rising Star- Shining Bright

Vansh Luthra

It's been 365 days, 12 months, and more than 25 international film festivals for our film Destination Paradise. Since the interview in the 'Stars On the Horizon' section of the magazine, I have come a long way, and I am extremely thankful to my Fauji family for all the support and wishes that have come my way.

In the interview I spoke about the film which I produced and acted in, I spoke about my life as an actor in Prague, the skillsets Fauj life had provided me, and today I write to boast about the success of the team behind the film.

Destination Paradise has been to more than 10 Countries in 25+ International Festivals, winning accolades and honours such as 'Best Short Film', 'Best Director' awards. It has also been selected for the Dada Saheb Phalke International Film Festival to be held in February 2023, and Jaipur International Film Festival 2023, both of them being India's top notch film festivals.





But the biggest new so far comes from the fact that you can watch Destination Paradise on Disney+ Hotstar. <http://www.hotstar.com/1260119321>

In other news I was lucky enough to get a substantial role in an European Netflix film, which cannot be named, but I'll surely let the readers know about it when it is out. I am also excited to share that I'd be playing a MMA fighter in our next film, for which I am having a strict regime, and I hope to share more information soon.



I would be waiting for your mails, messages about the review of the film I can be reached at

Instagram - @vanshluthractor
<https://www.instagram.com/vanshluthractor/>

Facebook - Vansh Luthra
<https://www.facebook.com/VanshLuthractor>

LinkedIn - Vansh Luthra
<https://www.linkedin.com/in/vanshl/>

Twitter - Vanshluthra25
<https://twitter.com/VanshLuthra25>

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.



*Clicked from iPhone 13
By Col Col BS Rai*



*Title: Eurasian sparrowhawk
Shutter Speed-1/200 s; ISO 100; Apperture f/ 5.6;
Focal Length 250.00mm; Camera Canon
1300d; Lens Used 55-250mm By Ayush Bhatia*

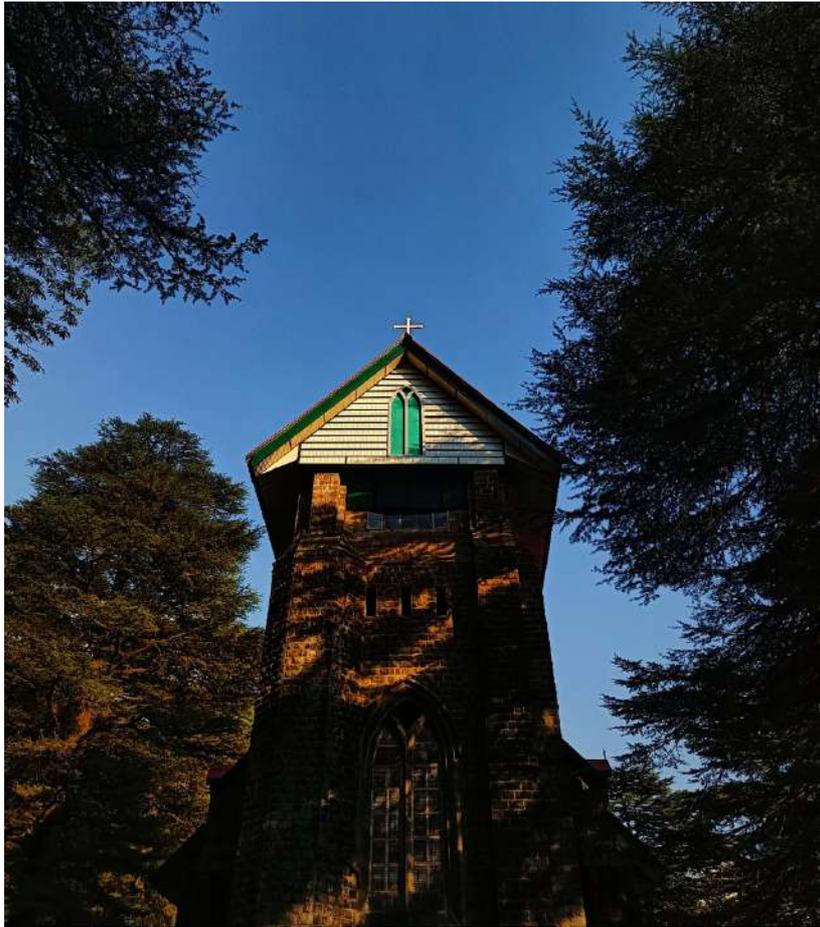
*Clicked from iPhone 13
By Col BS Rai*



*Rabbi Rabbi Shergill at Ziro Festival of Music
By Col J Sharma*



Reveler at Ziro Festival of Music
By Col J Sharma



St. John in the Wilderness, (Catholic Church), McLeodganj
Camera OnePlus Nord 2 5g
By Ayush Bhatia



An Apatani old lady from Ziro valley Arunachal
By Col J Sharma

Wisdom Bytes

Know the Price of a Cyber Attack – Prevention is Much Better Than Cure

BY IQBAL SINGH

Introduction

Cyber security is often relegated in business priorities. Many a times it may also be reduced in some organizations to a compliance checkbox exercise. This thinking is dangerous and fraught with several risks. We take a look at a cyber attack launched on a company called UKG in Dec 2021 in the USA. This would help us understand as to why just being good enough isn't enough in cyber security. Cyber security has today become a business imperative – if you do not agree read on!

About UKG



The UKG logo

Ultimate Kronos Group (UKG) is an American multinational technology company with dual headquarters in Lowell, Massachusetts, and Weston, Florida. It provides workforce management and human resource management services. The company was founded in April 2020 as a result of the merger of Ultimate Software and Kronos Incorporated. The combined company, valued at \$22 billion, became one of the largest cloud computing companies. Kronos CEO Aron Ain became CEO and chairman of the new company, with more than 12,000 employees. The merger was officially completed on April 1, 2020 and in August, the company's name was announced as Ultimate Kronos Group (UKG), which became effective on October 1.

The company served over 70,000 customers globally spread across 150 countries. UKG products included payroll systems, employee Timesheet management systems, Scheduling services (eg appointment scheduling) amongst its other products. The company had a large number of public sector customers like New York Metropolitan Transportation Authority, the City of Cleveland, the state of West Virginia, the Oregon Department of Transportation, the University of California system, and Honolulu's EMS and Board of Water Supply, Several hospitals and health sector organizations, etc. As regards private/ public companies UKG counted Tesla, Pepsico, Whole Foods, Gamestop, etc amongst its key customers.

The Ransomware Attack Dec 2021

On Monday December 13, UKG announced that it was the victim of an ongoing ransomware attack affecting the Kronos Private Cloud, which hosts UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions. The company further disclosed that the Kronos Private Cloud solutions systems are currently unavailable and it may take up to several weeks to restore system availability for clients. The breach is forcing many issuers across the spectrum of public finance to resort to manually tracking and estimating employee hours, having to issue paper paychecks and possibly causing paycheck delays during the holidays.

The communication sent by the company to its impacted customers is reproduced:

"We are reaching out to inform you of a cyber security incident that has disrupted the Kronos Private Cloud. As we previously communicated, late on Saturday, December 11, 2021, we became aware of unusual activity impacting UKG solutions using Kronos Private Cloud. We took immediate action to investigate and mitigate the issue and have determined that this is a ransomware incident affecting the Kronos Private Cloud—the portion of our business where UKG Workforce Central, UKG TeleStaff, Healthcare Extensions, and Banking Scheduling Solutions are deployed. At this time, we are not aware of an impact to UKG Pro, UKG Ready, UKG Dimensions, or any other UKG products or solutions, which are housed in separate environments and not in the Kronos Private Cloud.

We are working with leading cyber security experts to assess and resolve the situation and have notified the authorities. The investigation remains ongoing, as we work to determine the nature and scope of the incident.

While we are working diligently, our Kronos Private Cloud solutions are currently unavailable. Given that it may take up to several weeks to restore system availability, we strongly recommend that you evaluate and implement alternative business continuity protocols related to the affected UKG solutions. Support is available via our UKG Kronos Community and via our UKG Customer Support Team to provide input on your business continuity plans.

We deeply regret the impact this is having on you, and we are continuing to take all appropriate actions to remediate the situation. We recognize the seriousness of this issue and will provide another update within the next 24 hours."

The ransomware attack caused immense administrative chaos for millions of people, including 20,000 public transit workers in the New York City metro area, public service workers in Cleveland, employees of FedEx and Whole Foods, and medical workers across the country who were already dealing with an omicron surge that has filled hospitals and exacerbated worker shortages.

As centralized providers of mission-critical software to thousands of employers nationwide, companies like UKG are at constant risk of cyber attacks. In the eyes of ransomware attackers, who seek to maximize their leverage to extract as large a ransom as possible, a workforce software provider like UKG during the holiday season are "a pretty juicy target".

The timing and the choice of target seems to have been meticulously planned and for UKG it could not have come at a worse time. With UKG servicing more than 40 million employees and 70,000 customers was indeed a juicy target. One can also say that the timing was critical with end of year tax implications, the onset of the festive season and people, most importantly, looking for their checks and bonuses.



Sound Business Contingency Planning & Rehearsals are a Necessity

Impact of the Ransomware Attack

- **Outage.** Unavailability Of Payroll & Timesheet systems millions of users at tens of thousands of customers unable to check pay, arrange rotas, or request paid leave. In the US public sector alone, the New York Metropolitan Transportation Authority, the City of Cleveland, the state of West Virginia, the Oregon Department of Transportation, the University of California system, and Honolulu's EMS and Board of Water Supply, along with scores of smaller local authorities were impacted. 8million employees across 2000 companies were impacted. UKG took nearly 10 weeks before the restoration.
- **Manual Processing.** The outage issue continued to be devil the customers IT teams globally who were been forced to spend time in early 2022 supporting their companies with Excel-based workarounds provided by UKG and other related HR/payroll issues. In the most severe cases, that backlog could delay issuing W-2s and other tax information.
- **Healthcare Workers Impacted.** One of the Kronos products knocked offline was designed specifically for health care providers to help them manage the complex employee schedules at 24-hour facilities. The outage became an unneeded administrative nightmare timed precisely as the omicron surge was hitting hospitals. Some struggled to pay workers accurately. Employees across the country turned to their unions, social media, or local news outlets to report inaccurate pay cheques. Employees of the University of Florida Health system in Jacksonville told local TV station News4Jax that they had not received overtime or holiday pay for six weeks. In Montana, more than 250 nurses at Missoula's Community Medical Center missed out on pay due to the hospital's decision to pay employees by duplicating an early December pay cheque.



Data is the new oil and must be zealously guarded at all times

- **Data Exfiltration.** The company's private cloud-based applications were hit in the attack, with data centres in the US, Frankfurt, and Amsterdam all affected by the ransomware attack. There was data exfiltration, and some customers data loss was confirmed. Sportswear label Puma a customer confirmed in January 2022 the data loss. The attackers stole data of 6,632 Puma employees in the ransomware attack that affected Ultimate Kronos Group (UKG) HR management tools. The stolen information included names, Social Security numbers, and other personal information. Additionally, the City of Cleveland sent out an urgent message saying that UKG contacted them and other clients to tell them that the ransomware attack may have compromised employee information like names, addresses, social security numbers, and employee IDs. There were legal suits filed for the data breach. UKG acknowledged that it notified authorities in Australia, Belgium, Brazil, Canada, Hong Kong, India, Singapore and New Zealand of data loss for those nationals.
- **Lawsuits.** In addition to the data breach suit, employees at PepsiCo, the New York MTA and Allegheny General Hospital in Pittsburgh, among others, filed class-action lawsuits alleging that they were improperly paid due to the system outage.
- **Payment of Ransomware.** While there has been no confirmation from either UKG or the law enforcement agencies grapevine has it that a ransom was paid by UKG.
- **Backup Access Attacked.** The attackers disabled UKG's ability to communicate with their back-up environment, this was confirmed by UKG have as data restoration took more time than what was announced by UKG.
- **Investigation Costs.** The company hired Mandiant, a cybersecurity firm, to conduct an investigation of the incident and West Monroe, a digital consulting firm, to help restore operations. They must have paid hefty fees as in times like these the victim company is in no position to negotiate.
- **Reputational Damage.** The company suffered immense reputational damage in the aftermath of the ransomware attack. The Kronos incident demonstrates vividly the disruption that can occur with a ransomware attack. It's bad enough that Kronos suffered a disruption that will cost the company money but more importantly its reputation was severely damaged, not just with the clients but also their employees many of whom lost personal data in the hack. It is likely that UKG may have lost many customers as well.
- **Third Party Risk.** The incident brought center stage the discussion of 3rd Party risks in the case of a cyber attack. This is a prime example of third-party risk. As much as your company might have all of its cybersecurity ducks in a row, your company is still at risk if you rely on a vendor that has security gaps. Protecting your organization from a ransomware attack similar to the one that happened to

Kronos means going beyond just protecting your organization from malware. You must ensure that all vendors you rely on are accurately assessed for security risks as well.

Managing Third-Party Risk

To help remove third-party risks, and keep you from experiencing a similar ransomware attack to Kronos, here are the key steps to understanding and managing your third-party risks:

- **Step 1: Identify your vendors:** You need to know who all your vendors are before you can perform a risk analysis. For some organizations, the list may be small. For others, it can take a while to track down and catalogue all vendors.
- **Step 2: Analyze risk for each vendor:** Assess the security posture of each vendor and determine the relative risk they pose to your critical operations and infrastructure.
- **Step 3: Prioritize vendors based on risk:** Once you understand the risk associated with each vendor, you can categorize vendors based on their overall importance to your business and any potential threats they pose. This will help you address the most critical issues first or determine where a shift in vendor prioritization would be more beneficial.
- **Step 4: Monitor continuously:** Just checking in with each vendor once is not enough. With all businesses these days, technology and configurations are constantly evolving, as is the threat landscape. Continuous monitoring of third-party risk will alert you if something changes and enable you to act accordingly.

Conclusion

The cyber incident of UKG was only used to illustrate the immense damage that can be caused due to a cyber attack. Aim was to sensitize the readers about the size, scale and the range of damage that can be caused. This incident underscores that cyber security is NOT just the responsibility of the CISO but everyone including the CEO and the Board. Another important point to learn from the incident is that as a CISO you are NOT just responsible for the security within your company but across its entire supply chain including vendors, third parties, etc. This should highlight to those seeking a career in cyber security that they have selected a domain which has a very, very bright future.

One very important aspect that this incident clearly brings out is that it is important to do things right first time. There is a business case for investing in cyber security upfront, hiring skilled security talent, extremely strong business continuity processes and a dynamically agile Security team in an organization. Attacks like the one on Kronos should serve as reminders that “good enough” isn’t actually always enough and meeting one Compliance framework here and another one there doesn’t equal a mature Compliance strategy in today’s challenging and increasingly risky landscape.

Tech Corner

Solar Power: An Insight - Part II

BY RAJESH NAIR

(This is second and final article of the series on the subject)

In the last edition we learnt about the Sun, Solar energy, types of PVC and their working. Let us know more on how solar power is used and its future.



Share of global electricity from wind and solar is currently at 10% of global requirement. Solar PV generation increased by a record 179 TWh (up 22%) in 2021 to exceed 1000 TWh. It demonstrated the second largest absolute generation growth of all renewable technologies in 2021, after wind. An average annual generation growth of 25% in the period 2022-2030 is needed to follow the Net Zero Emissions by 2050 Scenario. This corresponds to a more than threefold increase in annual capacity deployment until 2030, requiring much greater policy ambition and more effort from both public and private stakeholders, especially in the areas of grid integration and the mitigation of policy, regulation and financing challenges.

This is particularly the case in emerging and developing countries.

During COP26, held in November 2021 in Glasgow, India announced new 2030 targets of 500 GW of total non-fossil capacity and 50% renewable electricity generation share (more than double the 22% share in 2020), as well as net zero emissions by 2070, with solar PV being one of the main technologies used to achieve these goals.

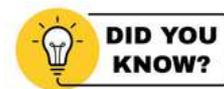


- *Vietnam has seen unparalleled growth in solar power. This has not only reduced power sector emissions, but also reduced its costly gas import bill.*

Characteristics of Solar Energy

Solar energy is created by nuclear fusion that takes place in the sun. Fusion occurs when protons of hydrogen atoms violently collide in the sun's core and fuse to create a helium atom. Solar energy is constantly flowing away from the sun. The energy, heat, and light from the sun flow away in the form of electromagnetic radiation (EMR). Almost all life on Earth relies on solar energy for food, either directly or indirectly. Solar energy is a renewable resource, and many technologies can harvest it directly for use in homes, businesses, schools, and hospitals. Some solar energy technologies include photovoltaic cells and panels, concentrated solar energy, and solar architecture.

As the sunlight hits each PV cell, the photovoltaic effect is set into motion. The photons, or solar energy particles, that make up the light start to knock electrons loose from the semi conductive material. These electrons begin to flow toward the metal plates around the outside of the PV cell. Like the flow of water in a river, the electrons create an energy current. The energy current is in the form of direct current (DC) electricity. Most electricity that is used is in the form of alternating current (AC), so DC electricity has to travel through a wire to an inverter whose job is to change



Sunlight takes approximately eight minutes to reach the Earth. More solar energy reaches Earth in one hour than the world uses all year

DC to AC electricity. Once the electrical current is changed into AC, it can be used to power electronics in a house or stored in batteries. In order for the electricity to be used, it must go through the home's electrical system. There are different models of electrical power system.

The three main types of Solar power systems are:

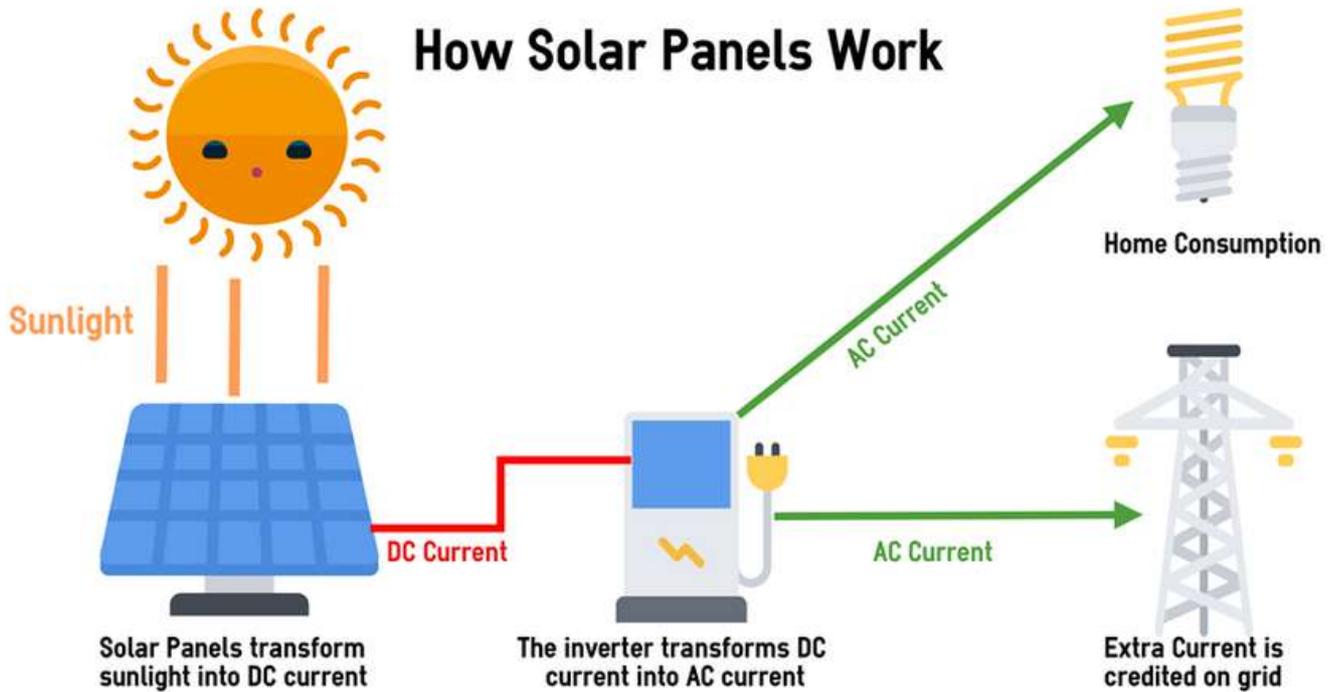
- On Grid – Grid feed system (Gross metering)
- Off Grid – Stand alone system
- Hybrid – Grid and battery connected solar system

In India there are two types of Solar metering - Net Metering and Gross Metering. The difference being the accounting of energy consumption and billing.



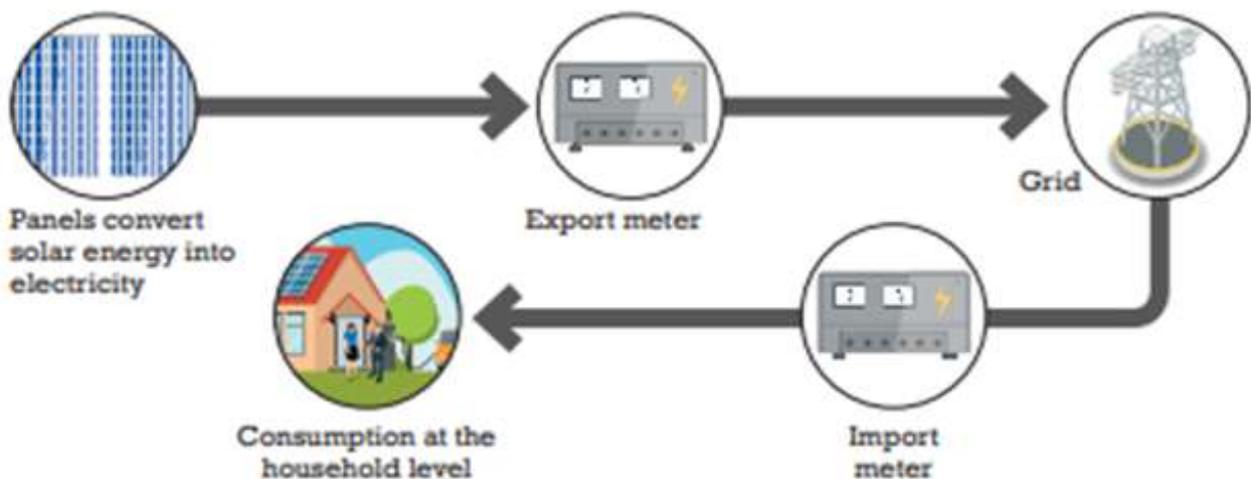
Las Vegas, Nevada is the largest city to operate on 100% renewable energy, which is largely solar power

Net Metering: When the sun is shining, solar panels convert sunlight to energy. If they produce more electricity than needed, that electricity is often sent back to the power grid and there is a credit on the electricity bill. This is known as "net metering."

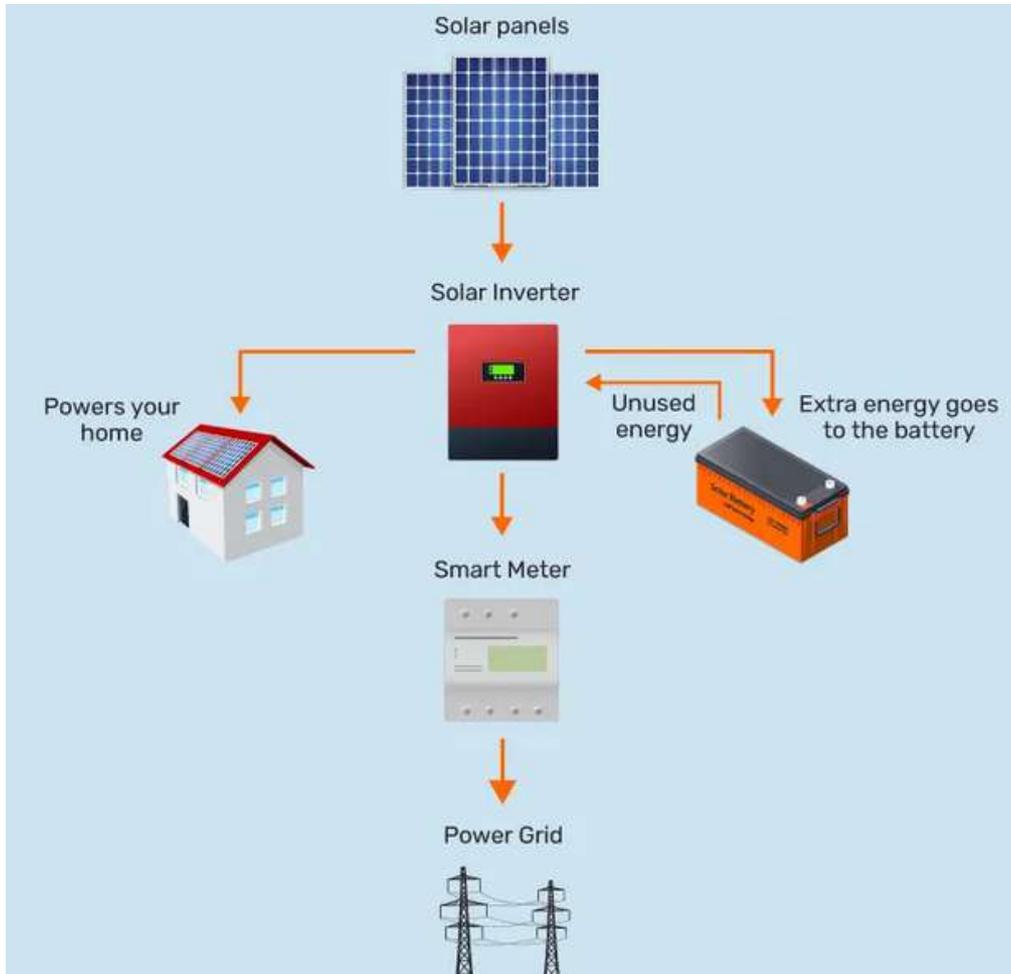


copyright - reliablecounter.com

Gross Metering: In gross metering, all electricity that is produced by residential solar panels is immediately sent to the power grid.⁴ Residents then pull power back from the grid. However, solar panels don't always produce electricity. If the sun isn't shining, homeowners might need to tap into the power grid anyway to draw the electricity. Then they will be charged by the utility company for the energy consumed. anyway to draw the electricity. Then they will be charged by the utility company for the energy consumed.



Hybrid System: In a hybrid system, people install batteries with their solar panels and most excess electricity that's generated by the panels can be stored there. Whatever is left over will be sent back to the grid. If required a person may import also from the power grid. At the end of billing period the net power consumed is calculated. If the export of power is more than import of power then the electricity board may pay back or adjust in next bill for the consumer.



173,000 terawatts of solar energy hit the Earth continuously – that's greater than 10,000 times the world's total energy use.

There are over 57 million square miles of land on Earth. In order to power the entire planet, we would need to install solar panels on just over 191,000 square miles.

Current and Future Trend:

The solar industry has seen tremendous innovations by integrating AI into its products. It's currently being used to forecast energy demand like a weather report and manage energy distribution so homeowners will have power at all times. Having AI manage energy distribution as efficiently as possible is a game-changer for the industry. This is because energy can't be stored for extended periods, depending on the system design. Unlike smartphones and laptops, which seem to cost more with each passing year, the cost of solar technology is on a steady downward trend.

In the early days of renewable energy systems, the technology was unreliable and ineffective on its best day. This, coupled with the massive upfront cost to install a solar power system, made it not worth looking at for many. However, every type of solar power system, has seen massive improvements in durability and effectiveness. In fact, the mass adoption of solar technology has pushed companies to continue developing innovative features and working to improve overall durability.

There is an increased demand to integrate solar into other products. Currently, consumers can benefit from the cost-savings of using solar-powered outdoor lights for general decoration and to power massive displays on their homes. Additionally, with the increased demand for solar products, the industry has seen a market interest for solar-powered chargers for electric vehicles and even solar-powered vehicles.

2022 is shaping up to introduce a wide selection of solar products to meet consumer demands. Of course, with this substantial increase in demand comes an increase in demand for solar professionals. The Solar power industry will see a demand for professionals with niche solar knowledge. The solar industry and renewable energy have made a quantum leap over the past decade. 2022 continues to signal strength for the industry and shows no signs of slowing down in the near future.

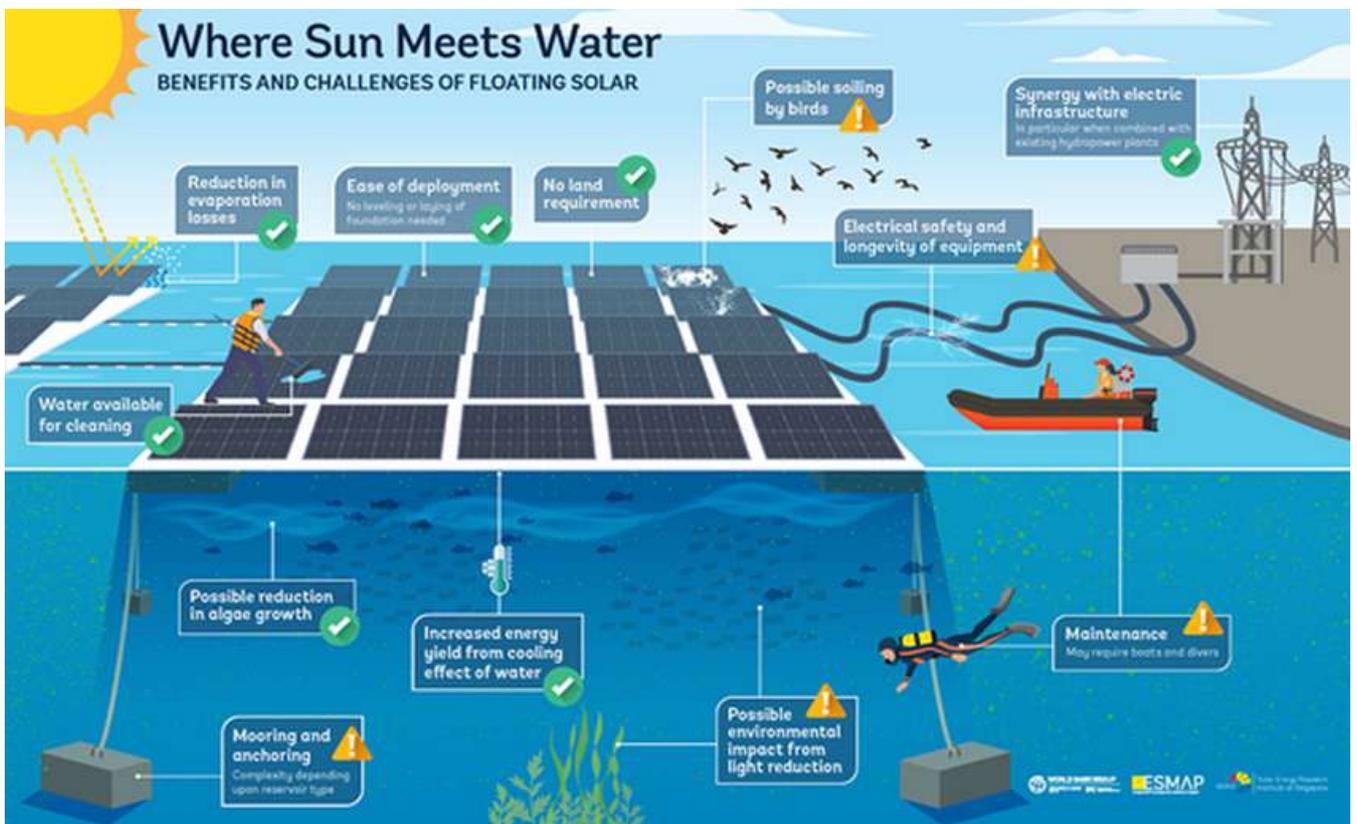
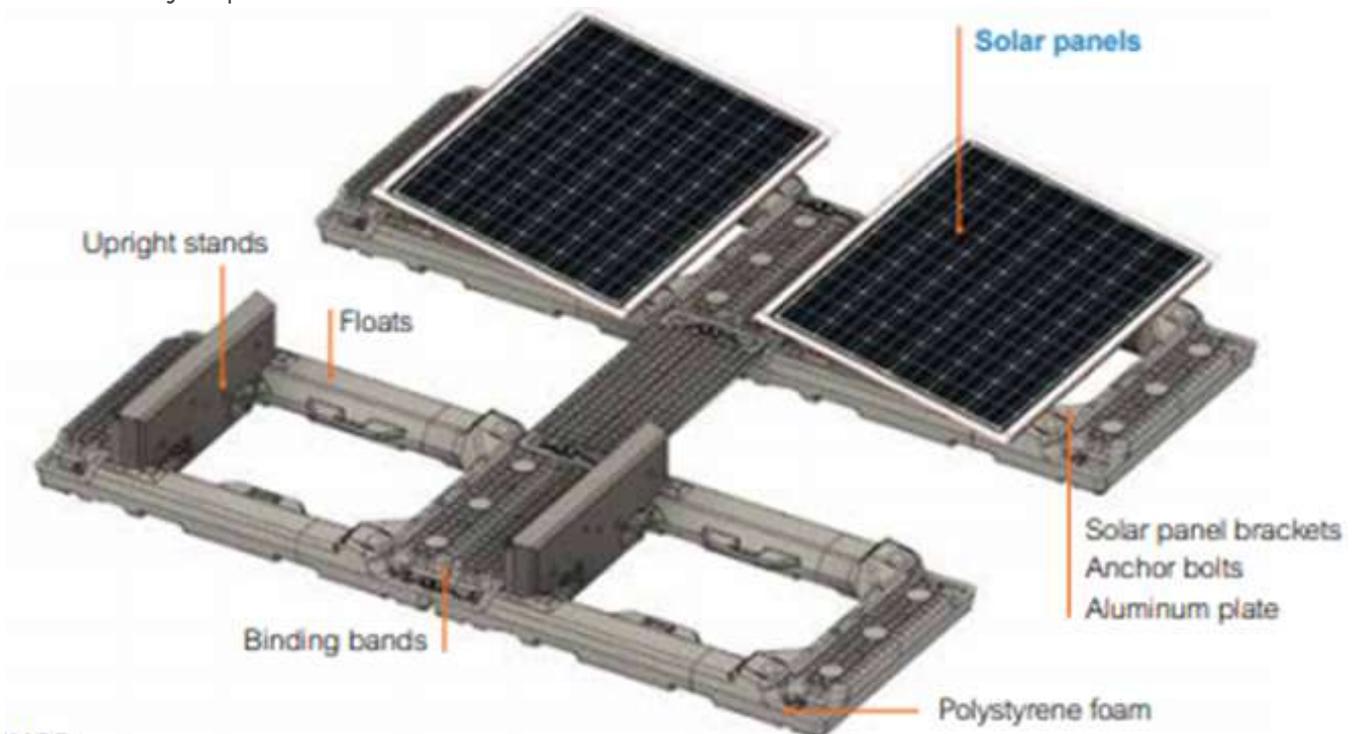
Future Products!!

Desert Farms:

Can desert be place for Solar panels? For many this would be the best, since desert are far spread and are very hot and enough of light. While the black surfaces of solar panels absorb most of the sunlight that reaches them, only a fraction (around 15%) of that incoming energy gets converted to electricity. The rest is returned to the environment as heat. The panels are usually much darker than the ground they cover, so a vast expanse of solar cells will absorb a lot of additional energy and emit it as heat, affecting the climate not only locally but globally also. Also, the heat from the sand would reduce the efficiency of the panels considerably. However, we do have panels placed in desert locations, which were also one of the initial solar farms.

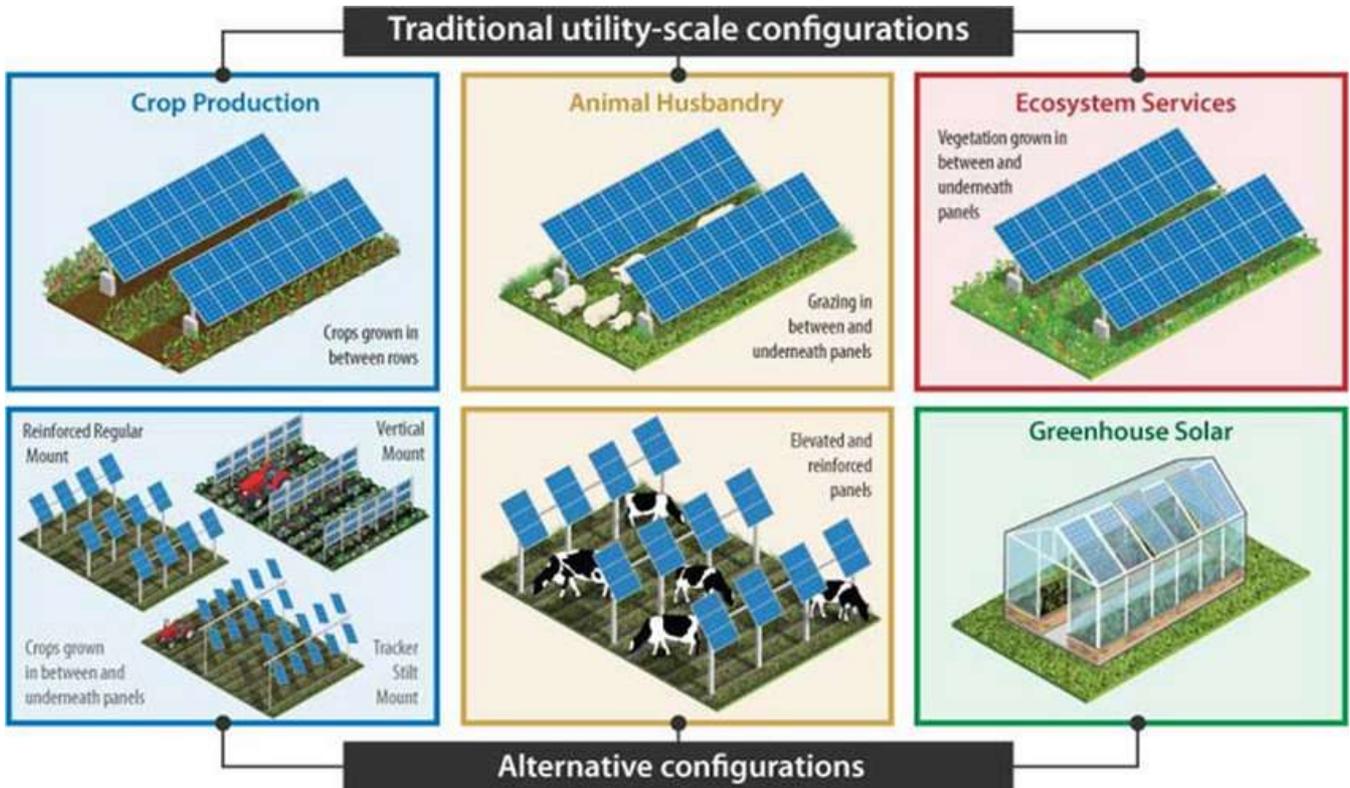


Floatovoltaics: Here Panels are placed on top of water bodies. It may be a dam or a pond. The main differences are that, there is a floating system used to keep the array above the waterline, and the mooring and anchoring system prevents the array from drifting and keeps the panels optimally oriented towards the sun. Still a long way from commercial viability and mitigating challenges. Currently 56 out of 70 such field are installed by Japan alone.



Floatovoltaics

Agrivoltics: Using PV installations to both create renewable energy and provide space for local agriculture or native habitats—is known as "agrivoltaics." A Win Win situation with Crop and cultivation. The crops also keep the panels cool and increases the effectiveness by 3%. Agrivoltaics is not necessarily more expensive than traditional solar development, but it can be more complex. This is being extensively in the US and has now started getting implemented in parts of India.



SmartFlower: Flower shaped panel uses dual axis trackers which makes the panels like sunflower. It moves with the movement of sun. Thus increasing the efficiency by 40%. It's a ground mounted equipment, however the technology is still costly and bulky and not practical for installation to many.

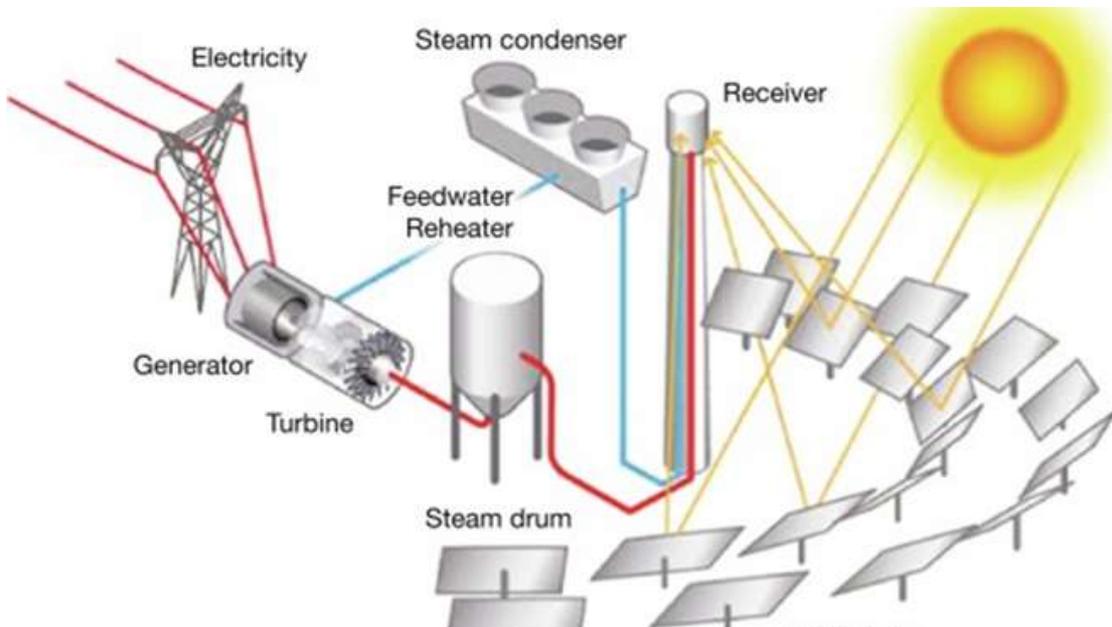


Changing face through the day



Solar electricity is measured in watts. 1000 watts = 1 kilowatt (kW). 1000 kW = 1 megawatt (MW). 1000 MW = 1 gigawatt (GW). 1000 GW = 1 terawatt (TW). 1000 TW = 1 petawatt (PW)

Heliostats Solar Thermal Plant: A heliostat is a device that includes a mirror, usually a plane mirror, which turns so as to keep reflecting sunlight toward a predetermined target, compensating for the sun's apparent motions in the sky. All the heliostat mirrors send accurately parallel beams of light into a large paraboloid reflector which brings them to a precise focus. The mirrors have to be located close enough to the axis of the paraboloid to reflect sunlight into it along lines parallel to the axis, so the field of heliostats has to be narrow. A closed loop control system is used. Sensors determine if any of the heliostats is slightly misaligned. If so, they send signals to correct it. A technology used during ancient times in Indian and Egypt culture.



Solar Weapon : In ancient times there are depiction of using sun as a weapon. The Heliostats Solar technology can be used to build the future weapon of precise target. A concave mirror mounted on a satellite to concentrate sunlight into a small area on Earth's surface can also be the future Space weapon. Although its still theoretical, it is used in many sci fi movies already. Weapons like Death lasers, Space mirror, micorwave or Sun gun may not be far from production. Using Solar powered tank comourflage is already in trails.



Solar Windows: Organic compound based cells can be used for making Solar windows. The solar glass works in the same way as solar panels to convert solar energy into usable electricity. However, they also allow light to pass through to the other side just like a normal window

Solar Architecture Homes: Buildings use passive solar energy to distribute heat efficiently and inexpensively. Calculating a building's "thermal mass" is an example of this. A building's thermal mass is the bulk of material heated throughout the day. Examples wood, metal, concrete, clay, stone, or mud. At night, the thermal mass releases its heat back into the room. Effective ventilation systems—hallways, windows, and air ducts—distribute the warmed air and maintain a moderate, consistent indoor temperature.

Passive solar technology is often involved in the design of a building. For example, in the planning stage of construction, the engineer or architect may align the building with the sun's daily path to receive desirable amounts of sunlight. This method takes into account the latitude, altitude, and typical cloud cover of a specific area. In addition, buildings can be constructed or retrofitted to have thermal insulation, thermal mass, or extra shading. In Indian Culture its part of the **Vastu Science**.

**DID YOU
KNOW?**

James Bond Movie, "Diamonds are forever" & "Die another day" uses sunlight as a weapon

Other examples of passive solar architecture are cool roofs, radiant barriers, and green roofs.

Cool roofs are painted white and reflect the sun's radiation instead of absorbing it. The white surface reduces the amount of heat that reaches the interior of the building, which in turn reduces the amount of energy that is needed to cool the building.

Radiant barriers work similarly to cool roofs. They provide insulation with highly reflective materials, such as aluminum foil. The foil reflects, instead of absorbs, heat, and can reduce cooling costs up to 10%. In addition to roofs and attics, radiant barriers may also be installed beneath floors. Mostly now seen in manufacturing setup.

Green roofs are roofs that are completely covered with vegetation. They require soil and irrigation to support the plants, and a waterproof layer beneath. Green roofs not only reduce the amount of heat that is absorbed or lost, but also provide vegetation. Through photosynthesis, the plants on green roofs absorb carbon dioxide and emit oxygen. They filter pollutants out of rainwater, air and offset some of the effects of energy use in that space.

Solar fabrics: Solar fabric architecture is still experimental, the result of combining fabric and solar cells, can be used to create canopies and other shaded gathering places where building occupants can relax while they recharge their devices. Solar cell fabric is a fabric with embedded photovoltaic (PV) cells which generate electricity when exposed to light. Truck tarps, for example, could be used to produce the electricity consumed by the driver when underway or parked up for the night, or to power electronic systems used to locate trailers in shipping terminals. At the moment, solar cell textiles are still in the testing phase.



Solar thermal fuels: The solar thermal fuel is a chemical that can absorb solar radiation, store it for a number of days, and release it again as heat. Although the fuel is not yet a mature technology, it has a wide variety of applications in the areas of heating.

**DID YOU
KNOW?**

The solar industry is creating jobs five times faster than the job market. In 2017, renewable energy jobs, including solar, overtook the number of jobs related to fossil fuels.

Conclusion:

Distributed solar PV expansion, driven by rapid cost reductions and policy support, is transforming electricity markets. Currently, some distributed solar PV policies can have undesirable effects in the long term, disrupting electricity markets by raising system costs, challenging the grid integration of renewables and reducing the revenues of distribution network operators. Tariff reforms and appropriate policies will be needed to attract investment into distributed solar PV while also securing sufficient revenue to pay for fixed network assets and ensuring that the cost burden is allocated fairly among all consumers.

India's mission objective is to establish India as a global leader in solar energy by creating the policy conditions for solar technology diffusion across the country as quickly as possible. The Mission targets installing 100 GW grid-connected solar power plants by the year 2022. In order to achieve the target, Government of India have launched various schemes to encourage generation of solar power in the country like Solar Park Scheme, VGF Schemes, CPSU Scheme, Defence Scheme, Canal bank & Canal top Scheme, Bundling Scheme, Grid Connected Solar Rooftop Scheme etc. Indian Ranks fourth globally in Solar power generation in 2021. India has established nearly 42 solar parks to make land available to the promoters of solar plants. Kochi International airport is the first airport to run complete on Solar power. The world's Largest Solar Park (Below) in Rajasthan generates 2,245MW of solar electricity.



Capt Rajesh Nair is from the 75th Course, OTA, and was commissioned into 14 Maratha Light Infantry. Post Army service, he has worked in the field of administration for more than a decade, having worked with companies like Wipro, Mahindra Automobile, Tata Communications and Credence Global Solutions.

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+**

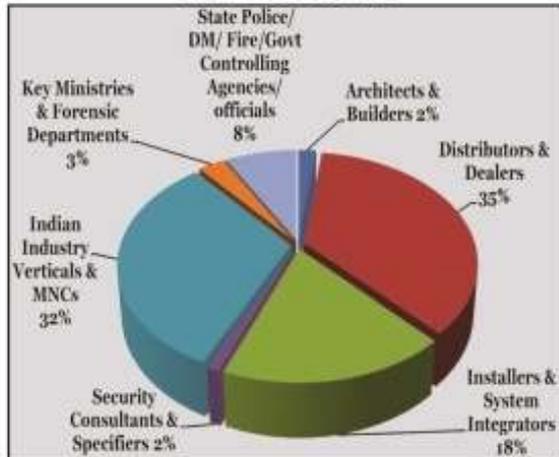
e-Newsportal: www.securitylinkindia.com

✓ **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

Book Review

“The Vortex: A True Story of History's Deadliest Storm, an Unspeakable War and Liberation”

BY SCOTT CARNEY AND JASON MIKLIAN

A RIVETING TALE OF A CATAclySMIC STORM AND THE BIRTH OF A NEW NATION

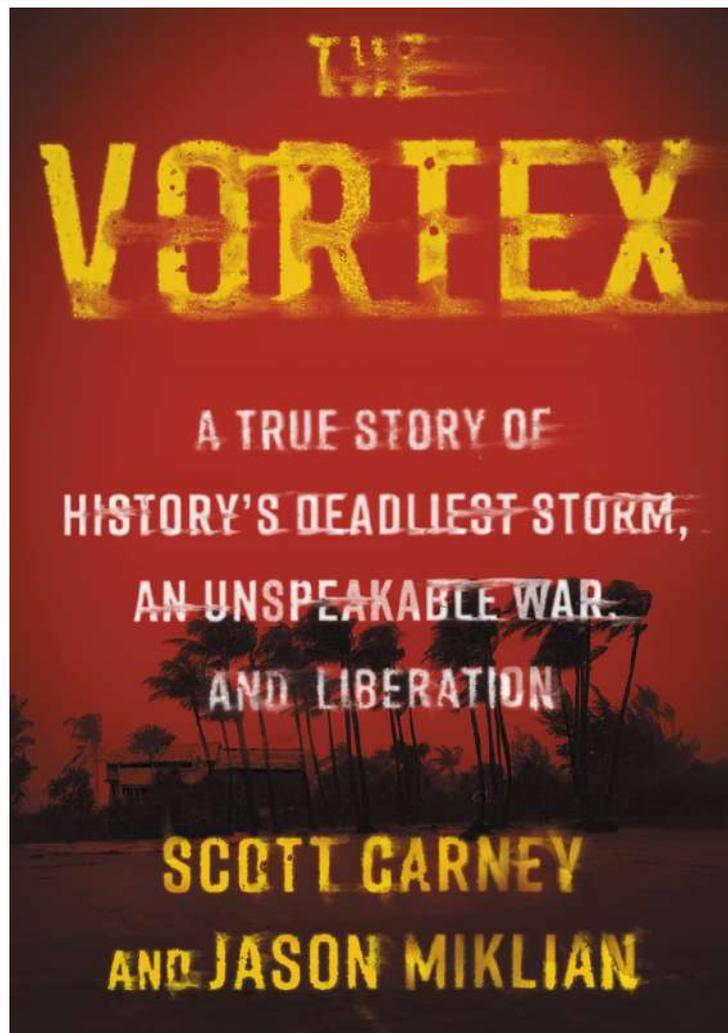
About The Author:

Scott Carney is an investigative journalist and an anthropologist, as well as the author of the New York Times bestseller *What Doesn't Kill Us*. He spent six years living in South Asia as a contributing editor for *WIRED* and writer for *Mother Jones*, *NPR*, *Discover Magazine*, *Fast Company*, *Men's Journal* and many other publications. His other books include *The Red Market*, *The Enlightenment Trap* and *The Wedge*. He is the founder of *Foxtopus Ink*, a Denver-based media company.



Jason Miklian, PhD, is a senior researcher at the Peace Research Institute Oslo, Norway. Miklian has published over sixty academic and policy works on issues of conflict and crisis, based on extensive fieldwork in Bangladesh, Colombia, India and the Congo. He serves on the United Nations Expert Panel on Business and Human Rights, has won several awards for his academic publications, and serves as an expert resource for various government knowledge banks in the US, the UK, the EU and Norway. Miklian has also written for or been cited in an expert capacity by the *New York Times*, the *BBC*, *The Economist*, *Washington Post*, *France 24*, *The Guardian*, *The Hindu* and *NPR*.





“The Vortex: A True Story of History's Deadliest Storm, an Unspeakable War, and Liberation” – at the first instance, I found the title of the book quite intriguing. I was further intrigued when I physically saw the book- it was quite voluminous and surprisingly written by two Westerners. For the uninitiated- the book which is basically about the 1971 War and liberation of Bangladesh, a war most of us Indians know about but I have not seen any detailed western accounts of the same so far.

In November 1970, a huge tropical -“Cyclone Bhola” (which I’m sure none of the readers would have heard of or remember) hit the densely populated Ganges delta and would eventually kill half a million people in erstwhile East Pakistan. The book examines how this calamitous natural event was the last nail in the coffin of Pakistan’s repressive rule in the Eastern part of the country. The Vortex is this dramatic story of how that storm sparked a country to revolution.

The imagery of the physical cyclone vis a vis the geo-political storm of equal intensity brewing in the same geography paints a very poignant and enthralling tale of heroism and courage, deceit and war as also tragedy and the triumph of common people against great odds. It has strong women characters accomplishing the near-impossible, good people helping others, and characters you can't help but care fiercely about.

The storm that set it all in motion calls to mind the increasingly destructive weather events we're seeing now. It makes this riveting story all the more relevant to our world, and our political realities. This book is a testament to the prelude which led to the creation of Bangladesh as an aftermath of deaths, genocide and war.

In November 1970, a storm set a collision course with the most densely populated coastline on Earth. Over the course of just a few hours, the Great Bhola Cyclone would kill 500,000 people and begin a chain reaction of turmoil, genocide, and war. The Vortex is the dramatic story of how that storm sparked a country to revolution.

Cyclone Bhola made landfall during a fragile time, when Pakistan was on the brink of a historic election. The fallout ignited a conflagration of political intrigue, corruption, violence, idealism, and bravery that played out in the lives of tens of millions of Bangladeshis. Authors Scott Carney and Jason Miklian take us deep into the story of the cyclone and its aftermath, told through the eyes of myriad men and women from different walks of life who lived through it, including the infamous president of Pakistan, General Yahya Khan, and his close friend Richard Nixon; American expats Jon and Candy Rhode; soccer star-turned-soldier Hafiz Uddin Ahmad; and a young Bengali revolutionary, Mohammed Hai. The tale not only spins beautifully around all these contrasting protagonists but also sets a thrilling pace to the narrative.

The Vortex is not just a story about the painful birth of a new nation but also a universal tale of resilience and liberation in the face of climate emergency that affects every single person on the planet and how an long forgotten climate event was the final trigger in the strife and war which lead the birth of a new nation- Bangladesh.

Overall the authors have indeed done justice to this not so well remembered theme and narrated it in a non-conventional manner to make the tale riveting and interesting. Definitely recommended for all history and geo-politics buffs as well as to the readers of the younger generation for who it will give a very good insight of a very important event which took place over 50 years ago in which India played a major part.

Pros:

- It is a painstakingly detailed account of one of the most significant and decisive military conflicts fought after the Second World War which eventually led to the liberation and formation of an independent nation.
- Most of us know about the 1971 Bangladesh War but did not know much about the natural calamity which was an important catalyst in triggering it. This book is able to establish this not so well understood link between climatic events and political happenings.
- The narration is very well-paced and the writing style is gripping which makes this piece of historical writing a stirring and interesting read.

- The political drama and intrigue featuring major historical figures such as Nixon, Yahya Khan, Mujib and Indira Gandhi makes the narrative completely believable and compelling.
- The Vortex brings to light the immense struggles and valour of the Bengali freedom fighters who fought against great odds and at great risk against a ruthless and immoral oppressor.

Cons:

- In spite of the extensive research I found a few errors in the dates of certain events mentioned in the book.

About the Book:-

Title: The Vortex: A True Story of History's Deadliest Storm, an Unspeakable War, and Liberation
Author: Scott Carney and Jason Miklian
Publisher: HarperCollins India
Pages: 528
Cost: Rs 599.00



Col Arun Hariharan a.k.a Harry, is an Indian Army veteran. An avid biker, author, poet, compulsive traveller, photographer and history buff- he's always loved exploring the unexplored. His collection of Short Stories titled "A Baker's Dozen- 13 Chilling Indian Tales of Macabre" which incorporated three of his passions - travel, history and exploring local legends-was published in October 2021 by Creative Crow Publishers, New Delhi, India. In 2022, his poetry and stories have also been published in a number of international anthologies including "Quarantine Days", "I Ain't a Saint", "Guru Kalpana", "Coupled Uncoupled", "Open Skies Poetry", "Dandelions: Multiverse of Poems", "Efflorescence" and in the literary journal "Rhyvers Beat".

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



Col Narender Bahal and Capt John K Chandy at Dublin

No one can miss Capt John in Dublin, Ireland

Incase you do meet, 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/>

