The Shivapuri

Volume: XXVI, 2025

DOI: https://doi.org/10.3126/shivapuri.v26i1.75841

Army Command and Staff College, Nepali Army

Shivapuri, Kathmandu, Nepal

Vulnerabilities of the Communication System to an Electromagnetic (EM) Attack, Threat Assessment and Mitigation

- ***Brig Gen Shobendra Singh Mahat***

Abstract

The rise of electromagnetic (EM) technology has introduced a significant security challenges, particularly for military operations. Opponents regularly try to exploit EM weaknesses to disrupt communications and other weapon systems either physically or remotely. A recent example is the Lebanese Hezbollah's pager and radio explosion incident where communication system had been weaponized by the adversary attracting worldwide attention in which remotely controlled EM technique was used and thereby presenting a grave concern to all electronic equipment users around the world including Nepal and its security agencies. In Nepalese context, security forces are facing the challenges of lacking reliable modern quality based electronic communication system due to various reasons including budget constraints, limited awareness, meager technological advancements like inadequate EM shielding and so on. As a future strategist and reliable successful military commander, we should visualize another spectrum of our signal vulnerability by EM attacks in our communication system. We need to understand the consequences that could disrupt not only command structure and jeopardize troop safety but also undermine operational effectiveness.

Keywords

Electromagnetic Technology, Electromagnetic Interference, EW attacks, Mitigation Strategies

Introduction

A Lebanese man is standing at a cash register on 17 September 2024 when the pager at his waist explodes, hurling him to the ground. Less than a meter away, the cashier panics but seems unhurt. Another man, shopping for green almonds in a market, collapses when smoke bursts from his midriff. Some shoppers run away, others stare in confusion (The Economist, 2024, November 2). First, hundreds of pagers blew up, next to the following day, more wireless devices (walk talkies) exploded, adding to the human toll and spreading terror that any portable gadget in people's hands or pockets could suddenly became a weapon (The New York Times, 2024, Nov 5). The attack against Lebanese Islamic militia group Hezbollah, highlights how electronic technology can be weaponized for precision target, where details are limited. In this incident, a remotely triggered mechanism allegedly involved to tigger pagers and radio sets belonging to Hezbollah leading to an explosion. The attackers, marked one of the largest security failures in Hezbollah's history and showed chaos inside Arab World. In the alleged Hezbollah pager incident, adversaries supposedly used RF (Radio Frequency) signal to tigger a devise, causing it to explode. The devices either pager, cell phone, smart watches and radio sets are critical to the communication of any security agencies may become the very tool likely to be used as a double-edged sword. This kind of attacks exemplifies the vulnerabilities of unshielded or cheaper commercial devices, which may not have any protection against RF interference or EM based attacks. In various military operations, these types of vulnerabilities can be exploited to cause disruptions, fatalities or even demoralization among the troops.

These are the latest examples that Electromagnetic web has been attacked causing international attention. This web refers to the inter connected network of various electronic devices utilizing electromagnetic waves such as radio, wi-fi, cellular signals and Bluetooth. This signal provides an opportunity for the transformation of real-time data easily and effectively. Now has become a backbone of modern electronic devices, military communication and surveillance networks etc. EM waves can travel long distance through bounded media such as light waves emitted by the sun and radio waves transmitted by radiating elements like antennas (Gupta, 2019).

EM web offers immense utility, it also introduces security challenges like electromagnetic interference (EMI), Signal Jamming and Electronic Magnetic Pulse (EMP) attacks. As dependency on this web technologies increases, protection of EM web against adversaries become critical to protect both civilian and defence application from vulnerabilities.

In Nepalese context, although our security forces are yet to adopt a fully modernize communication technology in its day to day affair, one should understand communication vulnerabilities and ways to mitigate likely electronic interference, threats as well as electronic disruption. This paper tries to provide an overview of how advancements in communication technology have increased both the utility and vulnerability of devices in communication spectrum of our security forces.

Types of Electromagnetic Threats

The recent incident in the Middle East underscores the potential for harm that EM based attacks can cause affecting not only equipment but also personnel security. The rise of weaponization of Electromagnetic Technologies has made a new realm of security threats in the form of “Electronic Web” attacks where devices like pagers and surveillance equipment are essential to security forces are being hugely targeted.

Conflict zones in Ukraine, Lebanon, Syria and Gaza; adversaries are targeting radio and satellite communication to create operational difficulties for their opponents' interference can range from temporary to total incapacitation of devices with far reaching effects. For example, imagine a convoy of security forces relying on radio contact that suddenly goes silent due to a well-coordinated EM attack, leaving the personnel vulnerable to dangerous consequences. Some of the commonly used threats have been described below.

Electromagnetic Interference (EMI)

It is also called Radio-Frequency Interference (RFI) when in the radio frequency spectrum, it's a disturbance caused by an external source that affects the circuit of the equipment. This disturbance may reduce the equipment performance. EMI can be divided in several categories on the basis of source and characteristics of signal communication.

Electromagnetic Pulse (EMP) Attacks

It is a brief burst of electronic magnetic energy. The origin of an EMP can be natural or artificial, and can occur as an electromagnetic field. The EMP can disrupt communications and damage electronic equipment. In modern warfare, weapons delivering a high energy EMP are designed to disrupt communications equipment, the computers needed to operate modern warplanes, or even put the entire electrical network of a target country (Wikipedia, 2024, December 23).

Signal Jamming

This is a method to disrupt communication by transmitting noise or interfering signals on the same frequency. This makes receiver being unable to receive the data. The

jamming technology is widely used and one of the easiest and cheapest ways to jam unwanted signal communications.

Hacking via EW waves

This method involves such equipment that is used with a intent of gathering information, adversary try to hack signal emission or inject malicious signals generated by communication devices.

Challenges for the Nepali Security Forces

Like many other military organization, Nepali security forces totally depend on various electronic devices for exchange of data, coordination and communication and so on. These devices if unprotected, likely to be vulnerable to various EM based attacks. Some key challenges include:

Limited EM shielding

Communication devices like radios are not protected against EM web attacks.

Budget Constraints

Acquiring and developing EM resistant equipment requires huge amount of budget and is expensive, due to budget constraints and limitation, may hinder the ability of the security force comprehensively upgrade its system.

Lack of awareness and training

This EM threats are relatively new to all security force and the personnel may not be trained to counter EM threats.

Reliance on commercial equipment

Military gradate-Shielded equipment may not be available for every operation leading to reliance on commercial devices that are more vulnerable to EM attacks.

Likely Consequences of EW Attacks on Nepali Security Agencies

If the Nepali security agencies were to face EM-based interference, the potential consequences could include:

Communication Breakdowns

Radio Frequency (RF) jamming could isolate units, leaving them without access to coordination and command. This could lead to jeopardize in planning and execution of any operation.

Sabotage and Explosion of Devices

We can't deny like the Hezbollah pager incident may not happen in Nepal, remote triggering of devices could result in fatal incidents, affecting personnel safety and morale.

Errors in Navigation

GPS disturbances could lead to incorrect positioning, potentially causing troops to enter hostile areas or disturb strategic movements.

Mitigation Strategies for the Nepali Security Agencies

Threats to electromagnetic web could be unlimited in terms of time, place and the degree of enemy's fierceness. The Nepali security agencies should visualize the

extent of EM threats and foresee all practical means to address how to adopt different mitigation approaches. Some effective measures include:

Invest in EM Resistant Devices

Wherever possible, the Nepali security agencies should acquire communication and navigation equipment designed with EM Shielding to withstand EMPs and RF resilient to jamming and RF spoofing.

Retrofitting Existing Devices

When acquiring new equipment is impractical, retrofitting existing devices with EM shielding materials can provide a layer of protection. Materials like copper mesh or aluminum can be effective in blocking or reducing the effective of EM waves on the device's circuitry.

Procurement Standardization

Although its costly and impractical due to budget constraint and may be beyond economical means of all security forces in Nepal, there is no harm to think that the user agencies should bear in mind the future procurement could include EM resistance as criterion which ensures equipment is built to withstand EM -based threats.

Training Strategy on EM Threats

Owing to Nepalese geo-strategic location and its proximity to big Asian powers; Nepali security agencies cannot deny the possibilities of EM based future conflict on its soil. The friction between India and China may transfer from Northwestern Himalayas to greater Himalayan range. On Nov 17, 2020 The Times magazine claims that the Chinese military used "high-energy electromagnetic radiation" technology to effectively turn "two strategic hilltops that had been occupied by Indian soldiers. The attack left the

Indian troops "vomiting" and unable to stand within 15 minutes, enabling the People's Liberation Army to retake two strategically important hilltops in the Himalayas without any exchange of live fire (The Week, 2024 December 28). This incident highlights that how electromagnetic web can be weaponised in this modern age. The future conflict in Nepalese proximities may not be confine only between the two borders of big Asian Hubs. Because of these reasons, our training doctrine also incorporate likely electromagnetic based armament technology of modern times. Therefore, our signal training strategy should include

Raise Awareness

Personnel should be educated on the potential risks posed by EM-based attacks, including jamming, spoofing and remote triggering.

Training in Anti-jamming Tactics

Familiarize troops with techniques to identify and counteract jamming.

Mock Drills and Simulations

Conduct regular exercises that simulate EM attacks to train soldiers in response strategies, such as fallback communication methods and identifying signs of EM interference.

Survival Technique

If the future friction between our neighbours extends out of present locations, we can't assure that the conflict space only restricted out of Nepalese Himalayan Range, the situation may arise like "when elephants fight, it is the grass that suffers." therefore, Nepalese security forces should know the survival technique against any

electromagnetic attacks that could affect Nepalese communication spectrum when such circumstances comes into our territory.

Invest in Detection and Monitoring Equipment

Now a days, it has been observed that the development of AI and Electromagnetic technology has emerged as a new weapon system. The technology which adversaries are exploiting in their favour, has compelled the defender to develop counter measures in relation to its enemy's resistance. Hence, Nepal also look forward to acquire such minimum capability against electromagnetic threat that include,

Deploy EM Detection Sensors

EM detectors and RF spectrum analyzers can help identify interference or malicious EM activity in the field. Early detection enables the security agencies to counteract attacks before they escalate.

Monitor for Unauthorized RF Signals

By monitoring RF frequencies around sensitive operations, potential threats can be identified and neutralized early. For instance, personnel could use handheld spectrum analyzers to detect and localize jamming sources.

Utilize Drone-Based EM Scanners

Drone quipped with EM detection technology can scan operational areas in advance to identify suspicious or hostile EM activity. This proactive approach could prevent EM-based threats.

Collaboration with Various Stakeholders

Another strategy for under developed country like Nepal to acquire equipment, technology and training is joint partnership with technologically advanced partners in support of following.

Participate in Joint Training

Engage in joint exercises with countries that have developed EM defence capabilities can provide valuable insights into EM mitigation tactics.

Leverage Expertise from Technology Partners

Work with defence technology firms and cybersecurity experts to develop and implement EM-resistant technologies.

Engage in Intelligence Sharing

Intelligence on EM-based threats and tactics can be invaluable. Partnering with all security agencies within the country can provide with valuable information.

Conclusion

The threat posed by electromagnetic interference and attacks is evolving, and incidents like the alleged Hezbollah pager explosion demonstrate the potential for harm. For the Nepali security agencies, understanding and addressing these vulnerabilities is critical for safeguarding personnel and ensuring operational continuity. By implementing a combination of upgraded equipment, secure protocols, training and collaboration, the Nepali security agencies can mitigate the risks posed by EM threats. As technology advances, continuous assessment and adaptation of these strategies will be necessary to protect against the ever-evolving landscape of EM-based attacks.

References

The Economist (2024 November 2). A pager bomb attack caused disarray for Hezbollah. https://www.economist.com/middle-east-and-africa/2024/09/17/a-pager-bomb-attack-causes-disarray-for-hizbullah

The New York Times (2024 November 5) .Middle East Hezbollah Israel pager Lebanon.https://www.nytimes.com/2024/09/18/world/middleeast/hezbollah-israel-pager-lebanon.html?smid=url-share

Gupta, N. (2019). Electromagnetic Field and Waves. NEW AGE International Publishers.

Electromagnetic pulse (2024 December 23). In Wikipedia. https://en.wikipedia.org/wiki/Electromagnetic_pulse

The week (2024 December 28). China Deploys microwave weapons against Indian troops. https://theweek.com/108688/china-deploys-microwave-weapons-against-indian-troops