THE CRPF ACADEMY JOURNAL

CRPF ACADEMY, GURUGRAM, HARYANA
ISO 21001 : 2018

Annual Issue- Edition II

Jan-Dec- 2025

> Discipline, Courage, and Commitment - the foundation of every warrior trained at the CRPF Academy

The CRPF Academy Journal

Annual Issue- Edition II Jan-Dec-2025

Website: crpf.gov.in/Training/CRPF-Academy

The CRPF Academy Journal

Annual Issue- Edition II Jan-Dec-2025

Published by

CRPF Academy, Gurugram

OUR MISSION

The CRPF Academy develops and delivers professional training to prepare leaders for current and emerging security challenges. Our purpose is to groom officers in battle craft, human resource management, combat logistics, and leadership, enabling them to serve the Force and the Nation with distinction.

Our mission is vital to the Nation and the CRPF. As a premier training institution, the Academy provides strategic advantage by shaping highly trained, disciplined, and professional warriors who strengthen the bond between the CRPF and the people it serves.

OUR VISION

To carry forward the proud legacy of the CRPF and its tradition of multi-spectrum combat excellence by building a forward-looking institution that delivers world-class training and develops exceptional leaders of character, competence, courage, and unmatched operational effectiveness.

To achieve this vision, the CRPF Academy shall pursue the following objectives:

HUMAN RESOURCE DEVELOPMENT

Assist the Directorate General in preparing a roadmap for recruiting, training, developing, and retaining top-quality professionals who are physically fit, mentally resilient, ethically grounded, and ready to be deployed, fight, and win decisively in any operational theatre.

ORGANISATIONAL EXCELLENCE

Ensure that officers are trained in the art and science of building effective organisations, covering the complete spectrum from human resource management to logistics, intelligence to reconnaissance, and electronic warfare to cyber operations. This will enable them to face complex, multi-domain challenges with confidence and professionalism.

TRAINING

Focus on training for high-intensity asymmetric warfare, hybrid threats, internal security challenges, and emerging forms of conflict. The Academy shall progressively incorporate synthetic training environments, simulation-based learning, technology-enabled instruction, and realistic field exercises to enhance operational readiness.

LEADERSHIP

Prepare and groom confident, thoughtful, innovative, and ethical leaders who are comfortable with complexity and capable of operating effectively from the tactical to the strategic level. The Academy shall develop a talent-based training system that leverages the knowledge, skills, attitude, and behaviour of officers to prepare them for higher responsibilities.

CONTINUOUS IMPROVEMENT

To achieve and sustain these objectives, the CRPF Academy shall continuously assess all aspects of training and institutional functioning. It shall identify lower-value training activities for rationalisation, strengthen essential training areas, and improve methods to optimise the use of time, human resources, and financial resources.

INDEX

S. No.	Contents	Page No.
01.	**Cognition, Metacognition and Dognition** **Dr. B. Veerraju**, DIG Principal, DB & TS, CRPF, Bangalore	1-5
02.	**भारत में नक्सलवाद** **श्री प्रशांत कुमार**, पुलिस अधीक्षक, जिला–नारायणपुर	6-9
03.	**MOB Violence, RIOT Control and RAF** **Sh. Manoranjan Kumar**, Second-in-Command, 3rd BN, CRPF	10-17
04.	**Multi-Tasking K9s: Sentinels of Internal Security of the Nation** **Sh. Mahendra M Hegde**, Second-in-Command, 42 BN, CRPF	18-25
05.	**Understanding the IED Threat Picture and Comprehensive C-IED Policy: Need of the Hour** **Sh. D Bagade**, DC, IIM Pune	26-31
06.	**The Evolving Landscape of Challenges in the Cyber World** **Sh. Shubham Gupta**, Asstt. Comdt., Ministry of Home Affairs	32-38
07.	**Digital Connectivity and Emerging Threats in India** **Sh. Azimul Haque**, Asstt. Comdt., CIS Kadarpur, (Int Dte)	39-45
08.	**Naxalism in India; Its Economic Impact** **Sh. Arvind**, (Chief Security & Brand Protection), Tata Steel Limited	46-49
09.	**Admissible Dues in CRPF** **Sh. Vijay Kumar Bains**, Second-in-Command, Welfare Dte., CRPF	50-53
10.	**सिलगेर स्कूलः नई सुबह की पहली किरण** **श्री कुलदीप सिंह**, उप कमांडेंट, 229वीं वाहिनी, के०रि०पु० बल, बीजापुर (छत्तीसगढ़)	54-57
11.	**Invisible Threats, Visible Solutions: Strengthening CRPF's Tech Defences** **Sh. Tarang Bansal**, Asst. Comdt., 4th Signal BN, Neemuch	58-60

1 Cognition, Metacognition and Dognition

Dr. B. Veerraju, DIG
Principal, DB&TS, CRPF,
Bangalore

Humans and dogs are the most successful species in the evolutionary trajectory on planet Earth. The collective journey and bonding were made possible due to interspecies communication, symbiotic living and mutual support rendered by both. The literary and material evidence suggests that the bonding and appreciation of dogs' importance in human communities for ages. Many memorials were erected to commemorate the role of dogs both in wars and in peace. Some societies deified dogs and even erected temples. The anthropological evidence of social evolution has brought out that humans lived as hunters and food gatherers in primitive societies. In such societies the dogs were used for quarrying, retrieving game to facilitate human hunting expeditions and food gathering. As the human societies graduated into sedentary agricultural societies, dogs became guards, shepherds, scouts and have alerted humans to lurking dangers. When humans had conflicts with other groups, dogs also fought battles at the instance of their masters. Further, when the wars were fought from trenches and well-defended positions the flat trajectory weapons were rendered useless. The stealth attack of trained war dogs on enemies used to create panic and lead to ejection of troops into the field of fire. During World Wars, dogs were also used as suicide bombers by strapping explosives around their bodies. The dog-human communication, inferential learning, human intention reading and dogs' species potential made them omnipresent on the face of the earth. Unlike our evolutionary ancestors, the primates, understanding dog's intelligence will throw new light and amazement to humans and makes it a curious conundrum. It is the growing literature on dogs' cognitive abilities that has made them the most sought-after species to address growing security challenges in the world.

Deploying Concepts:

Cognition is all about how humans understand the world around drawn through sensory experiences. Metacognition is the interpretative tool we deploy to understand why we think the way we think. It is about knowing the mental processes and self-awareness. It is a thought process facilitating understanding of humans as concept-bearing animals. Dogs have been domesticated by humans since times immemorial and the close living has made them read human intentions, which could enable them to draw inferences of human communicative intent, thereby facilitating humans in better understanding themselves. Dogs' inferential learning and intention reading can be termed as dognition.

Tracing the Dog-Human relations:

Since the role of dogs in human societies spans beyond historical times, it is difficult to figure out as to when the collective journey commenced. Modern humans' arrival around 43,000 years ago on the Earth is a game changer. Their hunting expeditions drove large Ice age animals to extinction. Our success story as feeble, yet intelligent species would not have been possible without dogs. The humility with which we locate our past narrative in the shared ecological space will make us behave responsibly to the species which made us what we are on the planet Earth. The success of human hunting expeditions owes much to Dogs as companions by leading us to prey, quarrying and shooting at the hunted and their retrieval. Dogs' olfaction picked up scent signature of all the prey movements leading humans from the forefront. Dogs

defended humans in counterattacks in prey–predator conflicts. Needless to say, it is the dog-human co-option that has made us the predominant and fate deciding species of the planet Earth.

According to evolutionary biologists, humans share 98.5% genepool with primates and dogs share 99% genepool with wolves. Yet, no two other species in the wild have successfully ganged up in hunting like Humans and Dogs despite having diverse evolutionary history and different cognitive abilities. Of course, it is the cognitive convergence which made the success story possible. The ability to forecast moves of prey and carefully working through manipulation by dogs to foreclose the escape made humans successful hunters. Even today tribal societies the rely heavily on dogs for hunting. Humans have selected, manipulated, experimented in the dog evolution to make the dogs into different breeds. The dog breeds we see today as hunters, retrievers, shepherds etc. are the products of human manipulation and our tampering of dogs' gene pool. Exposure hypothesis suggests that in the company of human habitat the dogs have started understanding gestures, gaze and pointing by humans. War has been a human enterprise but dogs have been deployed to settle scores between states even in ancient times. The modern invention of weapons and the immense destructive power of nation state have also not done away with war dogs. Dogs' maneuverability, ability to penetrate into enemies well defended positions, capacity to cognitively figure out the friendly forces and enemies came in handy to the warring nations to deploy them in the war enterprise. The scent discrimination capabilities of war dogs have also come handy in tracking the enemy movements and facilitated mobile and position wars possible.

Need of deploying cognitive tools in K9 Training:

There is a need to overcome the behaviorism-based training modules developed and deployed in most of the K9 training schools in India. The operant conditioning developed by B. F. Skinner, and positive reinforcement methods by Thorndike have been found not all comprehensive and fraught with certain shortcomings, which are as follows.

1. Behaviour is dictated by nothing more than a series of stimulus-response mechanisms.
2. In reaction to consistent stimulus, the response should become stronger over time (that was what the charts coming out of the Skinner boxes showed so beautifully).
3. Behavioralism suffers from the fallacy of presumption that all animals and humans are uniform (what works for a pigeon should work for a dog, pig, rat, human, et cetera).
4. All behavior can be predicted and controlled, and therefore the inner workings of the mind (thoughts, memories, emotions) are irrelevant.

All the tenets espoused by Behaviourist fall short of explaining the community living and cognitive learning of humans as well as animals. The lab conditions cannot be replicated in a social setting. The stimulus-response mechanism does not explain the learned behavior of animals and humans. Secondly, the repetitive responses conditioning the behavior is a short-sighted view of cognitive potency of animals. Thirdly, one single model of behaviour testing that will fit all animals is fraught with many shortcomings. As such sweeping conclusions have conveniently ignored individual cognitive competencies of species. Fourthly, making inner feelings, emotions, thoughts and memories irrelevant just because they cannot be gauged is incomplete in drawing inferences about cognizance of different species.

Dog behaviour cannot be understood without knowing its unique intelligence which can be summarized as under:

1. Learning new things from others
2. Ability to cooperate and gain strength
3. Ability to learn from peers
4. Dogs are sometimes faster at solving problems when they observe someone else's success rather than experiencing the same success themselves, which is part of an inferential learning.
5. All dogs are quite skilled at reading human gestures.

In nature different species have different cognitive capabilities. Siberian Cranes travel across continents without using any GPS, to breed in India and revert back. Nutcrackers hide as many as one lakh seeds and safely retrieve them during lean season. Dog's as a species have variety of cognitive capabilities. They have supplemented and complimented human intelligence in working solutions to many complex security related problems of human societies. In primitive societies, dogs accompanied humans in hunting expeditions, defended caveman families against predators, acted as alarm systems for humans by alerting them to impeding threats by using their olfactory, auditory, visual capabilities. In the modern human societies, dogs have more jobs than they had in previous centuries. In modern wars, they have acted as messengers, attackers, trackers, suicide bombers and performed multiple functions as humans made them to do. Their enhanced capabilitiy to detect trace amounts of chemical scent in the air and from the ground beneath has made them human vanguards. The pressure mines, Improvised Explosive Devices used against security forces have been neutralized through the help of well-trained K9 teams. The modern-day police K9 units have been able to solve crimes in civil society by tracking the criminals by taking clues from the scent. The job profile of the K9 has increased manifold. The trades performed by K9s include sniffers, guards, explosive detectors, police patrol K9s, infantry patrolling K9s, Narcotics and other contraband detection and so on. The K9 use is constrained by our own imagination.

It is in the right earnest to gauge dog's intelligence to understand and open up new vistas in cognitive psychology, to draw inferences and inputs facilitating interspecies communication.

Our behavior should be adjusted according to the communicative intent. Psychologists have studied dogs' behaviour to understand humans as they have shown different cognitive skills. Through domestication they have understood human communicative intent. Through bonding they have been able to read the mental state of humans and acted accordingly as a motivator. They have understood the human gesture of pointing and relied more on human help in various activities viz. retrieving, finding food, moving in the direction of a happening, or to search for objects etc. They can also understand human speech and respond accordingly. Dogs can also make out the difference between intentional and unintentional actions of humans, whether a person intentionally trampled the tail or it was accidental.

The theory of mind describes human's ability to attribute mental states to other people and to animals. It is established that the dog has its own way of appreciating human communicative intent.

In the early days of behaviorism, the focus of Watson, Skinner, and many of their followers presupposed that in a social set up what matters most is the observable, measurable behavior. Since subjective mental states cannot be gauged, their study is of little relevance. The cognitive psychology has

given equal importance to the mental processes like learning, memory, thought process and problem solving.

But as the cognitive science has developed the mental events taking place inside the mind have taken precedence over the observable overt behavior.

(The cognitive science deals with inferential learning, new problem-solving capabilities.)

Understanding dogs will give insights into human intelligence. As the 'Exposure Hypothesis' suggests that in the company of human family dogs learn gestures and understand human gaze and pointing.

Whereas the Behaviorists predict the response to be overt and predictive, the counter intuitive patterns suggest that the dog's cognitive abilities prove otherwise. Let us say that when a dog predicts an earthquake it will not run away to save its life, But will alert the human master and try to take him away from the possible danger of a building collapse.

Understanding dognition will also help humans in developing cooperative behavior in a social setup. Though conflicts are natural in the animal world, the feral dogs do not inflict mortal wounds on one another. The dog's evolution success story establishes that it is the survival of the friendliest species, contrary to the Darwinian version of fittest, which produced, multiplied and prevailed on the earth. It is the selection against aggression, ability to cooperate and communicate with humans made them successful. Needless to say, if dogs have not come to our rescue, in the evolutionary journey, human progress could have been short circuited.

The comparative social cognition addresses the challenges of social living – it factors in the social communication, social learning, social understanding. Understanding dog changes human life in multiple facets – communicative, cooperative, social, attachment behavior.

Social cognitive learning theorists, who emphasize the importance of both the influences of other people's behavior and of a person's own expectancies on learning, hold that observational learning, modeling, and other cognitive learning techniques can lead to the formation of patterns of personality. One of the more well-researched learning theories that includes the concept of cognitive processes as influences on behavior is the social cognitive theory of Albert Bandura. In the social cognitive view, behavior is governed not just by the influence of external stimuli and response patterns but also by cognitive processes such as anticipating, judging, and memory as well as learning through the imitation of models.

Whereas the life processes of animals are fixed to the smallest details by rigid and hereditary instincts, the social pattern and interrelationships of human beings are very variable and susceptible to change. Human memory system and oral communication have enabled them to overcome the biological determinants and facilitated the evolution of science, technology and literature. Humans also have evolved traditions, institutions, and organizations to develop better life-support systems and cooperate through his own conduct and conscious thinking. Dogs through human bonding have been able to overcome some of the biological determinants making them a distinct species.

Conclusion:

The dogs' close understanding of human communication intent and inferential reading of human intentions is an aspect that still holds relevance and will be key to solving many mysteries. The insights will not only cement the bonding further but also holds the key to solving many of the current day policing challenges. Dogs' cognitive faculties have many cognitive convergence functions with humans, viz., solving crime mysteries, detection of cancer, narcotics detection, bomb detection, protection of endangered species, as early warning systems for the impending climatic and natural calamities, and many other human problems for which solutions are yet to invented.

***

2 भारत में नक्सलवाद

श्री प्रशांत कुमार
पुलिस अधीक्षक
जिला–नारायणपुर

प्रस्तावना – नक्सलबाड़ी गांव के नाम पर ही उग्रपंथी आंदोलन को नक्सलवाद कहा गया है, इसकी उत्पत्ति पश्चिम बंगाल से हुई है, जो जमींदारों द्वारा छोटे किसानों पर किये जा रहे उत्पीड़न पर अंकुश लगाने के लिए भारतीय कम्युनिस्ट पार्टी के कुछ नेता सामने आए। इन नेताओं मे चारू मजूमदार, कानू सान्याल और कन्हाई चटर्जी का नाम प्रमुख है। चारू मजूमदार को नक्सलवाद का संस्थापक भी माना जाता है।

1. **जिला नारायणपुर में नक्सलवाद की समस्याओं की पृष्ठभूमि/उत्पत्ति/रूझानः**– जिला नारायणपुर छत्तीसगढ़ राज्य के दक्षिण पश्चिम सीमा पर राजधानी रायपुर से 230 किमी0 की दूरी पर स्थित है। जिले का भौगोलिक क्षेत्रफल 6640 वर्ग किलोमीटर है। उत्तरी सीमा जिला कांकेर व दक्षिण सीमा जिला दन्तेवाड़ा, बीजापुर व पूर्व सीमा जिला बस्तर व पश्चिम सीमा महाराष्ट्र राज्य के जिला गढ़चिरौली से लगा हुआ है। यहां मुख्यतः हिन्दी, गोण्डी, हल्बी, छत्तीसगढ़ी भाषायें बोली जाती है। यहाँ प्रमुख कुकुर व माड़ीन नदी बहती है। जिला नारायणपुर विधानसभा क्षेत्र क्रमांक 84 (नारायणपुर) बस्तर लोकसभा क्षेत्र क्रमांक 10 के अंतर्गत आता है। जिला नारायणपुर का संपूर्ण क्षेत्र नक्सल प्रभावित अतिसंवेदनशील एवं सघन वनों/पहाड़ियों से आच्छादित क्षेत्र है, यह क्षेत्र अबुझमाड़ में अधिक सघनता एवं सर्वाधिक वन क्षेत्र है। छत्तीसगढ़ राज्य की समीक्षा वर्ष 2013 के अनुसार सर्वाधिक वन क्षेत्र नारायणपुर के अंतर्गत पाये जाते है। नारायणपुर जिला व अबुझमाड़ क्षेत्र जहां वन/पहाड़ियों की सघनता और आच्छादन होने के कारण इसी का लाभ नक्सलियों ने अपने छुपाव एवं शरणस्थली के साथ–साथ अपने संगठन को सुदृढ़ बनानें के लिए इसका चयन किया है। अबुझमाड़ क्षेत्र में रहने वाले आदिवासी भोले–भाले एवं सरल स्वभाव के है। शासन द्वारा आदिवासी बाहुल्य क्षेत्र होने के कारण वन, संस्कृति, भाषाशैली एवं परंपरा को सुरक्षित रखने के उद्देश्य से अबुझमाड़ को आरक्षित क्षेत्र घोषित कर दिया गया था, जिसका लाभ उठाने में नक्सलियों ने अपनी कोई कसर नहीं छोड़ी क्योंकि इस दौरान पुलिस एवं प्रशासन की उपस्थिति शून्य हो गयी थी। यहां के निवासियों का नक्सलियों के साथ पहली बार आमना–सामना हुआ, तब उन्हें देखकर एक नाम दिया "गुफा पल्टून" – यह शब्द क्षेत्रीय बोली गोण्डी, हल्बी, दण्डामी, भतरा का था और न ही हिन्दी अथवा अंग्रेजी शब्दकोश में छुपा था। इसका अभिप्राय शब्द विच्छेदन से गुफा अर्थात कंदरा या जहां छिपाव प्राप्त किया जा सके तथा पल्टून का मतलब सैनिकों का दस्ता से किया गया। नक्सलियों द्वारा प्रकाशित पत्रिकाओं के आधार पर 1910 में "भूमकाल" बगावत के दौरान जल, जंगल, जमीन के लिए संघर्षरत आदिवासियों के लिए इसका उपयोग करते थे।

जिला बस्तर लोहण्डीगुड़ा (जगदलपुर) में मारडूम से विस्थापित लोगों को अबुझमाड़ के पश्चिम क्षेत्र कोहकामेटा के रानीगांव में दण्डामी माड़िया जन जाति के लोगों को बसाया हुआ है। वे जंगल साफ कर कृषि योग्य एवं आवासीय स्वरूप झोपड़ियों का निर्माण कर रहे थे, उन झोपड़ियों को वन विभाग के कर्मचारियों द्वारा जला दिया गया। जन–जातियों और आदिवासी पीड़ित परिवारों द्वारा शासन को शिकायत की गई किन्तु कोई कार्यवाही नहीं की गई। ये अंत में हार मानकर नक्सलियों के पास "गुफा पल्टून" गये। उन्होने उन वन विभाग के कर्मचारियों को बहुत पीटा और आदिवासियों का विश्वास जीत लिया। यह समय दशक 1980 के अंत और 1990 का शुरूआती दौर था और यह संभावित नारायणपुर की प्रथम नक्सली गतिविधि थी। धीरे–धीरे दौर आधुनिकीकरण और परिवर्तनशील होने लगा और नक्सली अपने संगठन को मजबूत करने में ग्रामीणों के साथ संगठित होकर अपनी फरमाईशों की ओर अग्रेषित

होने लगे। क्षेत्र के पिछड़ेपन का लाभ लेते हुए नक्सलियों द्वारा ग्रामीणों का विश्वास हासिल करने के लिये शासन की नीतियों का दुष्प्रचार कर उनकी छोटी–छोटी समस्याओं का निराकरण कर हितैशी बनने का प्रयास होता रहा। किन्तु नक्सलियों को यह भी भय बना हुआ था कि ग्रामीणों का विश्वास हमसे उठ जाने पर कोई हमारा विरोध न कर सके, इसके लिये नक्सली क्षेत्र के ऐसे व्यक्ति जो नक्सलियों की नीतियों का समर्थन नहीं करता है उसकी निर्मम हत्या करने लगे और परिवार को गांव से भगाने लगे ताकि अन्य लोगों में दहशत बनी रहे और ग्रामीण संगठित होकर उनका विरोध न कर सकें। जिसमें पूरे बस्तर क्षेत्र में नक्सली अपनी विचारधारा को लागू करने में कुछ हद तक सफल भी रहे। नक्सलियों द्वारा अपने संगठन में समर्पित ग्रामीणों को शामिल कर उनकी मदद से पुलिस के आधुनिक हथियारों को लूटने, उन्हें क्षति पहुचाने तथा शासन की योजनाओं को विफल करने में जुट गये। अबुझमाड़ क्षेत्र में नक्सलियों के बढ़ते जनाधार एवं उनके आतंक पर लगाम लगाने तथा नक्सली उन्मूलन में तेजी लाने के लिए वर्ष 2003 में नारायणपुर को पुलिस जिला के रूप में गठित किया गया तथा इसी क्रम में जिला बस्तर से पृथक कर दिनांक 11 मई 2007 में नारायणपुर को जिला घोषित किया गया।

वर्ष 1993 में नारायणपुर के पनीरा में स्थित मतदान केन्द्र से विधानसभा निर्वाचन सम्पन्न कराकर पुलिस पार्टी ट्रक वाहन में सवार होकर वापस आ रही थी कि धनोरा के पास माओवादियों द्वारा बम विस्फोट किया गया जिसकी चपेट में आने से ट्रक में सवार बीएसएफ के 13 जवान शहीद हो गये थे। ऐसा माना जाता है कि यह नारायणपुर का द्वितीय नक्सली घटना थी, जिसका थाना छोटेडोंगर, तत्कालिन जिला बस्तर (वर्तमान जिला नारायणपुर) में नक्सलियों के विरूद्ध अपराध में आलेखित किया गया। इसी प्रकार नारायणपुर में नक्सलियों द्वारा किये जाने वाली वारदातों में वृद्धि होने लगी, जिसका जिला पुलिस बल एवं राज्य सशस्त्र बल की कमियों के कारण इससे निपटारा पाना संभव नहीं था। शासन द्वारा जिला बस्तर के विभिन्न नक्सल प्रभावित इलाकों में नक्सलियों से संघर्ष करने एवं लोहा लेने के लिए केन्द्रीय बल का स्थापित होना आवश्यक हो गया। वर्ष 2000 में नक्सलियों द्वारा नारायणपुर थाना से 07 किमी0 दूर बाजुलयाही ग्राम की ओर जाने वाले रोड़ (फौचवाही नाला के पास) में अतिरिक्त पुलिस अधीक्षक, नारायणपुर श्री भास्कर दीवान के हमराह फोर्स 407 वाहन में सर्चिंग पर जा रहे थे कि नक्सलियो द्वारा बिछाये गये बारूदी सुरंग से 407 वाहन को विस्फोट से उड़ा देने पर सभी 23 पुलिस जवान मौके पर ही शहीद हो गये। नक्सली, पुलिस जवानों के हथियार, कारतूस एवं गोलाबारूद भी लूटने में सफल हो गये जो नारायणपुर की सबसे बड़ी वारदात मानी जाती है। नक्सलियों द्वारा पी0एल0जी0ए0 (PLGA) के नफसती गौतम उर्फ गोपन्ना के नेतृत्व में इस घटना को अंजाम दिया गया था, जिसमें कोहकामेटा, केशकाल, अबुझमाड़ कोण्डागांव के नक्सली सदस्य शामिल हुए थे। पुलिस की जवाबी कार्यवाही के दौरान माह डिविजन के नक्सली सोमन्ना, सविता, कविता, रमेश एवं लिंगा को मार गिराने में पुलिस सफल रही। वर्ष 2008 में दिनांक 13.08.2008 को तत्कालीन स्थानीय सांसद बलीराम कश्यप के नारायणपुर आगमन के दौरान थाना बेनूर क्षेत्रान्तर्गत छेरीबेड़ा – चौड़ंग के पास पुलिस पार्टी को जान से मारने की नियत से पुलिया में बारूद रोपित कर पुलिस पार्टी की जीप को लैंडमाईन विस्फोट कर क्षतिग्रस्त कर दिया गया। जिसमें सवार पुलिस जवान घायल हो गये। वर्ष 2010 में थाना धौड़ाई के अंतर्गत केन्द्रीय रिजर्व पुलिस बल की पुलिस पार्टी आर0ओ0पी0 ड्यिूटी हेतू निकली थी कि ग्राम माहरावेड़ा (राकरानाला) के पास अधिक संख्या में उपस्थित होकर पुलिस पार्टी पर एम्बुश कर प्राणघात हमला किया गया जिसमें के0रि0पु0 बल के 27 जवान शहीद हो गये। यह नारायणपुर में शहीद जवानों की सूची में सबसे बड़ी वारदात मानी जाती है।

नारायणपुर में दण्डकारण्य भाकपा (माओवादी) के उत्तर रिजनल कमेटी में आता है, अन्तर रिजनल कमेटी के अंतर्गत माड़ डिविजन, उत्तर बस्तर डिविजन एवं पूर्व बस्तर डिविजन शामिल है। माड़ डिविजन घनी पहाड़ियों से भरा ईलाका है जो 1988 के लगभग, बस्तर और गढ़चिरौली डिविजनों में शामिल था। माओवादियों द्वारा परलकोट विद्रोह 1825 एवं भूमकाल 1910 जैसी बगावतों को ऐतिहासिक बताते हुए एक विशेष प्लान में माड़ डिविजन का चुनाव किया गया, जिस समय एस.जेड.सी. सचिव के पद पर भूपति पदासीन था। वर्ष 1999 के जुलाई माह में भाकपा (माओवादी)

द्वारा माड़ डिविजन को नया स्वरूप प्रदान किया गया, जिसके सचिव की कमान कोसा को सौंपी गई। कोसा द्वारा इस अधिवेशन में माड़ डिविजन के अध्यक्ष मण्डल के तौर पर जूरी, राधा, और राजमन को तथा स्टीयरिंग कमेटी के तौर पर पाण्डू और सोनू की नियुक्ति की गयी। माड़ डिविजन को पृथक करने का उद्देश्य पी.एल.जी.ए. की स्थापना और दण्डकारण्य को मुक्त इलाके में विकसित करने के लक्ष्य से किया गया था। इसके बाद माड़ डिविजन स्थापना वर्ष 2010 में प्रभारी अल्लूरी कृष्ण कुमारी उर्फ सुजाता उर्फ सुजाताक्का, के नेतृत्व में 03 एरिया कमेटी (इन्द्रावती एरिया कमेटी, कुतूल एरिया कमेटी एवं नेलनार एरिया कमेटी), 02 एल.जी.एस. (ओरछा, कोहकामेटा), 08 एल.ओ.एस. (कुतुल, फोहकामेटा, परलकोट, इन्द्रावती, जाटलूर, ओरछा, नेलनार, झारा), 01 प्लाटून (प्लाटून नं0 16) और 01 कम्पनी (कम्पनी नं0 01) सक्रिय रूप से कार्यरत हुई। माड़ डिविजन की कम्पनी नं0 01 जिसका कमाण्डर अरूण उर्फ रूपेश सी.वाय.पी.सी. निवासी आमगांव जिला कांकेर था। नारायणपुर में माड़ डिविजन ही सक्रिय रूप से कार्य करती थी, जिसके अंतर्गत इन्द्रावती एरिया कमेटी, कुतूल एरिया कमेटी एवं नेलनार एरिया कमेटी सहित तीनों एरिया कमेटी सक्रिय रूप से कार्य कर रही थी। उत्तर बस्तर डिवीजन की स्थापना वर्ष 2014 (वर्ष 2014 में एस.जेड.सी. मीटिंग के अनुसार माड़ उत्तर बस्तर संयुक्त डिवीजन में पुनः विभाजित किया गया) जिसके प्रभारी एवं सचिव राजमन मण्डावी निवासी आन्ध्रप्रदेश (एस.जेड.सी. सदस्य) थे। कम्पनी नंबर 05 जिसके कमाण्डर राजू डी.व्ही,सी.एम. निवासी मर्दा बने। इस डिवीजन के अंतर्गत जिला नारायणपुर में 03 एरिया कमेटी एवं 03 एल.ओ.एस. तथा कम्पनी नंबर 05 सक्रिय रूप से कार्य करती है। पूर्व बस्तर डिवीजन की स्थापना 2007 में की गई, जिसका कार्य क्षेत्र जिला कोण्डागांव का संपूर्ण भाग एवं नारायणपुर जिले का पूर्वी क्षेत्र आता है। जिसके प्रभारी कमलेश निवासी एनमालूर आन्ध्रप्रदेश (एस.जेड.सी. सदस्य) एवं सचिव उर्मिला उर्फ नीति निवासी गंगालूर नियुक्त किये गये। इस डिवीजन के अंतर्गत 04 एरिया कमेटी (बारसूर, बयानार, अमदई, बोघघाट), 03 एस.जी.एस. (बारसूर, बयानार अमवई), 01 एल.ओ.एस (बोघघाट) एवं 01 कम्पनी कार्यरत हुई। कम्पनी नंबर–06 के कमाण्डर नंदु मण्डावी – CYPC निवासी कोतारम कोंटा जिला बीजापुर को दायित्व सौंपा गया।

02. **बलों की तैयारी**:– जिला नारायणपुर में वर्तमान में 14 थानें एवं 13 कैंप स्थापित किये गये। जिनमें केन्द्रीय बल की आईटीबीपी की 45वीं0 वाहिनी (05 कम्पीन तैनात), 53वीं0 वाहिनी (05 कम्पनी तैनात), 29वीं0 वाहिनी (05 कम्पनी तैनात), 41वीं वाहिनी (01 कम्पनी तैनात) तथा बीएसएफ 11वीं वाहिनी की 03 कम्पनी और बीएसएफ 135वीं0 वाहिनी की 05 कम्पनियाँ तैनात की गई, एवं छत्तीसगढ़ सशस्त्र बल की 05 कम्पनियाँ तैनात की गई। क्षेत्र की नक्सल संवेदनशीलता को देखते हुए जिला नारायणपुर में नक्सल विरोधी अभियान हेतू जिला बल से पृथक कर लड़ाकू दस्ता तैयार किया गया जिसे डीआरजी (डिस्ट्रीक्ट रिजर्व गार्ड) का नाम दिया गया। इस फोर्स के गठन के पश्चात नक्सल क्षेत्र में महत्वपूर्ण उपलब्धियां हासिल हुई। चूंकि इसमें स्थानीय भर्ती एवं आत्मसमर्पित नक्सली तथा नक्सल पीड़ित शामिल किया, जिन्हें नक्सल क्षेत्र, नक्सलियों की पहचान के साथ–साथ स्थानीय बोली– भाषा का भी ज्ञान था। यह नक्सलियों के खिलाफ लड़ाई में मील का पत्थर साबित हुई। इसी क्रम में बस्तर फाइटर्स का भी गठन किया गया जिसमें स्थानीय पुरूष एवं महिला बल शामिल किये जिसे स्थानीय परिदृश्य का भी ज्ञान था।

डीआरजी टीम के गठन के उपरांत टीम के जवानों को सीटीजेडब्ल्यु जंगल वारफेयर कॉलेज कांकेर, सीआईटी, ग्रेहाउंड्स (हैदराबाद), सीटीजेडब्ल्यु जंगल वारफेयर कॉलेज वारंगटे, मिजोरम एवं आईईडी संबंधी तथा अन्य प्रशिक्षण देने के पश्चात नक्सलियों के विरूद्ध नक्सल विरोधी अभियान में षामिल किया गया। डीआरजी द्वारा अबुझमाड़ क्षेत्र में लगातार ऑपरेशन संचालित कर हार्डकोर नक्सलियों को मारने एवं उनके सहयोगियों को गिरफ्तार करने में समय समय पर सफलता मिलती रही। जिससे नक्सलियों में पुलिस के प्रति भय कायम हुआ जिस कारण अधिकांश नक्सली संगठन छोड़कर आत्मसमर्पण करने लगे। नक्सलियों के प्रभाव को कम करने के लिये नक्सल प्रभावित क्षेत्रों में क्रमबद्ध तरीके से नवीन कैम्प स्थापित कर सुरक्षा बल तैनात किये गये। नक्सल उन्मूलन हेतू राज्य सरकार द्वारा एसटीएफ, डीएसएफ, गोपनीय सैनिक एवं बस्तर फाईटर्स की विशेष टीम का गठन किया गया।

नक्सलियों द्वारा सुरक्षाबल को नुकसान पहुंचाने के लिए वृहद रूप से आईईडी बारूदी सुरंग का इस्तेमाल किया गया, जिससे निपटने के लिए इकाई में बी0डी0एस0 टीम भी गठन किया गया। जिला नारायणपुर में नक्सलियों के आधार क्षेत्र में सुरक्षा बलों की पहुंच व शासन की कल्याणकारी योजनाओं का लाभ पहुंचाने के लिए नये स्वीकृत कैम्पों का विस्तार किया गया।

03. विभिन्न प्रशिक्षण तकनीकी हस्तक्षेपों की आवश्यकता:— जिलों में तैनात सभी सुरक्षा बलों को बस्तर क्षेत्र के अंदरूनी थाना/कैम्प में तैनात किये जाने से पूर्व सभी अधिकारियों/कर्मचारियों को प्रारंभिक प्रशिक्षण के बाद सीटीजेडब्ल्यु जंगल वारफेयर कॉलेज कांकेर, सीआईटी, ग्रेहाउंड्स (हैदराबाद), सीटीजेडब्ल्यु जंगल वारफेंयर कॉलेज वारंगटे मिजोरम एवं आईईडी संबंधी तथा अन्य प्रशिक्षण दिये जाने के पश्चात सभी जवानों के पूर्ण रूप से पारंगत होने के पश्चात जवानों को तैनात किया गया ताकि नक्सलियों द्वारा जंगल की आड़ में छुपकर लड़ने वाले गोरिल्ला युद्ध पद्धति से जीत हासिल की जा सके। सभी जवानों को शारीरिक एवं मानसिक रूप से मजबूत बनाये रखने के लिए समय–समय पर रिफ्रेशर कोर्स भी कराया गया। जिला नारायणपुर में नक्सलियों को टारगेट करने हेतू नेलनार एरिया कमेटी, बयानार एरिया कमेटी, यारसुर एरिया कमेटी, किसकिड़ो एरिया कमेटी, आमदई एरिया कमेटी, प्रतापपुर एरिया कमेटी, रायपाट एरिया कमेटी, इन्द्रावती एरिया कमेटी, फुतुल एरिया कमेटी एवं बोधघाट एरिया कमेटी में कमेटी वाईज नोडल अधिकारियों को नियुक्त किया गया।

नक्सल मोर्चे में तैनात सभी जवानों को अत्याधुनिक हथियार इंसास, एस0एल.आर, एके–47, एल0एम0जी0, मोर्टार, यूबीजीएल, बाईनोकुलर, एनवीडी, ट्रेकिंग स्टीक एवं कम्यूनिकेशन हेतू सेटेलाईट फोन, सेटेलाईट पर्सनल ट्रेकर, वायरलेस सेट आदि सुविधाऐं प्रदान की गई। नक्सल गतिविधियों का पता लगाने हेतू UAV ड्रोन एवं अन्य तकनीकियों का उपयोग किया गया। जिले में टैक्निकल दृष्टिकोण से सूचना संकलन हेतू कैम्प आमदई घाटी (डोंगरहिल्स) में सेटअप स्थापित किया गया।

04. कानूनी पहलू:— जिला नारायणपुर में नक्सलियों के विरूद्ध समय–समय पर लागू कानूनी प्रावधानों के तहत कार्यवाही की गई। नक्सल उन्मूलन अभियानो के दौरान नक्सली एवं नक्सली सहयोगियों की गिरफ्तारी हेतू हरसम्भव प्रयास किया गया। नक्सलियों के गिरफ्तरी के पश्चात नियमानुसार कानूनी कार्यवाही कर नक्सली आरोपियों को सजा दिलाने का प्रयास किया गया। नक्सल उन्मूलन अभियान एवं छत्तीसगढ़ राज्य की आत्पसमर्पण एवं पुनर्वास नीति के तहत लगातार नक्सलियों को आत्मसमर्पण के पश्चात दी जाने वाली सुविधाओं का व्यापक प्रचार–प्रसार कर उन्हें आत्मसमर्पण हेतु तैयार किया गया। जिला नारायणपुर में दिसम्बर 2024 तक 828 माओवादी आत्मसमर्पण तथा 1603 गिरफ्तार किये गये हैं। इसके अतिरिक्त लगातार जिले में नक्सल ऑपरेशन चलाये जा रहे है। क्षेत्र के विकास एवं अन्य मूलभूत सुविधाओं के परिचालन हेतू सुरक्षा उपलब्ध कराई जा रही है।

नक्सलियों को दी जाने वाली फण्डिंग, पहुँचाई जाने वाली अन्य जरूरतें जैसे राशन, दवाई की सप्लाई चैन को तोड़ने हेतू जिला स्तर पर टीम का गठन कर नजर रखी जा रही है। शासन की योजनाओं को जन–जन तक पहुँचाने हेतू हर सम्भव प्रयास किया जा रहा है। क्षेत्र की जनता के मन में सुरक्षाबलों के प्रति विश्वास बढ़ाया जा रहा है एवं नक्सलियों की खोखली विचार धाराओं से अवगत कराया जा रहा है। ।

***

3 MOB Violence, RIOT Control and RAF

Sh. Manoranjan Kumar
Second-in-Command,
3rd BN, CRPF

Mob violence is like a jungle fire in that if it is not controlled immediately it will spread very fast and damage property extensively. Besides, it will also cause loss of lives and injury to many.

"I am the people – the mob- the crowd – the mass." "Do you know all the great work of the world is done through me?" - Carl Sandburg

A riotous mob is born when members of a crowd are no longer concerned about laws and authority and follow their leaders into unlawful and disruptive acts. Mob behavior is highly emotional, usually unreasonable and likely to erupt into violence.

Any crowd can form into a mob in the following circumstances:-

1. Gathering of a group to vent grievances or protest.
2. Redirection of group's anger from certain issues.
3. Increase of in the size of the group by opportunists, onlookers and bystanders
4. Inciting people to behave irrationally by the agitators
5. Influence of criminal elements to act illegitimately.
6. When groups with antagonistic views face off

What is the most important component of mob violence? Mob violence can't take place until and unless a catalyst is present. It may be called a trigger. As the trigger in a weapon is pulled and the explosion takes place likewise the catalyst results in chaos or mob violence.

In India, we have numerous examples of Mob Violence:-

1. Moradabad Riot
2. Bhagalpur Riot
3. Godhra Riot
4. Muzaffarnagar Riot
5. Shia-Sunni riot in Lucknow
6. Jaat Andolan
7. Gujjar Andolan
8. Koregaon Riot

All these riots are lessons for the enforcement agencies which handle law and order.

Mob Violence has certain traits:-

1. Presence of a Catalyst
2. Suddenness
3. Spontaneity
4. Chaos
5. Protest for Grievance
6. Insanity
7. Illegitimate

Mob violence can be of different types:-

1. Happy Riot or Good News Riot
2. Sporting Riot
3. Communal Riot
4. Caste Riot
5. Racial Riot
6. Prison Riot

In Riot prevention and control, Capt. Charles Beene lists five types of troublemakers found in a typical mob. They are as follows:-

1. **Followers:** They follow their leaders and hardly apply their mind.
2. **Encouragers:** They instigate the mob violence but never participate to keep their hands clean in the eyes of law.
3. **Opportunists:** They wait for the opportune time. They perpetrate violence when no representatives of enforcement agencies are around.
4. **Criminals and thugs:** These are basically opportunists with clear intentions and actions. They have a specific goal to foment trouble to rob the shops, loot banks etc.
5. **Psychopaths:** They are mentally unbalanced persons who don't understand social or moral responsibility. They gratify themselves with their bizarre behaviour and commission of crime.

How does a violent mob think? They think as if they are right in their decision. They think that they are collectively working for a big cause. Mob violence is basically based on mob mentality or mob psychology

Social psychologist Irvin L. Janis, a professor emeritus, at University of California, Berkeley coined the term "groupthink" to describe certain systematic errors by groups while making collective decisions.

Deep analysis of unruly groups shows that only a few in the group are aggressive and

majority are onlookers who are instigated by these handful of aggressors. Curious onlookers, if instigated, become frenzied rioters.

Crowd and riot control is a police science that demands specialized, aggressive, positive action by law enforcement agencies. Controlling an unruly crowd situation is based on factors like intelligence at ground zero, number of participants, capabilities of riot control police, available manpower, quality of training to supervisory and on – line officers and available riot control equipment.

Violent mob-control techniques include show of force, mob containment, dispersal tactics, encirclement of mob and arrests. The key principle of mob control is - SAID. S stands for Speed, A for aggressiveness, I for impartiality and D for decisiveness. Wherever the mob violence has taken place the anti riot force should reach in minimum possible time. The earlier the force reaches the spot, the sooner the violence will be the containment of violence.

The force should be very aggressive and it is required to be reflected in their drills. Half of the mob runs from the spot seeing the aggression of the force and most of them follow the escaping party out of fear.

The force deployed on the ground must be impartial in approach and it must not be affected by the fact as to who is who. Real culprits must be nabbed and the innocent must be spared.

Force deployed on the ground zero must be very decisive. Quick and prudent decisions on the ground can avert looming crisis. The commanders on the ground must follow three Cs, i.e. Command, Control and Communication. These three Cs if used effectively, can control any unruly mob.

Riot Control refers to the measures used by police, military or other security forces to control, disperse, and arrest persons who are involved in a riot, demonstration or protest. If a riot is spontaneous and irrational, actions which cause people to stop thinking for a moment then loud noises or issuing instructions in a calm tone can be enough to stop it. However, these methods usually fail when there is severe anger with a legitimate cause, or the riot was planned or organized. Law enforcement officers or military personnel have long used less lethal weapons such as batons and whips to disperse crowds and detain rioters. Since the 1980s, riot control officers have also used teargas, pepper spray, rubber bullets, and shock batons. In some cases, riot squads may also use Long Range Acoustic Devices, water cannons, armoured fighting vehicles, surveillance team, police, or mounted police on horses. Officers performing riot control typically wear protective equipment such as riot helmets, face visors, body armour (vests, neck protectors, knee pads, etc.), gas masks and riot shields.

Riot has different dimensions which in some way or another creates a divide in the society. History shows how much a society is affected by riot socially, politically and economically. The people who earn one square meal per day are the most affected lot of riot and riot like situation. In India the history of riot may be associated with the divide and rule policy of English rule. Morley-

Minto reform sowed the seeds of divide in society and it snowballed over the years. Subsequently the Govt. of India act 1919 and Ramsay McDonald award of 1932 have created a big rift in the society. The following years and year of Indian Independence have witnessed horrible blood bath. Millions of people died and millions of them became homeless.

In the early 1990s the country witnessed severe social and political crisis in the form of riots and riot like situation. Govt. of India felt the need of a force expert in controlling riots with secular credentials. Thus the RAF (Rapid Action Force) was born out of CRPF by converting its 10 units and placing them strategically across the country.

In last 27 years RAF has played a role of saviour in the country and its presence as blue troopers has earned respect and accolades in the society. Today it is not only communal violence that has forced the state governments to seek the service of the RAF but severe law and order crises also. Resultantly the RAF has become a reliable force but it is an overused and overworked force. Only fifteen battalions having strength of 1222 personnel each are catering to the need of the states.

The main objective of the RAF is to deal with riots and riot-like situations. Its services are also taken for crowd control and crowd management too. It is pertinent to mention that RAF will be seen in all the communally sensitive pockets during Dussehra, Deepavali, Ramnavmi, Id-ul-fitr, Id-ul-Ajha etc.

The RAF is normally deployed for control and containment of emergent situations. The duration of such period shall not exceed ten days unless explicitly and specifically concurred by Ministry of Home Affairs, Government of India due to extraordinary situation on the requisition of the affected states or union territories. In the absence of Ministry of Home Affairs' concurrence the force may be unilaterally withdrawn by the orders of Director General, Central Reserve Police Force.

RAF follows the principle of Zero response time. Zero response time is a specific time period in which RAF is required to leave its base and reach the riot affected area minus the journey period. This time limit is part of standard operating procedures of RAF. One company is always kept on call to move to the affected area.

The time limit for the movement of RAF Coy/Coys already on call within same station in own transport with equipment, stores and weapons immediately on receipt of orders is half an hour, and to move without stores is within 15 minutes. When the deployment is assigned in cities/areas other than the location of the coy, the coy should move within 2 hours.

The RAF unit is led by a Commandant and it has four companies. One company has two platoons. The company is commanded by an officer of the rank of Deputy Commandant and platoons are commanded by Assistant Commandant. One platoon has four teams and each team is commanded by an officer of the rank of Inspector. In one company there are eight teams and one team is purely of women and commanded by a woman of the rank of inspector.

The team is the smallest component to deal with the crisis. According to standard operating procedure of RAF the whole company is deployed in riot or riot like situation. The company cannot be split into platoons for deployment. It can be deployed in platoons only when it is deployed in district where the RAF unit Headquarter is located, that too the platoons remain at visual distance with each other for command and control.

The smallest functional unit in the force is a Riot Control Team which has three components namely Riot control element, Tear smoke Element and Fire Element, The Riot Control Team is under the command of an Inspector. It has been organised as an independent striking unit, capable of moving into action at short notice. A team consists of twenty-four personnel but the operational strength of the team is of fifteen personnel.

Each unit has two areas of responsibility. One is primary area of responsibility and the second is secondary area of responsibility. Each area of responsibility consists of communally sensitive districts. Why is RAF so successful in controlling riot or riot like situation? It is because of its structure, operating procedure, training and Famex, i.e. familiarisation exercise.

Familiarisation Exercise

While undertaking the familiarization exercise, the following should be ensured:-

1. To patrol the area of responsibility in Teams and familiarize with routes and alternative routes for various destinations and prepare a map/sketch thereof.
2. To conduct mock exercise as to :
    a. How to cordon riot affected areas,
    b. How to organize general search,
    c. To identify places where stop parties should be positioned to prevent infiltration of undesirable elements into riot-affected areas.
    d. To identify places where camps can be organized if people are to be evacuated from the riot affected areas.
3. To familiarize with locations of hospitals, dispensaries, Railway Stations, bus stands and airport etc.
4. To meet village/locality elders, other prominent persons and social workers.

The whole of India was divided into 10 major pockets from the point of view of communal sensitivity and all 10 RAF units have fixed area of responsibility when RAF units were raised. Now with the increase of five RAF battalions the country is divided into fifteen major pockets.

- To understand the area the platoons of RAF do the familiarization of the area.
- In a quarter a RAF unit has to cover 4 districts normally including a hypersensitive district.

It is important to mention here the districts which are communally sensitive are divided as hypersensitive and sensitive.

What is the modus operandi of RAF? RAF follows a set drill which is part of its standard operating procedure. It primarily uses the non lethal means to control the mob. The non-lethal means include tear smoke grenade, tear smoke munitions, cane, anti riot weapon and water cannon. Firing is the last resort; even then, it is done to only immobilise the rioter not to kill.

RAF has two specialised vehicles which are used to control the riot. The first is Varun, which is a water cannon and is used to spray water at very high speed. It immobilises the rioter for a few seconds but it does not hurt. It has three tanks. One has a capacity of ten thousand litres and the other two are of one thousand litres each. Bigger tank stores water and two smaller tanks store irritant and ink respectively.

The second specialised vehicle used by RAF is Vajra. Vajra has multi barrel launcher through which the long range and short range tear smoke munitions are fired to disperse the rioters. It is very effective when the rioters are in big numbers. The launcher is designed in a way that it fires both electric and non-electric shells.

The RAF follows specific drill to control the riots and riot like situation. The drill is devised taking the platoon into consideration.

Platoon Formations:

In dealing with larger mobs a platoon is a formidable unit of force. In operational maneuvers according to availability of space i.e. narrow or wide front and the need of the situation, a platoon adopts the following formations. A platoon has 4 teams. However to form up these formations 3 teams i.e. ¾ the strength of the platoon is sufficient. The fourth team available acts as a striking reserve.

1. **Platoon Wedge:** It is capable of covering a wide road, crossing or street of a metropolis where a mob has gathered. It is a strong and formidable formation with a lot of depth.
2. **Platoon Split Wedge:** In this formation the teams move in different directions. This is suitable to push back crowd from a street crossing or road junction in different directions. The elements of the teams form up with their respective teams.
3. **Extended Line:** All elements from up breadth-wise. This formation is useful when facing a mob on a very wide front like main thoroughfare of a metropolitan city or when a procession turns violent. The Commander has enough strength in depth.
4. **Extended Line One Deep:** Similar to the extended line but one riot control element will be positioned in depth in the centre; remaining elements will be as in the extended line formation. It is useful where, there are road dividers and the mob is on both sides of the road leading to a crossing or chowk. Commander has one riot control element and other elements in depth.
5. **Extended Line Two Deep:** On a wide front when the mob is not spread out this formation can be adopted keeping enough strength in reserve. In this, two riot control elements are in depth and only one in the front.

6. **Platoon Circular:** This is a defensive formation adopted in extreme emergency, wherein, the contingent runs the risk of being surrounded by rioters and attacked. It is held untill reinforcement arrive.

How do the RAF companies work in riot or riot like situation?

When ariot breaks out in a sensitive locality and the RAF is called upon to deal with the situation. On receipt of such an emergency call the RAF Control Room alerts the troops as laid down in the mobilization plan and the troops rush to the scene of occurrence at lightning speed.

The contingent arrives at the scene with wailing sirens and stops at about 50 meters distance from the actual rioting. The vehicles halt 50 paces apart from each other for unhampered debussing and forming up. As soon as the vehicle stops debussing commences swiftly and troops adopt the formation ordered by the Commander. Simultaneously, the commander decides the action to be taken and moves directly into action without losing time.

In any such action, the contingent may face following eventualities:-

a) Two groups fighting each other violently.

b) Arson, looting and stabbing in progress.

In the event of the first eventuality, soon after adopting suitable formation on arrival at the scene, the Commander orders the gas element to come forward and use stun shell, stun grenade, sting ball or dye marker grenade depending upon the distance from the scene of rioting. All the said munitions are suitable for gaining psychological advantage and temporary disengagement of the warring groups.

These munitions when fired or thrown cause a stunning bang. The stun shell and stun grenade are different only in their method of launching, whereas a stun shell is fired through a gas gun, the stun grenade is hand thrown. The range is also different. The grenade is effective at 25 to 30 meters whereas, a shell is effective up to 100 meters. A dye marker bursts with a bang at the same time sprays coloured dye which makes identification of rioters easy after the riot, as the dye cannot be easily washed off. The sting ball when thrown bursts with a loud bang and spread small plastic balls in all directions causing a stinging sensation at the point of contact.

The Commander may choose any of these and use it against the rioters. He keeps the riot control elements ready to move forward to take advantage of the stunning impact on the rioters to chase them away.

Soon after gaining this advantage, the Commander spreads out his teams to clear the adjoining streets and by-lanes to prevent small groups from indulging in violence. In accordance with dictates of the situation, the Commander orders the use of rubber bullets against the rioters. In the event of direct fire at the contingent from a rooftop or building, the Commander employs fire power only after locating and fixing the target. In all such cases, the firing is specifically directed at such targets to neutralize them.

Use of fire power is not recommended as it may damage the image of the force and adversely affect its public acceptability. Simultaneously, he orders his reserve team and rescue & relief elements to evacuate the injured and render first-aid. The fire-fighting elements douse fires if any, rescue people trapped in burning buildings and salvage properties.

Before the rescue and relief element goes into action the firing element of the reserve team takes all-round protective position. Photographic evidence is prepared of all events. The events as they transpired during the riot control action are diarized progressively and chronologically supported by photographic or video evidence.

The RAF Control Room is kept posted of the developments. The diarized report, photographic/video evidence and other documents & connected papers are handed over to the RAF Control Room for records.

RAF has been the most reliable force of India to deal with the riot or riot like situation. It has the distinction of training armed forces from different states like Bihar military police, Rajasthan Armed Constabulary etc.

Due to its impartial and secular nature, the RAF units are the first choice of states during mob violence. History bears witness to the remarkable achievements of RAF during mob violence or riot like situation. Many riots which seemed uncontrollable were reined by RAF in India. It would be pertinent to mention a few of them as follows.

- Handling of post Babri Mosque situation
- Controlling of Aligarh Riot in 2006
- Controlling of Farmer's Movement in 2010 in Tappal
- Controlling of Jaat Movement in 2011 in UP
- Controlling of Jaat Movement in 2012 in Haryana
- Controlling of Major Riot in Kosi Kala, Mathura in 2012
- Controlling of Muzaffarnagar and Meerut riot in 2013

RAF has become the need of the day due to the growing discontent in society. Every now and then one can witness protest or demonstration for one reason or other. India needs to have ten more RAF units to complement existing units as these are not sufficient to cater to the needs of states sometimes.

***

4 Multi-Tasking K9s: Sentinels of Internal Security of the Nation

Sh. Mahendra M Hegde
Second-in-Command
42 BN, CRPF

Canis lupus familiaris.

For ages, dogs (Canis lupus familiaris) have been serving humankind with unflinching loyalty. In fact, dogs were the first animals to be domesticated by humans, even before civilization took root. Dogs, or canines, have been used for myriad purposes by humans. From accompanying Stone Age humans in hunting to helping the medical practitioners in the 21st century in detection of cancer, COVID-19 and other life-threatening diseases and guiding the blind the canines have come a very long way. They are the time-tested, trustworthy companions of the humans.

Despite phenomenal and exponential growth in the field of science and technology, nothing has been invented so far which can be termed as a perfect substitute for service dogs. Dogs can smell 100,000 times better than humans; they can hear four times better than their masters and can see a small object moving kilometers away. Even it is said that they can see the earth's magnetic field!

Wolves from the wild became dogs living with the humans and started helping their masters in hunting the wild animals, guarding the tribe, cleaning the left-out foods and in many other ways. Realizing the potential of dogs' ability of hunting and guarding the humans started using them in battles to scare and attack the enemies. With the passage of time, aggressive breeds that were purposefully bred became an integral part of armies. It was only during World War-I that modern use of dogs in warfare was documented properly. During both the World Wars, trained dogs of various breeds were used on a very large scale by many countries. Military and police forces of almost every country train and utilize Service K9s in their sphere of duties. In India too, trained K9s were used by the police even before Independence.

However, till the end of the 20th century, "one dog, one trade" was the norm. K9s were trained either in sniffing or tracking. This was truer in the Indian scenario. And the number of breeds used too was very few. Moreover, sadly, very few people were aware of the concept of proper training and utilisation of service K9s in India. Compulsion –based or punishment-based training was widely used. Reward-based training, which is the best method to train the K9s, was unheard of! And there was no word about the concept of "Multi-tasking K9s" in India.

CRPF: the pioneer in introducing the Multi-tasking K9s in India

Central Reserve Police Force (CRPF) has been entrusted with the mandate of maintaining the Internal Security of the country. Though being the largest Central Armed Police Force (CAPF) and being the nodal agency in maintaining the internal security of the country, one crucial element, K9s, was missing for long. Later, there were a few hundred K9s which were trained by the sister agencies in a single trade. But these K9s were not found suitable to meet the force's requirement to face the emerging challenges. Considering the alarming rise in Left Wing Extremism (LWE) in many states of the country the Force decided to augment K9 element on a large scale. The Dog Breeding and Training School (DBTS), CRPF, was established on the outskirts of Bengaluru in 2011. In fact it is the youngest K9 school among all the Central Forces in India. Instead of following the conventional K9 training methodology, **Operant Conditioning** method was adopted. As breeds like the Labrador or German Shepherd Dogs were found unsuitable for the nature of duties the Force was undertaking, CRPF chose Belgian Shepherd Malinois. Along with many other pioneering steps taken by the force while establishing the K9 School, training and deploying the Multitasking K9s was a game changer.

What are Multi-Tasking K9s?

Though DBTS, CRPF, was the youngest K9 School among the CAPFs, it started functioning with many 'firsts' in India. Belgian Shepherd Malinois was introduced on a large scale and these K9s were trained in Multi-tasking, trained in more than one trades (unlike the conventional system where a dog was trained in a single trade only). Multi-tasking K9s were the need of the hour for CRPF which was intensely engaged in tackling Left Wing Extremism (LWE) problems in many parts of the country.

CRPF, at DBTS, trains its K9s in multiple streams. Most of the K9s are trained in Infantry Patrolling, Explosive Detection and Assault. Some K9s are trained in Tracking, Explosive Detection and Assault. As per need, a few K9s are also trained in Guarding, Explosive Detection and Assault. However, a K9 cannot be trained and utilized in both infantry patrolling and Tracking. In Infantry patrolling the K9 is trained in looking for air scent whereas a Tracker K9 is trained or conditioned to follow ground scent. Also, as per the requirement, a multitasking K9 is trained either in Explosive Detection or Narcotics Detection or any other detection work (on a pilot project basis, a K9 was trained in Cell phone Detection also).

Utility

To effectively address many kinds of law-and-order problems or tackling anti-national and anti-social elements, the multi-tasking K9s can be most effective and trusted 'force-multipliers'. As per the requirement of any Security Force or law enforcement agency, a K9 can be trained in desired trades/disciplines. CRPF is already using multi-tasking K9s in various operational theatres. Considering challenges being faced by the security forces and law enforcement agencies in the spheres of internal security of the country K9s can be trained in the following types of combinations of trades.

a) **Infantry Patrolling(IP) + Explosive Detection + Assault:** K9s trained in these trades are of great help in the LWE affected areas. K9s can give indication about the enemy presence or enemy ambushes from a distance and can alert the troops. As the K9s are trained in assault they can be sent to attack the enemies when the exchange of fire occurs. A K9 rushing towards the enemy will distract them and give valuable time to the troops to respond. Same K9 can save the troops by detecting the buried or hidden IEDs planted by naxals. K9s of CRPF even have alerted the troops about the presence of pits with spikes many times.

b) **Tracking + Explosive Detection + Assault:** Such K9s are not only effective in the fight against the LWE elements but are also very useful in the fight against the terrorists. When the naxals or the terrorists/militants run away after exchange of fire or committing killings of civilians or any other kind of anti-national or anti-social activity, a K9 trained in the above trades can be deployed to track down the escaped or fleeing ANEs. Once tracked, the same K9 may be used to attack them and immobilized them before the troops apprehend them. Such K9s are most useful for the law enforcement agencies in apprehending the criminals. Police forces of western countries widely use such K9s in urban patrolling.

One more effective utilization of such K9s is in Border Guarding. Once the security forces notice any kind of breach along the border they can engage such multitasking K9s in tracking down the infiltrators and overpower them.

c) **Guarding + Explosive Detection + Assault :** K9s trained in these trades can be utilized for patrolling vital installations, security camps, airport perimeters, high-security jails, VIP/VVIP locations etc. These K9s are useful in apprehending trespassers, conducting vehicle searches, frisking and sentry duty. The DBTS, CRPF, had even further trained such K9s in Drone Detection successfully.

d) **Tracking + Cell-phone Detection + Assault:** DBTS, CRPF, has trained a K9 in cell- phone

detection very successfully. A K9 trained in cell-phone detection, contraband- item detection can be utilized in the high security jails to find out any unauthorised mobile or any other electronic gadgets possessed by the inmates or visitors. When trained in tracking the same K9 can identify the inmate who might have used a recovered cell phone. Trained in assault the K9 can also be utilized for perimeter patrolling, escorting prisoners, overpowering the unruly inmate groups and access control.

e) **Tracking + Narcotics Detection + Assault:** Such K9s can be utilized again in the high security jails to check the use of narcotics by the inmates, in border guarding, frisking in airports, airport cargo, seaports, railways etc. There are plenty of instances in the Western countries where such multi tasking K9s have been very successful in detecting very huge quantities of drugs/narcotics and also helping the law enforcement agencies in apprehending the culprits. These K9s are very useful for identifying and apprehending the drug peddlers.

f) **Infantry Patrolling (Scout) + Wildlife Detection + Assault:** 'The prolific growth of wildlife smuggling makes it the fourth largest criminal enterprise globally after drug, firearm and human trafficking'. Protecting the wildlife from the criminals has become an urgent need of the hour. Few countries, especially in Africa, have successfully inducted trained Wildlife Detection K9s in this endeavor of wildlife protection. In India too there have been attempts to utilize such K9s for wildlife protection. All of them are Detection Dogs. However, There is a lot to be done yet. A K9 trained in Wildlife detection can detect wildlife related items like bones, teeth, nails, skins etc. When trained additionally in Infantry Patrolling skills the same K9 can give early warning about the presence of poachers in the forest. If the need arises the K9, trained in assault too, can chase and assault the poachers or criminals making it easier for the forest officials apprehending them. Such K9s can be effectively used in Wildlife sanctuaries, national parks, airports, seaports, railway stations etc.

g) **Tracking + Wildlife Detection + Assault:** Again, used in wildlife protection, these dogs can track the poachers from the site of poaching. As most of the time poaching cases are detected or reported after a considerable lapse of time such K9s will lead the forest officials in the direction of where the poachers escaped. Moreover, such K9s act as formidable deterrent for the poaching-related activities. Also, such K9s that are trained in Assault may be very useful in protecting the forest guards. Generally, forest guards, who are inadequately armed, get attacked by the poachers who come with automatic weapons.

h) **Special Task K9s:** K9s, meticulously selected for their temperament, intelligence, agility and high trainability, can be trained in multiple skills like Room Intervention, Assault, Explosive Detection, Slithering, retrieving things, dropping explosives, searching for explosives at a laser-pointed area or vehicle or attacking a laser-beam-pointed suspect/terrorist/kidnapper! An apprehended suspect, terrorist or kidnapper may be

escorted, guarded by the K9. All these things can be done by a single K9. Such K9s can be used not only for Room/Building Intervention but for Vehicle Intervention too. Such Special Task K9s can be very effective in the Kashmir valley and for Urban Patrolling. DBTS has trained many such K9s.

Advantages of Multi-tasking K9s

In either the military or in police a Service K9 trained in multiple trades can prove to be more effective compared to a K9 trained in just a single trade. This has been proved by hundreds of multi-tasking K9s trained and deployed by the CRPF.

a) **Harnessing true potential of the K9:** The most advantageous use of a Multi-tasking K9 is unleashing the true potential of a K9 which it has got through genetics. Canines not just have the ability to sniff, they can protect and guard too. Unfortunately, for long, in India, K9s were used only either to detect explosive/narcotics or track the criminals. K9s can indicate the presence of an enemy from a distance (Infantry Patrolling). They can be used for sentry duties. The aggression or prey drive present in a K9 must be harnessed for these trades. Now, with the CRPF using the K9s for multiple purposes, many other organisations have slowly started utilizing the K9s in unconventional trades, training them in multi-tasking. Contrary to common belief, training the K9s in multitasking substantially increases their capabilities across the disciplines in which they are trained.

b) **More economical:** Training a K9 in multi-tasking definitely saves significant resources. If a K9 can do more than one or two tasks, that will save the money to be spent in terms of procuring puppies, feeding, training, veterinary care, transportation, kenneling, handlers' salaries etc.

c) **Operational effectiveness:** In most of the Operations in the field it is not possible to take multiple K9s for each single task. That may adversely affect the operational efficiency of the whole team. In such situations a K9 which can do multitasking will prove as an effective "force-multiplier". Such K9s will also add to increasing the success rate.

d) **Very effective deterrence:** Normally a multi-tasking K9 is trained in assault also. Such K9s with multiple skills become an effective deterrence factor in maintaining Law and Order for law enforcement agencies or for conducting various kinds of operations by the Security Forces (SFs) against the anti-national elements.

Other than the above there are other benefits

too. It will be easier to put such K9s for rotational training and certify them. In the operational field, situations and requirements may change suddenly. In such scenarios it will not be possible to deploy a dog with a different type of skill. So, a K9 which is already present in the Ops can be pressed into service to address the new challenge. For example, a multitasking K9, trained in Explosive Detection (ED), Tracking and Assault is generally taken along with the troops in Anti-Naxal Operations for checking Improvised Explosive Devices (IEDs). If they detect one and the explosive is freshly laid then the same K9 can be used to track and follow the path used by the naxal who planted the same. Or the K9 can be used to track the fleeing naxals/militia. Not just that, the same K9, trained in assault, can be commanded to assault the fleeing naxals/militia/terrorists and help the troops to apprehend them.

A K9 trained in Infantry Patrolling can be utilized as Sentry when the troops halt in the jungles. Such K9s will silently alert the handler if any enemy, civilians or animals come near to the place where the troops are taking rest. Such K9s can be effectively utilized in camp security duties too.

They can be utilized in the sentry morchas, patrolling and guarding the gates and access points.

Suitable Breeds

There is no other animal species on the earth as unique as canines/dogs. 'There are approximately 400 separate breeds of purebred dogs worldwide'. Hundreds of breeds were developed as per the wishes and needs of the humans. Selective breeding and culling went on for centuries to get a suitable breed to fit a specific requirement. All breeds are not fit to become service K9s. And every breed in the category of service dog is not fit for training in multi-tasking. There are a few time-tested K9 breeds which are found most suitable to be trained and deployed for multi-tasking. Among them Belgian Shepherd Malinois (BSM) stands tall. They are highly aggressive, full of energy, agile, highly trainable, have highest prey drive, adaptable for varied weather conditions and are the most intelligent. Dutch Shepherd Dogs and German Shepherd Dogs (working line) are the other two breeds which are highly suitable for multi-tasking.

One more important aspect is selection of puppies possessing the right temperament. Every

line of a breed may not be suitable for police or military work. Hence there is a need to go for a right line of that breed. And, further, all puppies of a mother (Dam) may not fit into our requirement. Hence, again, proper puppy selection is the key to success of the training.

Training

What about the training period it takes to train a multitasking K9? Obviously, it is more than what it takes to train a dog in single trade. Normally it is of 40 weeks. Is that a downside of training multitasking K9s? No, absolutely not. The puppies are weaned away from the mother and their foundation training starts from the fifth week of their age. Puppy Foundation Training (PFT) is done for 08 weeks. From their 13th week of age their formal training starts. So, when they complete 40 weeks of training in multitasking and are ready for final assessment tests they are around 12 to 13 months old. The K9s trained in single trade, in conventional method of training, also get passed out when they are around 12 -14 months of age as they generally start get trained from their sixth month of age. One more very significant aspect of training methodology adopted in DBTS, CRPF, is that there are no exclusive sessions for Obedience training. Generally, in conventional method, there is a three-month period of exclusive Obedience training before the K9 is put into trade related training. However this exclusive Obedience training method makes the K9 either submissive or overaggressive at times. It kills the "curious puppy" in the dog. Handlers may also become more obsessive with obedience training which adversely affects the K9's natural behaviour. While training multitasking K9s, obedience training is never emphasized. Building a strong bonding between the handlers and the K9 is given more thrust and that ensures making an unbeatable K9 Team. Bonding, trust, mutual loyalty and affection bring the perfect obedience in the K9 without adversely affecting its natural behaviour or drives. This method also helps in bring the best performance out of a Multitasking K9. Not following this path will only lead to failure in training as well as during deployment.

The best part of training a multitasking K9 is that it emphasizes in harnessing the natural drives present in it and channelize it so that the K9 be trained in the desired trades. The well trained Decoys play a very crucial role in it. The natural drives are opened, harnessed, developed and channelized so that the K9 is trained in a positive environment. It also ensures that our most trusted companion is never abused or mistreated. The concept of animal welfare is also complied.

Decoys

The dogs come with certain drives inbuilt in their genetics. These drives are the same which made them survive in the wild as wolves before they got domesticated. They have got mainly two kinds of drives–Primary and Secondary. Oxygen, water, food, sex and pain avoidance make up the Primary drives. Play,

prey, pack and defense drives made the Secondary drives. Though being domesticated by humans for many thousands of years, for mutual benefit, those drives are still there more or less. All bundled up in their DNA. While training a Service Dog these drives are tapped to get the most out of them. The key to tap, simulate, channelize and balance these drives is none other than a Decoy. Basically a decoy is someone who acts as a threat to the K9 or to its 'pack'. He threatens the K9, he agitates and he challenges and takes the K9's bite on his body. Though he wears bite suits or sleeves, dog bites involve a lot of hard work and pain to him. There are two kinds of decoys. Trial decoy and training decoy. Thus well trained and experienced decoys play a very crucial role in training the Multi-tasking K9s right from the puppy selection, puppy foundation training to Certification at the end of the training. They are also crucial in behaviour modification training wherever necessary.

Way Ahead

There is no limit to how the K9s can be used in multiple roles. It all depends on the emerging security challenges and the ability to train the Multitasking K9s. There is an urgent need to accept that we, in India, need to do a lot when it comes to training and managing the K9 Teams to address the emerging challenges in the arena of Internal Security. Modern training methodology which is completely based on Operant Conditioning method, Positive Reinforcement, needs to be adopted without any delay. Trainers need to be reoriented for Multitasking training methods.

***

5 Understanding the IED Threat Picture and Comprehensive C-IED policy: Need of the Hour

Sh. D Bagade, DC,
IIM Pune

Understanding the Threat Picture

- *The criticality of understanding in support of any coherent C-IED enterprise is both cross-cutting and multi-dimensional.*
- *Understanding refers to the need to comprehend inter alia:*
- *Why and how IEDs are used?*
- *Use of appropriate terminology;*
- *What a national C-IED enterprise entails;*
- *Maintaining an accurate IED threat picture for effective C-IED decision making;*
- *Importance of exploitation in maintaining an accurate IED threat picture;*
- *Timely information sharing between C-IED stakeholders;*
- *Appropriate classification of C-IED information.*

Understanding Why and How IEDs are Used?

Understanding why IEDs are used refers to an appreciation of the root causes which lead to the insecurity and instability that facilitate their use, the baseline factors contributing to their use. Ultimately, understanding why IEDs are in use is key to successful efforts to counter them through a coherent, coordinated, and complementary whole of system approach.

IED threat actors achieve target effects by the ways they are employed and the modus operandi of their organisation. Being versatile, IEDs lend themselves to a wide array of employment methods. An understanding of IED employment methods in use is necessary to inform what must be implemented to counter them and support optimised risk mitigation.

IED employment methods can be considered on the strategic, operational, and tactical levels.

At the strategic level, IEDs are a tactical asymmetric weapon system with strategic impact, a weapon of irregular or hybrid warfare supporting the intention to destroy an opponent's political will to fight.

At an operational level examining how IEDs are employed involves an examination of the IED system which considers the network, processes and material involved in IED attacks and relation to their modus operandi, strengths, weaknesses, opportunities, constraints and limitations.

At the tactical level, IED emplacement and their tactical use the way IED attacks are

planned and conducted along with their intent (purpose of the device). The methods of employment of IEDs vary depending on the intended effect that an IED threat actor wants to achieve along with the constraints they face due to the C-IED efforts implemented. There are no fixed templates for IED tactics due to their versatility coupled with their complex, dynamic and evolving nature. This combines to make the method of employment of IEDs extremely wide ranging and often unique to a given area.

However, recurrent commonalities in IED tactics can develop as threat actors attempt to achieve the same tactical intent in a given area of operation. Such common IED tactics can be identified through appropriate analysis allowing effective C-IED measures to be developed. It is important that reliable and systematic methods to track such tactical patterns are developed and maintained as part of the system supporting the IED threat picture. As effective IED countermeasures are implemented, IED threat actors adapt their methods of employment to circumvent the countermeasures introduced.

This often becomes the action-reaction counteraction cycle between IED threat actors and C-IED stakeholders, which is the reason why maintaining an updated IED threat picture is essential requiring on-going timely information sharing between all C-IED stakeholders.

Comprehensive C-IED Policy Need of Hour

Strategy may be considered as a general plan or set of plans to achieve a goal, especially over a long period as part of policy. It is the bridge that connects policy with military power. For the need of SFs, the concept of strategy exceeds what may be considered classical military strategy; It reflects what India needs to complement wider security strategies as well as the national security architecture and interests. A comprehensive national strategy involves more elements than military power to effectively support C-IED efforts. Presently, India does not have any comprehensive National Counter-IED Strategy encompassing the four pillars of Counter-IED operations.

The US DOD definition of national security strategy better fits the needs. It explains that its purpose is for developing, applying, and coordinating the instruments of national power to achieve objectives that contribute to national security. It is not simply focused on the military and reflects the need for a strategic whole of government approach to C-IED. It is proposed that an optimally effective strategic approach to C-IED requires all elements of statecraft. A whole of government approach to C-IED needs to encompass the instruments of national power involving military; information; diplomacy; finance; intelligence; economics; legal; development along with law enforcement, regulatory instruments and civil society organisations.

Fragile, fragmented, or failed regions, states or localities are vulnerable to IED use, with their impact most acute in terms of their political, economic and social destabilising impacts. As such, the IED is likely to be a prevalent and enduring threat within such security landscapes for the foreseeable future.

C-IED Conceptual Evolution in Line with Emerging Threats

We could find what English dictionaries say about "improvise"; - "to make or do something using whatever is available, usually because you do not have what you really need" (Oxford Dictionary), "If you improvise, you make or do something using whatever you have or without having planned it in advance." (Collins Dictionary), "to make or fabricate out of what is conveniently on hand" (Merriam Webster).

The North Atlantic Treaty Organization (NATO) is officially defining an improvised explosive device (IED) as "a device placed or fabricated in an improvised manner incorporating destructive, lethal, noxious, pyrotechnic or incendiary chemicals and designed to destroy, incapacitate, harass or distract. (Note: It may incorporate military stores, but is normally devised from non-military components.)".

On the other hand, United States Armed Forces are defining an IED as "An improvised explosive device (IED) is a weapon that is fabricated or emplaced in an unconventional manner incorporating destructive, lethal, noxious, pyrotechnic, or incendiary chemicals designed to kill, destroy, incapacitate, harass, deny mobility, or distract".

Although may not be very updated, that definition is wider than expected, by including conventional military munitions whose fuzes have been manipulated to arm them by aligning the fire train (e.g. what a VOG-17 series grenade needs to be ready to detonate when dropped by a drone in Ukraine-Russia war).

If one considers that the "IED" concept could cause confusion, try to understand what "C-IED" is: "The collective efforts to defeat the IED system by attacking the networks, defeating the device, and preparing a force." Additionally, the term "C-IED" is often understood in a wrong or limited manner.

Pillars of Counter- IED Strategy. Source: JEDDO, USA

With a Defeat the Device (DtD) based on a reactive approach, mostly based on:

- BDD squads
- Explosive Ordnance Disposal teams (EOD)
- K9 Squads (Dogs)

It does not include Attack the Networks approach.

The typical understanding of C-IED is mostly based on analysis of databases of past IED events, defensive posture against generic enemy tactics-techniques and procedures, search and clearance tasks, and force protection measures at a low-tactical level. All of that is maybe forgetting that the main pillar of an effective C-IED approach should be the Attack the Networks one. It is not only the Allied doctrine which is reflecting that C-IED is much more than something

only based on Defeat the Device and Prepare the Force pillars.

The United Nations Institute for Disarmament Research (UNIDIR) states that the term C-IED (Counter-IED) "is used in its broadest possible context and includes all activities a State may undertake to prevent and mitigate the use of IEDs.

Components of Counter-IED capability are divided into two broad categories:

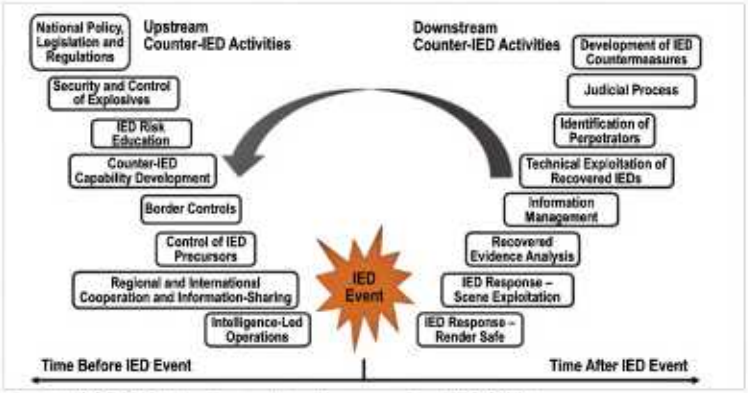


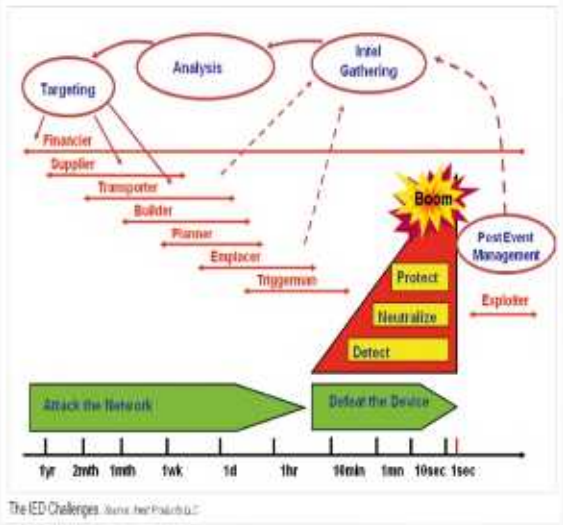
Figure 1. UNIDIR C-IED CMM upstream and downstream components. (UNIDIR 2020) [4]

1. Upstream components, which are focused on those activities aimed at deterring or preventing IED events from taking place,

2. Downstream components, which are associated with responding to a particular IED event or mitigating an IED event should it occur."

ATTACK THE NETWORK (AtN)

A firm and decisive endeavour, enables offensive operations against complex networks of adversaries, their financiers, leadership, ideology, communications, logistics, intelligence set up, IED makers, trainers and supporting infrastructure.



The IED Challenges

Intelligence Gathering

Collect various forms of intelligence from different agencies through user input to allow analysts to track specific entities. Put in place an all-source methodology designed to link specific insurgents to specific IED events, which over a time will provide better reliability on IED network signatures.

Establish special programs to vet and manage initiatives for rapid fielding of materiel and non-materiel technologies, giving full collection, exploitation and analytical (electronic intelligence, human intelligence, and communications intelligence) advantage to the security forces in attacking IED networks. Employ pattern analysis, an effective way to increase prediction accuracy on future events.

At the tactical level, gather intelligence on the location, tactical characterization and technical categorization of IEDs, the identities of people participating in the adversary network, the location and sources of their supplies and funding, and ways to influence people from participating in adversary network.

Building Relationships and Cooperation

Interagency partnership needs to be developed and strengthened among the security forces, intelligence organisations, law enforcement agencies, regulatory bodies, and chemical industry to identify networks responsible for the procurement, transportation, distribution and employment of IED components. Interagency partnerships need to be developed and strengthened among the security forces, intelligence organisations, law enforcement agencies, regulatory bodies, and chemical industry to identify networks responsible for the procurement, transportation, distribution and employment of IED components.

Initiate and genuinely implement civic action programmes to address the needs of the locals such as roads, electricity, medical aid, water supply, sanitation. Maintain frequent communications with the local power base and local community.

Use Information Operations to build trust and support with local populations and build effective relationships with the right people to gain the cooperation of the local power base. Deep understanding of local culture, building trust through positive actions and reducing collateral damage during C-IED operations would help in long-lasting and beneficial relationships with the local population.

Neutralising Hostile Networks

Effective and successful neutralisation of hostile networks entails:

- Providing physical security to the local population from intimidation and retribution by hostile elements.
- Minimising the drivers of instability.
- Disrupting adversary networks through information operations.
- Portraying the adversary as a threat to economic prosperity.
- Disrupting the easy supply of IED components.
- Focus on targeting critical vulnerabilities that will have the most impact on the networks affecting the area of operations.

References & Notes:

1. *UNIDIR Counter-IED Capability Maturity Model - https://unidir.org/publication/counter-ied-capability-maturity-model-and-self-assessment-tool/*
2. *Counter-IED Report AUTUMN 2023 - Published by Delta Business Media Limited.*
3. *US DoD. 2022. "Army C-IED Strategy." Washington DC: US DoD, February.*
4. *IED Exploitation activities will include collection and analysis of technical, tactical and forensic information. IED exploitation is an enabler that is required to attack /engage the network and defeat the device as it is a cross-cutting process that transcends all aspects of a whole-of-system C-IED enterprise.*
5. *Allied Joint Doctrine for Countering Improvised Explosive Devices C-IED.*
6. *C-IED enterprise is the collective term to describe all initiatives, activities, assistance, capabilities and capacities that contribute to the C-IED efforts and can involve anything which is intended to predict, discover / detect, prevent, protect against, respond to / neutralize, recover / exploit, mitigate against, or deter IED attacks.*
7. *The Joint Improvised Explosive Device Defeat Organization: DOD's Fight Against IEDs Today and Tomorrow – November 2008.*
8. *Abbreviations - IED (Improvised Explosive Device), CIED (Countering IED), tactics, techniques and procedures (TTPs), US DOD (United States Department of Defence)*

***

6 The Evolving Landscape of Challenges in the Cyber World

Sh. Shubham Gupta
Asstt. Comdt.
Ministry of Home Affairs

Introduction:

The rapid proliferation of technology and its integration into various aspects of our lives has brought forth a multitude of emerging challenges in the Cyber World. As our reliance on digital infrastructure grows, so does the complexity and scale of threats.

In this essay, we will delve into the evolving landscape of challenges in the cyber world, including cybercrime, data breaches, privacy concerns, emerging technologies, and geopolitical implications. As societies become increasingly reliant on technology, the threats posed by cybercrime, data breaches, privacy concerns, and emerging technologies demand our attention. We will explore these challenges and discuss their implications on individuals, organizations, and societies as a whole. By understanding these challenges in detail, we can better address them and strive for a safer and more secure digital environment.

1. **Cybercrime:** Cybercrime has become an increasingly lucrative and sophisticated industry. Cybercriminals employ various techniques, such as phishing, malware, ransomware, and social engineering, to target individuals, organizations, and governments. These attacks can result in financial losses, data breaches, and disruption of critical infrastructure. The rise of cryptocurrency has further facilitated cybercrime, providing anonymous and decentralized means for financial transactions. As cybercriminals constantly evolve their tactics, cybersecurity measures must adapt and strengthen to mitigate these threats effectively.
2. **Data Breaches:** Data breaches continue to plague organizations across all sectors, leading to significant consequences for individuals and businesses. Attackers exploit vulnerabilities in networks, software, and human factors to gain unauthorized access to sensitive information. The compromised data may include personally identifiable information (PII), financial records, and intellectual property. The consequences of data breaches encompass financial losses, reputational damage, and regulatory penalties. Stricter data protection regulations, robust encryption methods, and comprehensive incident response plans are vital to combat this challenge.
3. **Privacy Concerns:** With the increasing digitization of personal information, concerns regarding privacy have grown substantially. Social media platforms, online services, and IoT devices collect vast amounts of data, often without individuals' full awareness or consent. Governments and intelligence agencies also engage in surveillance programs,

raising questions about mass data collection and potential abuse. Striking a balance between technological advancement and preserving individual privacy rights requires transparent data practices, informed consent mechanisms, and enhanced user control over personal data.

4. **Emerging Technologies:** Emerging technologies, while offering numerous benefits, present their own set of challenges. Artificial Intelligence (AI) and Machine Learning (ML) systems raise ethical concerns, particularly in areas like bias, explainability, and accountability. The Internet of Things (IoT) introduces a vast network of interconnected devices, increasing the attack surface and potential for large-scale cyber-attacks. Blockchain technology, although heralded for its security, faces challenges in areas like scalability and regulatory frameworks. Proactive research, comprehensive risk assessments, and responsible implementation of emerging technologies are crucial to address these challenges effectively.
5. **Geopolitical Implications:** Cybersecurity challenges have transcended national borders and become intertwined with geopolitical dynamics. State-sponsored cyber espionage, sabotage, and disinformation campaigns pose threats to critical infrastructure and national security. These activities can lead to significant economic and political repercussions, eroding trust between nations. Establishing international norms, cooperation frameworks, and diplomatic efforts to address cyber threats are essential in mitigating geopolitical implications and fostering stability in the cyber world.

Cyber Offences and Legislations in the Indian Context

In India, cybercrime is governed by various piece of legislation that addresses different aspects of cyber offenses. The primary legislation related to cybercrime in India is the Information Technology Act, 2000 (IT Act) and its subsequent amendments. The IT Act provides a legal framework to deal with issues such as hacking, data theft, cyber terrorism, and other cyber offenses. Here are some key offenses and corresponding legislation related to cybercrime in India:

1. **Unauthorized Access and Hacking:** Section 43 of the IT Act deals with unauthorized access to computer systems, computer networks, or computer resources. It covers offenses such as hacking, introducing viruses, and damaging computer systems. Section 66 of the IT Act specifically addresses hacking and provides for punishment for hacking activities.
2. **Data Theft and Breach of Confidentiality:** Section 43A of the IT Act, along with the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011, focuses on the protection of sensitive personal data and information. It lays down obligations for organizations handling such data and provides for compensation in case of a data breach.
3. **Cyber Fraud and Identity Theft:** Section 66C of the IT Act deals with identity theft, which involves impersonating someone else with the intention of causing harm. It provides for punishment for offenses related to identity theft and misuse of electronic signatures,

passwords, or other unique identification features.

4. **Online Defamation:** Section 66A of the IT Act, which was struck down by the Supreme Court of India in 2015, dealt with online defamation. However, there are other provisions in the Indian Penal Code (IPC), such as Sections 499 and 500, which cover defamation offenses, including those committed online.
5. **Cyber Terrorism and Offenses against the State:** Section 66F of the IT Act addresses cyber terrorism offenses, including unauthorized access to critical information infrastructure and cyber warfare. These offenses are punishable with stringent penalties.
6. **Obscenity and Child Sexual Abuse Material:** Section 67 of the IT Act deals with the publication or transmission of obscene content over electronic platforms. Additionally, the Protection of Children from Sexual Offences (POCSO) Act, 2012, along with amendments, specifically addresses offenses related to child pornography and child sexual abuse material.
7. **Phishing and Online Financial Fraud:** Section 66D of the IT Act focuses on offenses related to cheating by impersonation using a computer resource. It covers phishing, online financial fraud, and other forms of cyber fraud targeting individuals or organizations.

It is worth noting that the IT Act is not the only legislation relevant to cybercrime in India. The Indian Penal Code (IPC) and the Code of Criminal Procedure (CrPC) also apply to various cyber offenses, including fraud, theft, and extortion. Additionally, there are specific guidelines, rules, and regulations issued by regulatory bodies such as the Reserve Bank of India (RBI) and the Telecom Regulatory Authority of India (TRAI) to address cybercrime-related issues in their respective domains. It is essential for individuals, organizations, and law enforcement agencies to stay updated with the evolving legislative landscape and collaborate effectively to combat cybercrime in India.

The Detrimental Potential of Cybercrime: Harm to Society and Individuals

Introduction: In the digital age, the potential of cybercrime to harm society and individuals has grown exponentially. The interconnectedness and dependence on technology have created new opportunities for malicious actors to exploit vulnerabilities and wreak havoc. Cybercrime encompasses a wide range of offenses, including hacking, identity theft, fraud, and data breaches. This essay explores the detrimental potential of cybercrime and the significant harm it can inflict on both society and individuals.

1. **Societal Impact:**
   a) **Economic Consequences:** Cybercrime causes substantial financial losses to individuals, businesses, and governments. The costs of investigating and mitigating cyber attacks, restoring systems, and compensating victims can be staggering. These financial burdens can hinder economic growth, disrupt industries, and result in job losses.
   b) **Critical Infrastructure Disruption:** Malicious actors targeting critical infrastructure, such as power grids, transportation systems, and healthcare facilities, can cause

widespread disruptions and pose threats to public safety. The consequences can range from inconvenience to potential loss of life, highlighting the significance of protecting critical systems from cyber threats.

c) **Erosion of Trust:** Cybercrime erodes trust in digital systems and undermines confidence in online transactions. When individuals fear becoming victims of cybercrime, they may hesitate to engage in e-commerce, online banking, or even sharing personal information, impeding the growth of the digital economy.

2. Individual Consequences:

a) **Financial Losses:** Cybercrime can lead to significant financial losses for individuals. Fraudulent activities, such as phishing, online scams, and identity theft, can result in stolen funds, compromised credit scores, and ruined financial stability. The impact on individuals' livelihoods and well-being can be severe.

b) **Privacy Invasion:** Cybercrime invades individuals' privacy by unauthorized access to personal information. This intrusion can have emotional and psychological repercussions, leaving individuals feeling violated and vulnerable. Personal data breaches can expose intimate details, leading to reputational damage and potential social stigmatization.

c) **Psychological and Emotional Impact:** Cybercrime victims often suffer from stress, anxiety, and a loss of confidence due to the violation of their digital lives. The emotional toll can be long-lasting, affecting relationships, personal well- being, and overall quality of life.

3. Social Consequences:

a) **Spread of Disinformation:** Cybercrime enables the dissemination of disinformation and fake news, leading to social unrest, polarization, and erosion of democratic values. Malicious actors exploit social media platforms and other online channels to manipulate public opinion, creating divisions within societies.

b) **Cyberbullying and Harassment:** The digital realm has provided a platform for cyberbullying, harassment, and online abuse. Individuals, particularly vulnerable groups such as children and adolescents, face threats to their emotional and mental well-being. The anonymity of the internet can embolden perpetrators, making it challenging to address and combat such issues effectively.

c) **National Security Threats:** Cybercrime extends beyond individual harm, posing significant threats to national security. State-sponsored cyber espionage, sabotage, and attacks on critical infrastructure can undermine a nation's defense capabilities, compromise sensitive information, and create geopolitical tensions.

Prevention and Mitigation of Cybercrime in India

Cybercrime poses a significant threat to individuals, organizations, and the overall security of the

digital ecosystem in India. As technology advances, so does the sophistication of cybercriminals, necessitating robust prevention and mitigation strategies. In this essay, we will explore the measures taken in India to prevent and mitigate cybercrime, along with case studies that highlight successful outcomes and challenges faced. By examining these initiatives, we can gain insights into effective strategies and the importance of collaboration in combating cyber threats.

1. **Strengthening Legislative Frameworks:** India has enacted comprehensive legislation to address cybercrime, primarily through the Information Technology (Amendment) Act, 2008. This amendment expanded the legal provisions related to cybercrime, covering offenses such as hacking, identity theft, data breaches, and online fraud. The introduction of specific sections within the Indian Penal Code (IPC) and the Code of Criminal Procedure (CrPC) has helped in prosecuting cybercriminals effectively.

   Case Study: The Shifu Banking Trojan Operation In 2015, the Shifu banking Trojan targeted Indian banks, leading to financial losses and compromised customer data. Indian law enforcement agencies collaborated with international partners to investigate and dismantle the cybercriminal network. The case highlighted the importance of robust legislation, cross-border cooperation, and intelligence sharing in combating sophisticated cyber threats.

2. **Capacity Building and Skill Development:** To effectively combat cybercrime, India has focused on enhancing cybersecurity skills and building the capacity of law enforcement agencies. Initiatives such as the Cyber Crime Prevention Against Women and Children (CCPWC) program and the Cyber Crime Awareness Program (CCAP) have been launched to raise awareness, educate citizens, and train law enforcement personnel on cybercrime investigation techniques.

   Case Study: The Navi Mumbai Cyber Lab

   The Navi Mumbai Police established a dedicated Cyber Lab to tackle cybercrime effectively. The lab conducts training programs for police officers, prosecutors, and other stakeholders. Its emphasis on skill development and practical training has improved the cybercrime investigation capabilities of the police force, resulting in successful arrests and prosecutions.

3. **Public-Private Partnerships:** Recognizing the need for collaboration between the government, industry, and civil society, India has fostered public-private partnerships to combat cybercrime. Collaborative initiatives involve information sharing, joint awareness campaigns, and sharing best practices for cybersecurity.

   Case Study: The Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center) The Indian Computer Emergency Response Team (CERT-In) launched the Cyber Swachhta Kendra to provide free tools, antivirus software, and cybersecurity resources to citizens. The initiative involves collaboration with leading cybersecurity companies and internet service providers. By working together, they have successfully identified and neutralized botnets and other malware, protecting users from cyber threats.

4. **International Cooperation:** Cybercrime knows no borders, necessitating international cooperation to address global cyber threats effectively. India has been actively engaged in international forums, sharing information, best practices, and collaborating with other countries in investigating and prosecuting cybercriminals.

   Case Study: The DarkMarket Operation

   In a collaborative effort between Indian and international law enforcement agencies, the DarkMarket online marketplace was taken down in 2021. The operation involved coordinated actions across multiple countries, resulting in the arrest of several individuals involved in the illicit marketplace. This case demonstrated the significance of international cooperation and joint efforts to combat transnational cybercrime.

Besides these, there are some more examples of cyber-crime and its implications in India:

1. **Ola and Uber Phishing Scam:** In 2017, a phishing scam targeted users of popular ride-hailing services, Ola and Uber. Fake messages were sent to users, tricking them into revealing their personal and financial information. The stolen data was then misused for various fraudulent activities, including unauthorized transactions.
2. **Cosmos Bank Cyber Heist:** In 2018, Cosmos Bank, a prominent Indian cooperative bank, fell victim to a cyber heist. Hackers used a malware attack to gain unauthorized access to the bank's systems and executed fraudulent transactions totaling approximately Rs. 94 crore (around $13.5 million). The attack involved several simultaneous ATM withdrawals across multiple countries.
3. **Aadhaar Data Breach:** In 2018, concerns were raised regarding the security of India's biometric identity system, Aadhaar. Several instances of data breaches and unauthorized access to Aadhaar information were reported, highlighting vulnerabilities in the system and raising concerns about the privacy and security of citizens' personal data.
4. **Wannacry Ransomware Attack:** In 2017, the global Wannacry ransomware attack affected organizations worldwide, including some in India. The ransomware infected computers, encrypted data, and demanded a ransom payment in Bitcoin to restore access. Some Indian organizations, including government agencies and private companies, were impacted by this widespread cyber attack.

Conclusion:-

The challenges in the cyber world are continuously evolving, necessitating a comprehensive and proactive approach. Cybercrime, data breaches, privacy concerns, emerging technologies, and geopolitical implications demand collective efforts from individuals, organizations, and governments. Strengthening cybersecurity measures, enacting robust data protection laws, fostering responsible technological innovation and international collaboration are critical steps toward mitigating these challenges. By investing in cybersecurity education, research, and infrastructure, we can build a resilient and secure cyber world for future generations.

The potential of cybercrime to harm both society and individuals cannot be overstated. Its financial, societal, and psychological impacts are far-reaching and require immediate attention and robust countermeasures. Governments, law enforcement agencies, businesses, and individuals must collaborate to develop comprehensive cybersecurity strategies, raise awareness, enhance digital literacy, and invest in cutting-edge technologies to mitigate cyber threats effectively. Furthermore, fostering international cooperation to combat cybercrime across borders is crucial, as cybercriminals operate in a global and interconnected environment. By addressing the potential harm of cybercrime head-on, we can strive for a safer digital world that fosters trust, innovation, and the well-being of individuals and society as a whole.

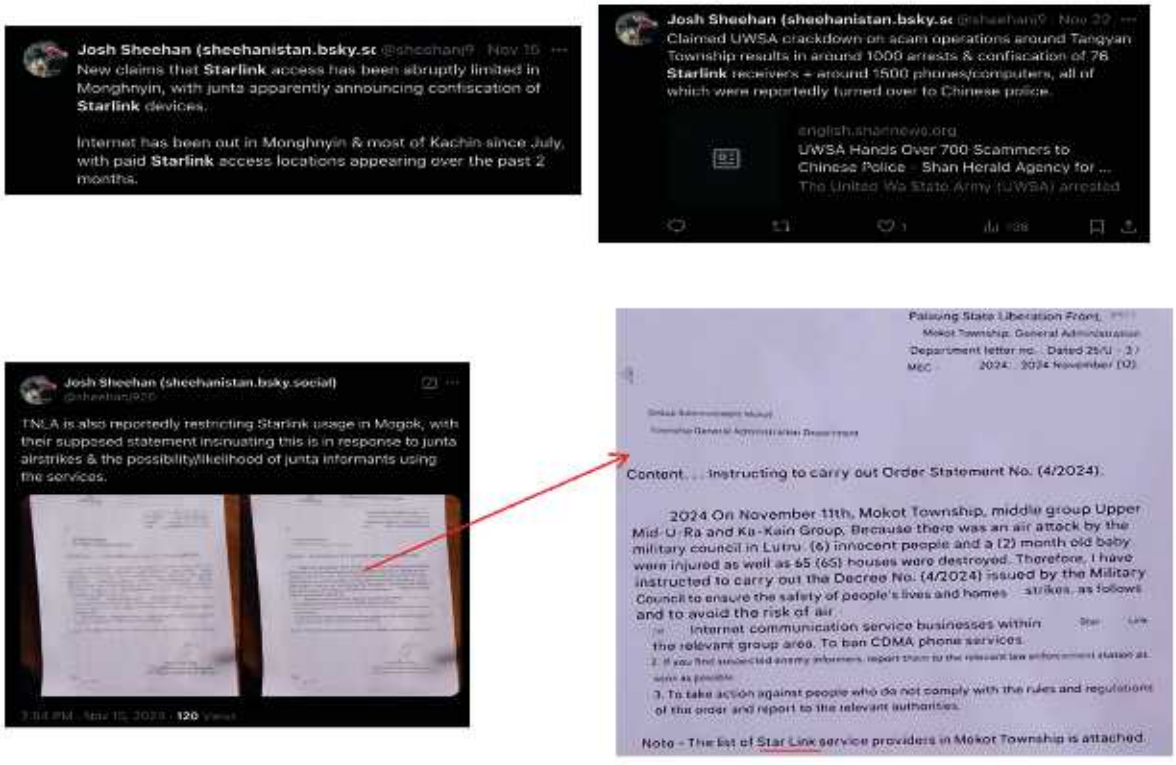
***

7 Digital Connectivity and Emerging Threats in India

Sh. Azimul Haque
Asstt. Comdt.
CIS Kadarpur, (Int Dte)

India, with its vast and diverse digital ecosystem, is witnessing significant transformations due to increased connectivity. The data revolution introduced by Jio, along with the widespread adoption of smartphones, has fueled India's internet penetration, connecting remote regions and creating a data-rich environment. However, this connectivity has also paved the way for new vulnerabilities.

Expanding Digital and Satellite Internet Services: Along with legal data connectivity, we are witnessing the expansion of satellite internet services, such as those from Starlink and Amazon's Project Kuiper, which introduces both opportunities and risks. Although these services are not yet legal in India, their presence in nearby regions like Myanmar highlights the potential for exploitation, especially by criminal groups. There have been instances of satellite internet devices being used by drug smugglers and extremists in disturbed areas like Manipur, underlining the unregulated nature of such technologies. We cannot neglect illegal entry/use of these devices in India. On social media several such allegations and official statements of confiscation of these devices from Myanmar are as shown below:



Generative AI further complicates the situation, as it enables the creation of sophisticated propaganda, deepfakes, and disinformation, which can destabilize societies, especially when combined with satellite internet. It provides access to a fast internet connection, with no legal restrictions of access in any remote areas of the world.

We can see in the flowchart – Figure 1-how this information is generated in a sophisticated manner through AI. These technologies empower malicious actors to operate from remote locations, beyond the reach of traditional enforcement mechanisms.

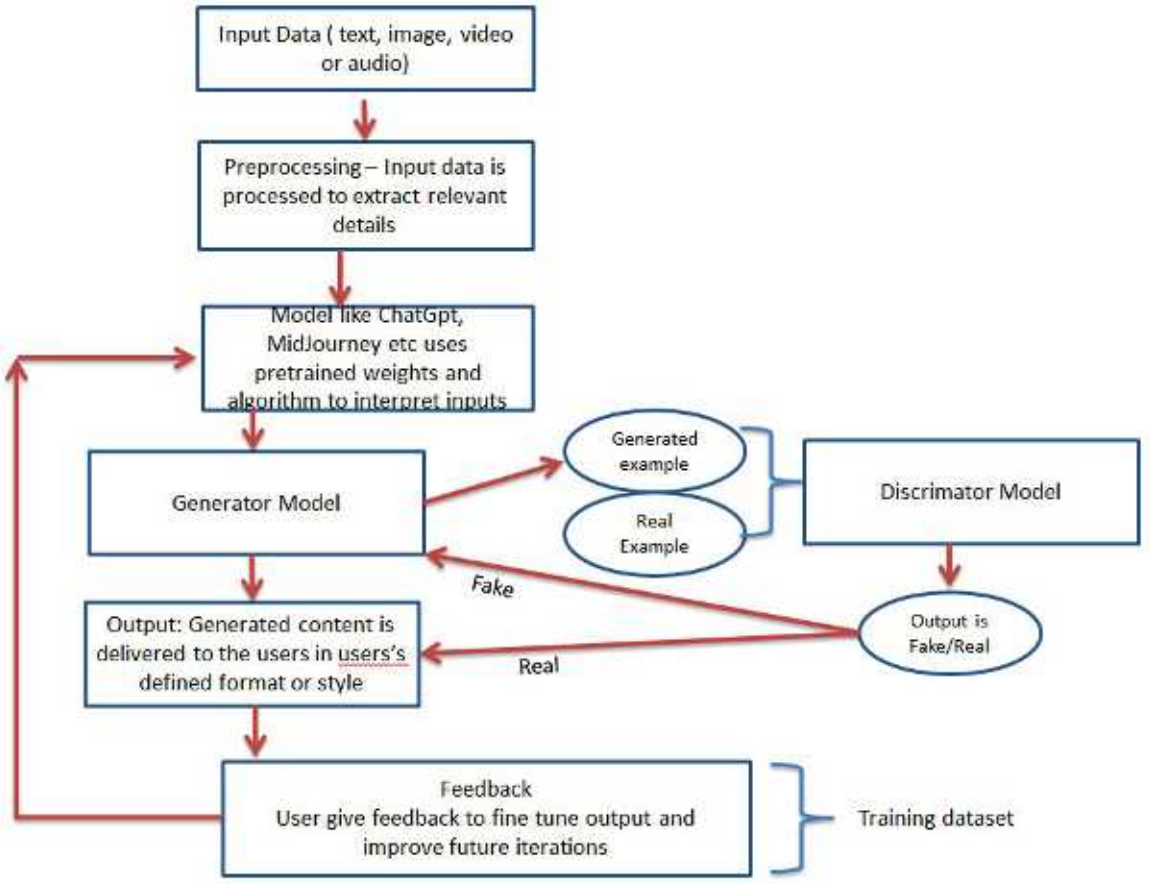


Figure 1: Flowchart showing generation of fake content through Generative AI

Impacts on the Indian Population: India's immense population and diverse socio-cultural fabric make it particularly vulnerable to the challenges posed by digital platforms. With over 700 million internet users, the country's online environment is rife with opportunities for economic growth, but also highly susceptible to misuse.

Social media platforms have been exploited to incite communal violence, spread fake news, and deepen societal divides. A new study published in Science reveals that falsenews spreads significantly faster, farther, and more widely than true information online. Conducted by MIT Media Lab's Soroush Vosoughi, professor Deb Roy, and MIT Sloan professor Sinan Aral, the

research shows that false news is 70% more likely to be retweeted than the truth on Twitter and reaches 1,500 people about six times faster. The study, which is the largest of its kind, highlights that false political news is particularly prone to this rapid spread.

This phenomenon has profound implications, particularly in the context of how adversaries exploit these patterns to spread propaganda through digital media teams. Such misinformation campaigns can have significant impact on a nation's domestic policies, economy, and internal security. In the case of India, the propagation of false information and the creation of an anti-India narrative can influence public perception and undermine national stability. Figure 2 below illustrates how fake information is disseminated, contributing to the construction of a false and damaging narrative.

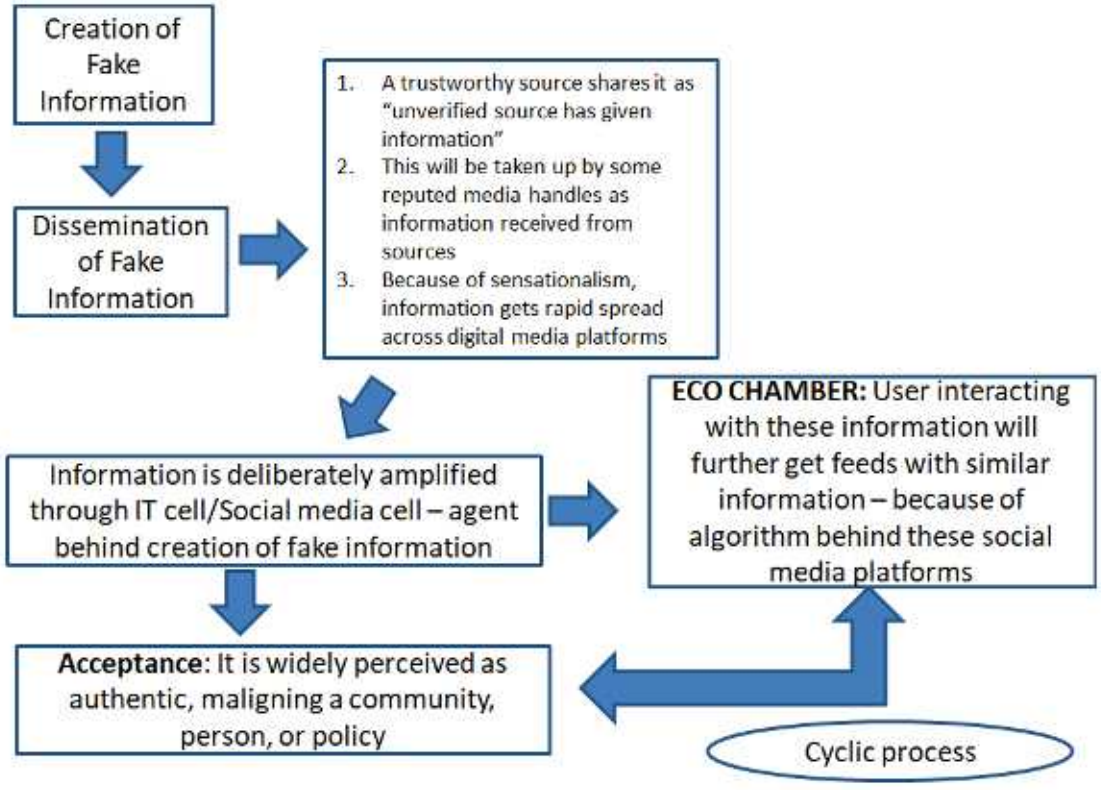


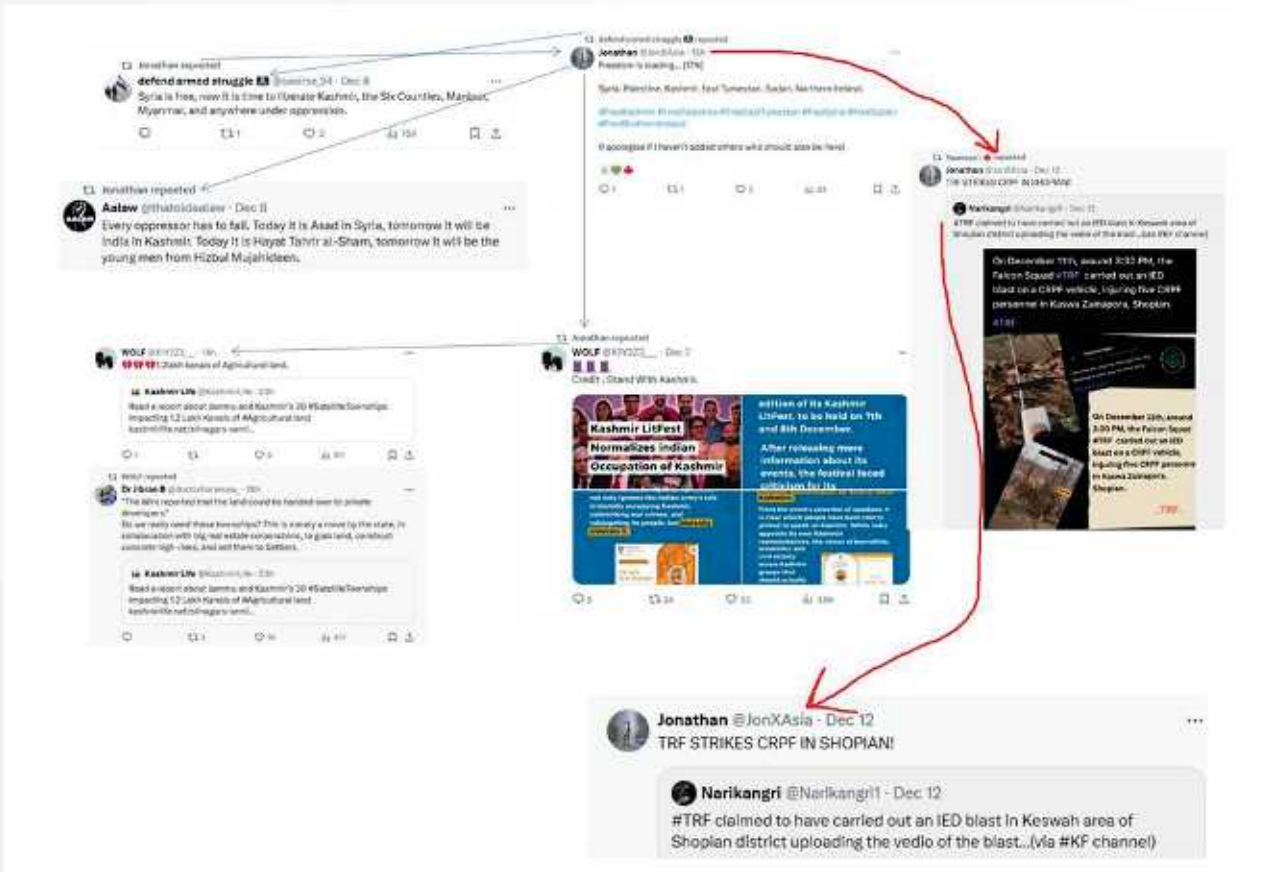
Figure 2: Block diagram showing generation and propagation of fake information

For instance, during elections, coordinated disinformation campaigns were used to polarize voters. Similarly, the Disinfo Lab uncovered efforts to manipulate narratives during India's elections, showcasing how digital platforms can be weaponized to disrupt the democratic process.

The psychological impact on the population is profound. Misinformation and polarizing content erode social trust, leading to fear, confusion, and divisiveness. Vulnerable groups, especially those in rural areas or with limited digital literacy, are often the most affected by scams and fake news.

Even one of India's largest paramilitary forces, the Central Reserve Police Force (CRPF), has become a target of malicious actors aiming to spread negative publicity. These efforts are often strategically orchestrated to damage the public perception of the CRPF.

In the case of the Kashmir issue, some accounts have drawn misleading comparisons between the situation in Kashmir and the changes in Syria, attempting to create a false equivalence. Moreover, these same accounts are also involved in spreading a negative narrative about the CRPF, which is deployed to maintain peace in these sensitive areas. By circulating false news and distorted narratives, these actors aim to erode public trust in the CRPF and its efforts to ensure security and stability in regions like Kashmir and Manipur.



Cyber-attacks targeting businesses and critical infrastructure in India have significant economic consequences, leading to financial losses and disrupting essential services. These disruptions not only impede organizational operations but also hinder the country's overall economic development. Additionally, such attacks can deter foreign investments, as potential investors may perceive India's cybersecurity defences as inadequate. A common tactic used by malicious actors is Distributed Denial of Service (DDoS) attacks, which overwhelm systems, disrupt operations, and compromise business continuity.

For instance, during the G20 Summit in September 2023, multiple hacktivist groups, including 'Ganonsec,' 'Jambi Cyber Team,' and 'Hacktivist Indonesia,' launched a campaign named #opIndia. These groups threatened to target Indian websites and ICT infrastructure on the 9th and 10th of September, soliciting global hacker support to escalate their efforts. Such events highlight the growing threat of cyber-attacks and their potential to undermine national security and economic stability.

Digital Platforms and Radicalization: Platforms like encrypted messaging apps, gaming communities, and social media are increasingly becoming breeding grounds for radicalization and recruitment. Extremist groups are leveraging these platforms to spread propaganda, recruit individuals, and organize attacks, including live-streaming acts of terror, as seen in incidents like the Christchurch mosque shooting. The ease of access and anonymity provided by satellite internet only amplifies these risks.

In the lead-up to Kashmir Self-Determination Day on January 5, 2025, Pakistan increased its efforts to amplify anti-India propaganda. This included social media campaigns and diplomatic outreach, aimed at criticizing India's policies in Kashmir and highlighting human-rights issues. Such activities are part of broader attempts to influence international opinion and rally support for Kashmir's separatist cause. These efforts have contributed to the geopolitical tension in the region and the continued spread of disinformation.

India's Exposure and Vulnerabilities: India's reliance on foreign-owned digital platforms and its rapidly growing digital user base expose it to significant risks. The decentralized nature of the internet further complicates efforts to monitor and control harmful content, as seen in global events like the Arab Spring.

The controversy surrounding WhatsApp's privacy policy updates has highlighted the global tension between user privacy and government regulation. In 2021, Turkey's media office abandoned WhatsApp over concerns about its updated policy, which enabled greater data sharing with Facebook, raising alarms about the handling of user data. Similarly, in India, the Competition Commission of India (CCI) fined Meta for unfair practices tied to WhatsApp's policy of mandating user consent for data sharing with Facebook. These incidents underscore the broader concerns about how tech companies balance user privacy with business interests.

In India, encryption and content moderation have also become contentious issues. The government has sought increased access to encrypted content, citing national security concerns, putting platforms like WhatsApp in a difficult position. Meanwhile, social media platforms like X (formerly Twitter) advocate for freedom of speech but face criticism for content disparity and management controversies. Challenges in regulating the information fed to citizens have drawn attention, with articles like those by Disinfolab addressing the complexities of countering disinformation in this digital landscape.

Further, emerging technologies like satellite internet and AI technologies represent a double-edged sword. While they can enable development and connectivity, they also empower malicious actors to spread extremist ideologies and conduct cyberattacks. The availability of high-speed internet in remote regions allows extremist groups to operate with unprecedented reach, while AI enables them to create deepfakes and micro-targeted propaganda, making digital manipulation more effective.

In India, where digital literacy varies widely, AI-driven disinformation campaigns are particularly dangerous. The potential for automating these efforts raises serious concerns about the future of digital security in the country.

Counter Strategies

The USA and China offer contrasting approaches to countering digital threats. The United States has established specialized units like the Global Engagement Center (GEC), now closed in December 2024 which was established to combat disinformation, collaborating with tech companies and international partners. Through advanced analytics and AI tools, the GEC counters foreign influence campaigns and promotes digital literacy among citizens.

China, on the other hand, takes a more authoritarian approach, tightly controlling its digital space through the Great Firewall and leveraging state media to shape narratives. While this model raises concerns about censorship, it has been effective in controlling the digital narrative and preventing foreign influence.

To tackle the growing digital threats, India must adopt a multi-faceted approach that integrates regulatory, technological, and collaborative strategies. Strengthening regulatory frameworks is paramount, with measures such as stricter content moderation policies, mandatory registration for satellite internet providers, and increased transparency in algorithmic decisions to ensure accountability of digital platforms. Special attention must be given to regulating social media content accessible to the younger population, drawing inspiration from steps taken by the Australian government. Public-private partnerships can play a crucial role, enabling the government and private tech companies to collaboratively develop advanced monitoring tools and real-time threat detection systems, thereby enhancing the resilience of India's digital ecosystem.

India's achievement of Tier 1 status in the Global Cybersecurity Index (GCI) 2024, with an impressive score of 98.49 out of 100, highlights its global leadership and commitment to robust cybersecurity practices. Joining the ranks of 'role-modelling' countries underlines India's progress in safeguarding its digital landscape. Building on this milestone, India should continue to enhance its cybersecurity infrastructure, leveraging its strong foundation to further protect its digital space and set global benchmarks in cybersecurity innovation and governance.

Additionally, India must prioritize digital literacy initiatives to empower citizens, especially in rural areas, to navigate digital platforms safely. Community-driven efforts can raise awareness about the risks of misinformation and online propaganda. Localized content moderation is another key area, with digital platforms encouraged to hire local experts who understand India's cultural and linguistic diversity to prevent the spread of harmful material. Lastly, India must strike a balance between privacy protection and national security. Engaging in international dialogues on encryption policy and promoting best practices for data security will be crucial for maintaining user trust while safeguarding national interests.

(Views/Opiniosn expressed here do not reflect the policies or positions of Government of India)

***

8 Naxalism in India; Its Economic Impact

Sh. Arvind
(Chief Security & Brand Protection)
Tata Steel Limited

This article comprehensively examines the multifaceted impact of Naxalism, a Maoist insurgency, on India's economic development. Originating in 1967 with the Naxalbari uprising, this Marxist-Leninist movement, fuelled by socio-economic inequalities and political oppression, has evolved into a widespread network affecting multiple Indian states and impacting several other countries. The insurgency's violent tactics, including attacks on infrastructure, extortion, and disruption of supply chains, have significantly hampered economic growth, particularly in resource-rich yet impoverished regions of central and eastern India. The article meticulously traces the historical evolution of Naxalism, detailing its spread from rural areas into urban centres and its profound effect on various sectors, including manufacturing, corporate security, and supply chains.

The significant financial burden on the Indian economy due to counter-insurgency efforts and the substantial losses incurred by businesses are thoroughly analysed. Furthermore, the article explores the various strategies employed to combat Naxalism, highlighting the need for a multi-pronged approach that encompasses both military operations and socio-economic development initiatives. The significant decline in LWE incidents in recent years and the government's ambitious goal of eradicating Naxalism by 2026 are also discussed, along with the challenges that still remain in achieving this objective. Finally, the article underscores the crucial role of sustainable development, inclusive governance, and community engagement in establishing lasting peace and fostering socio-economic progress in Naxal-affected areas.

The Naxalite insurgency, a form of Left-Wing Extremism (LWE), rooted in Maoist ideology, emerged in India in 1967 with the Naxalbari uprising. This initial localized revolt, fuelled by socio-economic inequalities and land disputes, quickly evolved into a broader movement, exploiting the government's neglect of impoverished rural areas in central and eastern India. States like Chhattisgarh, Jharkhand, Odisha, Bihar, and Maharashtra became epicentres of Naxalite activity.

The Naxalite movement's Marxist-Leninist ideology promoted violent revolution, initially focused on land reform. However, its reach extended beyond agrarian issues, encompassing broader socio-political grievances and utilizing tactics of violence, extortion, and attacks on industrial establishments. The movement's adaptability is evident in its expansion from rural strongholds into urban areas. This expansion highlights the deep-rooted nature of the conflict, intertwining ideological motivations with socio-economic disparities.

The impact on India's economic development is profound. The World Bank estimates significant losses in potential economic output due to Naxalite violence, which disrupts development projects, destroys infrastructure, and deters both foreign direct investment (FDI) and local investment. Billions of dollars have been allocated to counter-insurgency efforts, underscoring the substantial financial burden on the national economy.

"Between 2000 and 2012, the Indian government allocated approximately $13 billion to combat Naxalism, highlighting the immense financial burden on the economy (Source: <https://www.worldbank.org/en/news/feature/2013/01/31/understanding- the-naxalite-movement-in-india>). The lack of government presence and historical neglect in affected regions created a fertile ground for insurgency, further exacerbating the economic challenges."

The manufacturing sector, particularly in resource-rich states like Chhattisgarh, Jharkhand, and Odisha, suffers greatly. The steel and mining industries are particularly vulnerable. Production is disrupted by violence, extortion, and the constant threat of attacks. Companies face increased security costs, estimated at up to 30% of production costs in some areas. This, coupled with supply chain instability caused by hazardous transportation routes, severely reduces productivity and profitability. The uncertainty dissuades investment in human capital and technology, perpetuating a cycle of underdevelopment.

Specific incidents exemplify the impact on manufacturing. Attacks on construction convoys, extortion attempts against major steel companies, assaults on cement plants and mining operations, and ambushes of police convoys impacting production all highlight the unpredictable and destructive nature of Naxalite violence. These incidents lead to financial losses, operational disruptions, increased security expenses, and hampered economic growth. Small and medium-sized enterprises are especially vulnerable, facing immense challenges for survival, limiting job creation and entrepreneurship.

"Naxal violence in India has directly impacted manufacturing through numerous attacks. Examples include: attacks on construction convoys in Chhattisgarh (2017), extortion attempts against Tata Steel in Jharkhand (2014), attacks on Ambuja Cements in Chhattisgarh (2010) resulting in employee deaths, attacks on cement trucks in Andhra Pradesh (2011), ambushes of police convoys impacting operations in Gadchiroli (2018), sabotage of a cement plant in Odisha (2019), and attacks on mining trucks in Jharkhand (2020).

These incidents demonstrate the unpredictable nature of Naxal violence and its significant negative consequences for the manufacturing sector, causing financial losses, operational disruptions, increased security costs, and hampered economic development."

Corporate security in Naxal-affected regions faces unique challenges. Companies must implement comprehensive security measures to protect assets and personnel. This includes increased expenditure on private security, risk management, and contingency planning, diverting resources from core business operations. Extortion demands from Naxal groups create further financial vulnerability, with refusal resulting in potentially violent repercussions. The need to balance profit with employee and asset safety necessitates collaboration between businesses and law enforcement, integrating security strategies with community development initiatives.

Supply chain disruptions are another major consequence. Transportation and logistics face significant challenges due to the constant threat of violence. Delays in delivering supplies and raw materials escalate costs, forcing companies to re-route supplies through safer, albeit more

expensive, routes or invest in additional protective measures. The cost of these disruptions can reach 15-20% of operational costs. The impact extends to reduced efficiency, affecting production timelines and market responsiveness.

"According to a 2021 study by the Institute for Conflict Management, disruptions in supply chains can escalate costs by as much as 15-20% for companies operating in Naxal-affected states, as they re-route supplies through safer territories or invest in protective measures (Source: <https://www.sundayguardianlive.com/news/effect-naxalism-india-supply-chain-challenges>)."

Combating Naxalism requires a multi-pronged strategy. While military operations play a role, addressing the root causes through socio-economic development—improving infrastructure, education, and employment opportunities—is crucial. This requires counter-propaganda, dialogue, and technological advancements such as drones and data analytics. Strengthening legal frameworks must be balanced with oversight to prevent misuse. Ultimately, equitable development and inclusive governance are key to achieving long-term stability.

Recent years have witnessed a decline in LWE incidents, attributed to increased security measures, successful surrender campaigns with rehabilitation programs, and improved intelligence sharing. Government initiatives, such as the National Policy and Action Plan (NPAP), focus on improving infrastructure, education, and healthcare in affected regions, addressing the root causes of extremism. However, challenges remain, including socio-economic inequalities and the need for sustained community engagement to rebuild trust and reduce the appeal of Naxalite ideology. The government's aim to eradicate LWE by 2026 requires continued efforts in community engagement, employment creation, education, and awareness campaigns to achieve a lasting peace and foster a more prosperous future for all. The success of this endeavour depends on sustained commitment and collaboration between the government, local communities, and civil society. The long-term solution lies in addressing the underlying socio-economic issues that fuel the conflict and fostering a more inclusive and equitable society.

Combating Naxalism requires a multi-pronged strategy. While military operations play a role, addressing the root causes through socio-economic development—improving infrastructure, education, and employment opportunities—is crucial. This requires counter-propaganda, dialogue, and technological advancements such as drones and data analytics. Strengthening legal frameworks must be balanced with oversight to prevent misuse. Ultimately, equitable development and inclusive governance are key to achieving long-term stability.

Recent years have witnessed a decline in LWE incidents, attributed to increased security measures, successful surrender campaigns with rehabilitation programs, and improved intelligence sharing. Government initiatives, such as the National Policy and Action Plan (NPAP), focus on improving infrastructure, education, and healthcare in affected regions, addressing the root causes of extremism. However, challenges remain, including socio-economic inequalities and the need for sustained community engagement to rebuild trust and reduce the appeal of Naxalite ideology. The government's aim to eradicate LWE by 2026 requires continued

efforts in community engagement, employment creation, education, and awareness campaigns to achieve a lasting peace and foster a more prosperous future for all. The success of this endeavour depends on sustained commitment and collaboration between the government, local communities, and civil society. The long-term solution lies in addressing the underlying socio-economic issues that fuel the conflict and fostering a more inclusive and equitable society.

The Naxalite insurgency's devastating impact on India's economic development is undeniable. Decades of Maoist-fuelled violence, originating in 1967, have crippled crucial sectors, from manufacturing and supply chains to corporate security. Billions have been spent on counterinsurgency, yet the conflict's economic cost remains staggering, hindering growth, particularly in resource-rich yet impoverished states. The manufacturing sector, especially steel and mining, has suffered immensely from attacks and extortion, while supply chain disruptions have added significant costs. Small and medium-sized enterprises bear the brunt of this instability.

Though recent years show a decline in LWE incidents due to increased security and government initiatives like the NPAP, deep-rooted socio-economic inequalities persist. Sustainable peace requires more than military solutions; it demands addressing the root causes of the insurgency. A multi-pronged approach—investing in education, healthcare, and infrastructure, while fostering community engagement—is essential. Ultimately, achieving a Naxalism-free future hinges on a sustained commitment to inclusive governance, equitable development, and empowering local communities to build a more prosperous and peaceful India. Only through justice, equity, and empowerment can lasting peace and sustainable growth be secured.

***

9 Admissible Dues in CRPF

Sh. Vijay Kumar Bains
Second-in-Command
Welfare Dte., CRPF

Admissible dues refer to those dues which are payable to NOKs of CRPF personnel killed in action/ active duty/ natural death, and dues/payments made upon reaching the end of their service tenure or voluntary retirement. These admissible dues encompassthe following various components:

1. **Ex-Gratia (Central)** - The Ex-Gratia (Central) refers to a one-time payment made by the Central Government to the NoK of the deceased who laid down his life in action. At present, this amount is Rs. 35 lakhs w.e.f. 04/08/2016.

2. **Ex-Gratia (Duty State)** - Ex-Gratia (Duty State) refers to a one-time payment made by a state government to the NoK of the deceased who laid down his life in action where he performed his duty. The responsibility for administering and disbursing Ex-Gratia payment rests with the state (Duty State) government. This amount varies from state to state or as per orders of the respective state.

3. **Ex-Gratia (Home State)** - It refers to a payment made by a state government to NoK of the deceased who laid down his life in action. The responsibility for administering and disbursing Ex-Gratia payment (Home State) rests with the state government to which the deceased belongs. This amount varies from state to state or as per orders of respective state.

4. **GPAGIS -** GPAGIS stands for "General Personal Accidental Group Insurance Scheme". This is an insurance policy that provides coverage for accidental injuries or death to an employee of an organization. The coverage can include medical expenses, disability benefits and death benefits, depending on the terms of the policy. This is applicable in Chhattisgarh and Jharkhand only.

5. **Types of Pension :**

   - **Family Pension** - Family Pension is the regular monthly income received by the NoK after the death of an employee. If a government servant dies while in service, the family Pension payable to the family of a deceased government servant shall be equal to 50% of the last basic pay drawn by the deceased government servant. The enhanced rate of family Pension is payable from the date following the date of death of the government servant for a period of 10 years. After completion of 10 years family pension will be payable @ 30% of the last basic pay drawn (subject to a minimum of Rs. 9,000/- per month) by the deceased government servant till death or remarriage of NoK whichever is earlier.

   - **EOFP** - Extraordinary Pension also known as EOFP (Extra Ordinary Family Pension) in the form of disability pension/extraordinary family pension which may be paid @

60 % of last basic pay to the Government servant/his family if the disablement/death (or the aggravation of the disablement/death) of the Government servant, during his service, is attributable to the Government service.

- **EOP(LPA)** - Extraordinary Pension or Liberalized Pension Award under category 'D', which is given to NoK, @ 100% of the last reckonable emoluments drawn by martyr (killed in action) in case of wife and 75% in case of parents (both alive) and 60 % if only one parent is alive.

6. **DCRG** - It stands for Death-cum-Retirement Gratuity". It is a lump-sum one-time payment made to government employee upon their retirement or in the event of their death while in service (paid to the NoK.) The DCRG amount is calculated based on the employee's length of service and the last pay drawn before retirement or death.

7. **CGEGIS** - CGEGIS stands for "Central Government Employees Group Insurance Scheme". It is an insurance scheme for employees working in the Central Govt. of India. The scheme provides financial protection and security to the employees and their families in the event of death, disability or retirement. Under the CGEGIS, a part of the employee's salary is deducted and contributed to a common fund, which is managed by the government. The benefits provided under the scheme may include life insurance coverage, payment of a lump-sum amount on retirement and payment of a sum to the nominee in case of the death of the employee.

8. **LEAVE ENCASHMENT** - Leave encashment is a process by which an employee receives payment in exchange for un-availed leave period that they are entitled to. The amount of money an employee receives for their un-availed leave days is usually calculated based on their daily or monthly salary and any applicable taxes or deductions may also be taken into account.

9. **FIXED MEDICAL ALLOWANCE** - Fixed Medical Allowance is a specific amount of money that the government provides to pensioners to cover the cost of medical expenses. This allowance is usually given in addition to the pension.

10. **GPF**– GPF stands for General Provident Fund, which is a type of provident fund available to government employees. The GPF is a saving scheme that enables government employees to save a portion of their salary on a monthly basis and the accumulated amount earns interest over time. The purpose of the GPF is to provide financial security and stability to employees after retirement.

11. **DLI** - Deposit-linked Insurance is an optional scheme that can be linked with the GPF account. This insurance provides a lump-sum amount to the nominee in the event of the employee's death while in service. The insurance amount is linked to the balance in the GPF account and is typically a multiple of the balance, subject to a maximum limit. In other words, Deposit-linked Insurance is an insurance scheme available to government

employees who have a General Provident Fund account.

12. **PMSP (CAPSP)** - A specific scheme or benefit offered to Central Armed Police Forces personnel by the concerned salary account holding bank.

13. **Risk Fund** - The Risk Fund in Central Armed Police Forces (CAPFs) is a fund created to provide financial assistance to the families of the CAPF personnel who die while on active duty or while performing official duties or due to natural causes, etc. The Risk Fund is financed through contributions made by the CAPF personnel themselves. An amount Rs.500/- amount is deducted from the monthly salary of CAPF personnel and deposited into the Risk Fund account maintained at respective Force Headquarters. Assistance is provided from the Risk Fund lump-sum amount in case of Death/Invalidation/fitment of artificial limb cases and depending on other specific rules and regulations of the fund of respective force.

14. **CWF -** CWF stands for Central Welfare Fund created to provide welfare benefits and financial assistance to the force personnel and their families. The CWF provides a range of benefits and assistance to CAPF personnel and their families, including financial assistance to injured personnel, death cases, daughters' and sisters' marriage and medical advance for treatment as per the rules of the respective force. The Central Welfare Fund is financed through contributions made by the CAPF officers/personnel themselves as per rules of respective force.

15. **WAF -** WAF stands for Welfare and Amenities Fund, which is provided in Funds Manual 1976 (updated up to 2012). Its main purpose is to extend welfare measures in terms of activities and monetary benefits to the force personnel as per the rules of the respective force.

16. **BHARAT KE VEER** - Bharat Ke Veer Trust is a public charitable trust that was created by the Ministry of Home Affairs, Government of India, to support the families of Central Armed Police Forces (CAPF) personnel who are killed or disabled in the line of duty. The Bharat Ke Veer Trust has been set up as a platform to enable citizens and organizations to contribute to the welfare of the families of CAPF personnel. The trust accepts donations from individuals, organizations and corporate entities and the contributions are tax-exempted under Section 80G of the Income Tax Act,1961.

The following chart shows the applicability of admissible dues payable to NOKs of CRPF personnel killed in action, on active duty, due to natural death, or on supernnuation/voluntary retirement

SL.No.	ADMISSIBLE DUES	KILLED IN ACTION	DEATH ON ACTIVE DUTY/ACCIDENT ON DUTY/	NATURAL DEATH	ON SUPERANNUATION/ VOLUNTARY RETIREMENT
1	Ex-Gratia (Central)	Rs. 35 Lakhs	25 Lakhs	Not applicable	Not applicable
2	Ex-Gratia (State)	As per orders of respective State	Not applicable	Not applicable	Not applicable
3	Ex-Gratia(Home State)	As per orders of respective State	Not applicable	Not applicable	Not applicable
4	GPAGIS (General personal accident Group Insurance scheme	As per State policy Applicable in Chhattisgarh and Jharkhand only.	Not applicable	Not applicable	Not applicable
5	LPA/Family Pension	LPA (Last basic pay)	EOFP (60 % of Last basic pay)	Family Pension (50% of last basic pay & minimum 9000)	Pension (50% of basic pay)
6	DCRG	As per Admissibility provided in CCS (Pension) Rules {BP+DA X Number of SMP of Service (max. 66 SMP)/2}	As per Admissibility provided in CCS (Pension) Rules {BP+DA X Number of SMP of Service (max. 66 SMP)/2}	As per Admissibility provided in CCS (Pension) Rules {BP+DA X Number of SMP of Service (max. 66 SMP)/2}	As per Admissibility provided in CCS (Pension) rules {BP+DAX Number of SMP of Service (max 66 SMP)/4}
7	CGEGIS	As per entitlement/ admissibility	As per entitlement/ admissibility	As per entitlement/ admissibility	As per accumulation &fitment table
8	Leave Encashment	Last B/pay + DA X leave/30	Last B/pay + DA X leave/30	Last B/pay + DA X leave/30	Last B/pay + DA X leave/30
9	Medical Allowance	Rs. 1000/- P.M. or CGHS Facility.	Rs. 1000/- P.M. or CGHS Facility.	Rs. 1000/- P.M. or CGHS Facility.	Rs. 1000/- P.M. or CGHS Facility.
10	GPF	Amount accredited in account **(*Appointee before 01/01/2004)**	Amount accredited in account **(*Appointee before 01/01/2004)**	Amount accredited in account **(*Appointee before 01/01/2004)**	Amount accredited in account **(*Appointee before 01/01/2004)**
11	Deposit linked Insurance (DLI)	Rs. 60,000/- **(*Appointee before 01/01/2004)**	Rs. 60,000/- **(*Appointee before 01/01/2004)**	Rs. 60,000/- **(*Appointee before 01/01/2004)**	Not applicable
12	CAFSP (PMSP)	Rs. 60,00,000/- (w.e.f. 04/01/2022) (Only in Accidental cases)	Rs. 50,00,000/- (w.e.f. 04/01/22) (Only in Accidental cases)	Not applicable	Not applicable
13	Risk Fund	Rs. 30 Lakhs NOK - Rs. 18 Lakhs Parents- Rs. 7.5 Lakhs Children – 4.5 Lakh	Rs. 20 Lakhs NOK - Rs. 12 Lakhs Parents- Rs. 05 Lakhs Children – 3 Lakh	Rs. 20 Lakhs NOK - Rs. 12 Lakhs Parents- Rs. 05 Lakhs Children – 3 Lakh	Total Accredited to his A/C + bonus
14	CWF	Rs. 5 Lakh	Rs. 5 Lakh	Rs. 5 Lakh	Not applicable
15	WAF (Immediate Financial Relief)	Rs. 50,000/-	Rs. 50,000/-	Rs. 50,000/-	Not applicable
16	Bharat Ke Veer	Killed in Action: Rs. 25 Lakh Parents to married martyrs: Rs. 10L	Not applicable	Not applicable	Not applicable

Note: The above-mentioned information is only informative in nature.
However, it may vary as per rules and regulations of the department/Govt.of India.

10 सिलगेर स्कूल: नई सुबह की पहली किरण

श्री कुलदीप सिंह
उप कमांडेंट, 229वीं वाहिनी, के०रि०पु० बल
बीजापुर (छत्तीसगढ़)

कई दशकों से छत्तीसगढ़ नक्सली हिंसा से गुजर रहा है। जिसके चलते वहां के लोग देश की मुख्यधारा से अलग थलग हैं और एक अंधकारमय जीवन जीने को विवश हैं। अपना प्रभुत्व कायम रखने के लिए नक्सलियों ने इस क्षेत्र को मुख्यधारा से जुड़ने नहीं दिया तथा वहां के भोले–भाले लोगों को अज्ञानता के अंधेरे में रख कर नक्सली हिंसा में झोंक दिया। अज्ञानता से घिरे लोगों को गुमराह करके उनकी मानसिकता पर प्रहार करके उन्हें सरकार के विरूद्ध लडने के लिए तैयार किया। युवाओं की जिस ताकत ने राष्ट्र निर्माण में भागीदारी देनी थी, वो सरकार के विरूद्ध शस्त्र उठाए खड़ा है। अब परिस्थिति यह है कि अब नक्सलवाद इनके विचारों में रच बस गया है, जिसे शिक्षा और ज्ञान से ही दूर किया जा सकता है। देश मे चल रही परिवर्तन की लहर से बेखबर, यहां के निवासी नक्सली हिंसा को ही अपना भाग्य मान कर कई सालों से इस अंधकारमय जीवन जीने को मजबूर हैं। नये भारत के अन्य बच्चों की तरह यहां के बच्चों के हाथ में किताबें/अन्य सुविधाओं के स्थान पर, अपना जीवन यापन करना ही एक चुनौती है।

राज्य के पुलिस प्रशासन को मजबूत करने के लिए, इस क्षेत्र में नक्सलवाद से लड़ने के लिए, केन्द्रीय रिजर्व पुलिस बल को मुख्य जिम्मेदारी दी गई है। नक्सलवाद की शुरूआत से ही, कई वर्षों से केन्द्रीय रिजर्व पुलिस बल इस क्षेत्र मे नक्सलवाद से लड़ाई लड़ रही है। इस लड़ाई में इस बल ने अपने कई जवानों की आहूति दी है। परन्तु इन सब अपवादों के चलते इस बल ने निरन्तर नक्लवाद के खिलाफ अपनी लडाई जारी रखी। इस प्रतिबद्धता के निशान छत्तीसगढ़

तथा अन्य नक्सलवाद प्रभावित राज्यों में देखे जा सकते हैं। जिन क्षेत्रों में कोई सड़क नहीं थी तथा वहां पहुँचना ही एक चुनौती थी, वहां उच्च श्रेणी के राष्ट्रीय राजमार्ग हैं। लोग निर्बाध तरीके से आना जाना कर सकते हैं, इन क्षत्रों में विकास की नई हवा बह रही है।

केन्द्रीय रिजर्व पुलिस बल के अतिरिक्त, इस लड़ाई में भागीदार हर पक्ष ने अपना निष्ठा पूर्वक योगदान दिया है, चाहे वो केन्द्र सरकार हो या राज्य सरकार। इस

लड़ाई में बल प्रयोग के अतिरिक्त, केन्द्रीय रिजर्व पुलिस बल ने अन्य विकल्प का भी प्रयोग किया जिसमे सिविक एक्शन प्रोग्राम के द्वारा स्थानीय लोगों से मेल–जोल बढाना, समय–समय जागरूकता अभियान चलाना ताकि लोग नक्सलवाद के दुष्प्रभावों को समझ सकें, आपदा के समय लोगों की मदद करना इत्यादि। ये प्रयास लोगों से मेल–जोल बढ़ाने में लाभप्रद तो रहे परन्तु इतना मात्र पर्याप्त नहीं था। बन्दूक की नोक पर, बल पूर्वक लोगो को दबाया जा सकता है, नक्सलवाद की हथियारबंद लड़ाई को रोका जा सकता है, परन्तु चुनौती नक्लवाद की विचारधारा को हराने की है, लोगों को उस विचारधारा से बाहर निकाल कर उन्हें मुख्यधारा में शामिल करने के लिए एक राह प्रदान करने की है।

नक्सलवाद की लड़ाई के बदलते परिदृश्य में रणनीति निर्णय अनुसार, केन्द्रीय रिजर्व पुलिस बल ने नक्सलवाद प्रभावित दुर्गम क्षेत्रों में अपनी पहुंच को बढाने के लिए फारवर्ड आपरेटिंग बेस खोलने शुरू किए। इससे सरकार की इन इलाकों में पहुँच बढ़ी तथा नक्सलवादियों की गतिविधियों में भी अंकुश लगा परन्तु लोग अभी भी इस बन्धन से मुक्त नहीं है। कुछ डर के कारण तो कुछ अभी भी नक्सलवाद की विचारधारा से प्रभावित है।

फारवर्ड आपरेटिंग बेस खोलने के क्रम में 229 बटालियन, केन्द्रीय रिजर्व पुलिस बल को बीजापुर के अति संवेदनशील सिलगेर गांव में फारवर्ड आपरेटिंग बेस खोलने की जिम्मेदारी दी गई। इस फारवर्ड आपरेटिंग बेस को खोलते समय, ग्रामीणों का भारी विरोध का सामना करना पडा। परन्तु वहां तैनात अधिकारियों की कड़ी मेहनत तथा सूझबूझ के कारण फारवर्ड आपरेटिंग बेस खुल गया। वहां तैनात के दौरान मेरे मन में विचार आया कि क्यूं ना यहां एक स्कूल खोलकर बच्चों के लिए नई शुरूआत की जाए। ताकि नक्सलवादी विचारधारा को तोड़ा जा सके।

इस विचार को मैंने अपने मुख्यालय के उच्च अधिकारियों, विशेष तौर पर श्री पुष्पेन्द्र कुमार से साझा किया। यह विचार तो उत्तम था, परन्तु इसे हकीकत में परिवर्तित करना आसान नहीं था क्योंकि नक्सली ऐसे किसी भी विचार को वहां पनपने नहीं देते थे। वर्ष 2005 से पहले यहां एक आश्रम हुआ करता था जिसमें रहकर बच्चे पढ़ाई किया करते थे, परन्तु नक्सलियों ने आश्रम के स्कूल को तोड़ डाला था और तभी से लगभग दो दशकों तक यहाँ कोई शिक्षा संस्थान नही रहा और यह क्षेत्र अज्ञान के अंधकार में डूबा रहा।

परन्तु इरादों से मजबूत, श्री कुलदीप सिंह, उप कमाण्डेंट अपने दृढ़ इरादे और कार्यशैली के कारण अपने अधिकारियों को स्कूल खोलने के विचार पर सहमत करने में सफल रहे। संसाधनों को जुटाने और इसको सफल बनाने में श्री निशांत शर्मा, श्री राहुल माधव, श्री प्रकाश चन्द, श्रीमती वर्षा रूण शर्मा, सहायक कमाण्डेंट की महत्वपूर्ण भूमिका रही। जिन्होंने संसाधनों को जुटाने में अहम योगदान दिया और अपने व्यस्तम समय में से समय निकालकार बच्चों को पढ़ाया। प्रशासन तथा स्थानीय लोगों को विश्वास में लेकर तथा सीमित संसाधनों से 15 अगस्त 2022, को, केन्द्रीय रिजर्व पुलिस बल द्वारा संचालित, सिलगेर स्कूल, की स्थापना की गई। इस पूरे प्रयास में 229 बटा0 के कमाण्डेंट, श्री पुष्पेन्द्र कुमार की बड़ी भूमिका रही।

स्कूल का उद्घाटन, श्री आरिचि अंथनी माहिओ, द्वितीय कमान अधिकारी की उपस्थिति में सिलगेर गांव के पटेल श्री माड़ा कोरसा द्वारा किया गया। इसको स्थापित करने में पुलिस विभाग, स्थानीय प्रशासन तथा राज्य के शिक्षा विभाग की भी अहम भूमिका रही। शुरूआती विरोध के फलस्वरूप,

जल्द ही स्थानीय लोगों ने इसे अपना लिया। जिसे सिर्फ 57 बच्चों से शुरू किया गया था, वर्तमान समय में उस सिलगेर स्कूल में 87 से अधिक बच्चे हैं। यह अपने आप में यह एक अद्भुत प्रयास था जिसने ना केवल स्थानीय लोगों को आशान्वित किया है तथा स्थानीय प्रशासन भी इससे बडा उत्साहित है। इस सफल अनुभव के पश्चात, अन्य 03 फारवर्ड ऑपरेटिंग बेस में भी स्कूल खोले गए हैं, जिसके लिए के0रि0पु0 बल द्वारा विशेष प्रोजेक्ट स्कीम के तहत, संसाधन जुटाने के लिए बजट की व्यवस्था की गई।

इस स्कूल से जुड़े कुछ स्थानीय लोगों के अनुभव साझा करना जरूरी है ताकि इस स्कूल के कारण इस क्षेत्र मे हो रहे बदलाव को हम सही रूप में समझ सकें। सिलगेर गाँव मे रहकर, बाहर जगदलपुर व सुकमा में पढ़ाई करने के बाद वर्तमान में बी0 फार्मा कर रहे श्री कोरसा हुंगा और वर्तमान में बीए करने के बाद इसी स्कूल में बच्चों के उज्जवल भविष्य के लिए शिक्षक के रूप में कार्य करने वाले श्री कोरना जयराम का कहना है कि हम सभी सिलगेर निवासी 229 बटा0 के0रि0पु0बल का दिल की गहराइयों से धन्यवाद करते हैं, जिन्होंने हमारे गाँव से शिक्षा के अन्धकार को हटाकर स्कूल के रूप में रोशनी फैलाई। हमारे गांव से 50 से 60 कि0मी0 तक कोई स्कूल न होने के कारण एक पीढ़ी पढ़ ही नहीं पाई, जिससे वे नक्सलवाद की दलदल में धंसते चले गए। यह स्कूल हमारे लिए अविस्मरणीय रहेगा।

"कदम ऐसा चलो कि निशान बन जाए,
काम ऐसा करो कि पहचान बन जाए,
जिन्दगी जियो तो ऐसी जियो कि मिसाल बन जाए"

"देश का सम्मान मेरी ताकत, मेरी जान है,
इसीलिए मेरे द्वारा छोडा हर निशान, मेरी पहचान है"

11 Invisible Threats, Visible Solutions: Strengthening CRPF's Tech Defences

Sh. Tarang Bansal
Asst. Comdt.
4th Signal BN, Neemuch

Incident Overview:

On September 17, 2024, a shocking incident in Lebanon brought pagers, a rarely discussed technology, into the spotlight. Hundreds of pagers used by Hezbollah members and medics exploded simultaneously, killing at least 30 people and injuring nearly 3,000. On the very other day VHF sets have exploded and news of blast of solar panel have also been confirmed. While the political implications are significant, the technical aspects of how this attack was carried out are both fascinating and alarming. The explosions point to a potential supply chain attack, where the pagers, VHF sets were likely tampered with during manufacturing or transit, embedding explosives that were remotely triggered. This incident highlights the vulnerability of even low-tech devices to sophisticated sabotage.

Security Challenges for India:

India faces similar security challenges, particularly given its **heavy reliance on imported semiconductor chips.** Presently, India ranks as the second-largest importer of semiconductor chips globally, with a staggering 92% surge in imports over the last three years, as reported in the Rajya Sabha. Estimates suggest that **90% to 95% of India's semiconductors are imported**, primarily from Eastern regions such as China, Taiwan, and South Korea. In the current security scenario, where India faces threats from China and Pakistan, the risk of supply chain sabotage is significant. **Chinese agencies or the ISI** could potentially exploit this dependency, compromising our devices and posing a severe threat to national security.

How the Pagers and VHF Sets Exploded:

Several theories have emerged to explain how such low-tech devices could be turned into bombs:

1. **Battery Overheating:** One possibility is tampering with the batteries of pagers and VHF sets, causing them to overheat and explode. However, this theory is less likely since pagers lack internet connectivity, making remote triggering difficult.
2. **Supply Chain Attack:** Another likely scenario is tampering during manufacturing or transit. Some reports suggest Israeli intelligence may have infiltrated the supply chain, embedding explosives into the devices before they entered Lebanon. This points to a sophisticated operation aimed at sabotaging Hezbollah's communication network.
3. **Remote Trigger:** Analysts speculate that the pagers, once tampered with, could have been triggered by a remote signal, resulting in synchronized explosions across multiple devices. This would require advanced planning and access to the pagers during their production or distribution.

Hezbollah's Use of Pagers/VHF Sets:

Hezbollah has relied on pagers and VHF sets for their perceived security advantages. Pagers and VHF sets operate using radio frequencies, which make them more difficult to track than smartphones are. The use of pagers, a seemingly outdated technology, was part of Hezbollah's strategy to avoid sophisticated tracking techniques. However, this incident demonstrates that even low-tech solutions are not immune to sabotage if an attacker compromises the supply chain.

Countermeasures and Safety Strategy:

To protect against similar threats, the Central Reserve Police Force (CRPF) and other internal security agencies must implement robust countermeasures:

1. **Strengthening Supply Chain Security:**
   - Conduct stringent vendor audits to ensure the integrity of devices before they are procured.
   - Employ tracking and verification mechanisms to detect tampering during manufacturing and transit.
   - Partner with trusted manufacturers and maintain secure agreements with suppliers.
2. **Enhanced Device Vetting:**
   - Implement regular physical inspections of communication devices, especially before deployment in high-risk areas.
3. **Mitigating Hardware Exploits:**
   - Isolate critical communication devices from untrusted areas and avoid reliance on a single type of device for crucial operations.
   - Implement redundant communication methods to ensure that operations can continue even if primary devices are compromised.
4. **Transition to Modern Secured Devices:**
   - Gradually replace outdated devices with modern, secure communication platforms
   - that incorporate advanced encryption and security features.
   - Multi-factor authentication and end-to-end encryption should be standard on all communication devices.
5. **Training and Awareness:**
   - Increase cybersecurity training for officers to recognize potential vulnerabilities in communication devices.
   - Establish a dedicated monitoring team to watch for signs of tampering or unusual

behaviour in communication tools.

- Create a framework and include it in annual inspections.

Anti Sabotage Team

1. **Anti-Sabotage Techniques and Modern Equipment:** Utilizing advanced tools such as Non-Linear Junction Detectors (NLJD), infrared scanner, counter-surveillance radars, anti-spoofing and anti-espionage devices to detect and neutralize sabotage attempts.
2. **Cyber Security Expertise:** Incorporating experts skilled in red, blue, and white hat hacking to ensure the security of networks and devices, identifying and mitigating potential cyber threats before they can be exploited.

This initiative would significantly enhance India's capability to protect against both physical and cyber sabotage, ensuring the integrity and security of critical communication and technology infrastructure.

Conclusion:

The electronic-devices explosions in Lebanon signal a shift in the nature of cyber-physical threats, in which even low-tech devices can be exploited by adversaries. The CRPF must take proactive steps to strengthen its communication security, focusing on supply chain integrity, regular inspections, and the adoption of modern technologies. By implementing these countermeasures, we can mitigate the risk of future attacks and protect the internal security apparatus from sophisticated sabotage tactics.

***

The CRPF Academy Journal

Annual Issue- Edition II Jan-Dec-2025

Note for Contributors

The CRPF Academy Journal is the latest endeavour of CRPF Academy. Its publication is intended for the understanding of the Police Officers across the Country who are continuously engaged in Low Intensity Conflict Management round the clock. Its publication is envisioned yearly. It is circulated through hard copy as well as in e-book format. It is circulated to all the Police Forces of the Country. It aspires to be the leading Academic Journal of CRPF Academy, which provides critical inputs to the stake holders of Internal Security.

How to Submit Article/ Paper

The paper/article on Internal Security, Law & Order, Cyber Crime, Organized crime, Human resource development, Police reforms, Police training, Human Rights, Intelligence, Militancy, Terrorism and Insurgency related topics can be submitted.

The paper, article with key words and abstract should be between 2000-3000 words. The paper/Article should be original and have not been published in any Journal. A brief detail about Author should be submitted. The paper can be submitted through e-mail acdykar@crpf.gov.in

The paper/Article can also be submitted through post with hard copy in duplicate and a CD on the following address- The Editor, The CRPF Academy Journal, CRPF Academy, Kadarpur, Gurugram (HR) PIN-122101.

About CRPF Academy

The CRPF Academy, Gurugram commenced functioning on 18th October 2005 with the mandate to conduct basic training of Directly Appointed Gazetted Officers (DAGOs). The Academy also comprises Centre for Internal Security Studies (CISS) which has been designated as a Centre of Excellence (CoE) and conduct various Low Intensity Conflict Management courses for State and Central Police Force officers under the aegis of BPR&D. Till date the Academy has trained 2372 DAGOs including 79 female officers. So far, officers trained from this Academy have secured 02 Kirti Chakra, 14 Shaurya Chakra, 03 PPMG and 187 PMG. 06 Officers have made their supreme sacrifice in the Service of Nation.

The Academy received Union Home Ministers "Best Training Institution Trophy" (Officers category) for the year 2019-2020.

CRPF Academy
Gurugram, Haryana

Website: crpf.gov.in/Training/CRPF-Academy