Security Council (SC)

Evaluating the severity of using Electromagnetic Warfare

Research Report

Leiden Model United Nations 2024

"Out of this world"

Forum: Security Council (SC)

Issue: Evaluating the effects of Electromagnetic Warfare

Position: Deputy President

Introduction

Electromagnetic warfare (EW) has become an integral part of modern warfare. The ability to disrupt, deceive, and degrade enemy capabilities lies solely in EW. First developed during the world wars, Its capabilities have far exceeded jamming radios. It is providing the potential for smaller more technologically advanced groups to target larger groups who rely on electronic information. EW also allows for stronger groups to dominate information that is critical in times of war. Such as troop movements, which allow for swift action to be taken by those who possess the information.

EW is also used to disable enemy weapon systems rendering them defenceless while the effect is still active. Usually targeting Surface Air Missiles (SAM) and radar systems. However, the risk of collateral damage in EW is not as low as one would assume. Targeting densely habited areas or any urban areas results in critical civilian systems failing. A few consequences this can have are power outages, hospital support systems, and emergency services. These are but a few rendering technologies within a whole area inoperable and can have catastrophic side effects. As well as a high amount of civilian casualties.

This means that although EW is a fast and efficient way to handle military operations. The impact it has on civilians has to be considered. As well as all the infrastructural damage an electromagnetic weapon causes. Especially now with AI evolving at a rapid pace, it is only a matter of time before its involvement in EW. Creating countless privacy and security concerns. Going towards the future the international community needs to work on creating and strengthening guidelines that protect civilians from the use of EW.

Definition of Key Terms

Electromagnetic Warfare:

The strategic use of electromagnetic energy to control the electromagnetic spectrum, attack enemy systems, and protect friendly systems from electronic attacks. EW includes three main components: Electronic Attack (EA), Electronic Protection (EP), and Electronic Warfare Support (ES).

Jamming:

The intentional emission of electromagnetic signals to interfere with the reception of radio or radar signals, thereby disrupting enemy communication or sensor systems.

Interference:

The unintentional or intentional disruption of signals in the electromagnetic spectrum, can degrade or block the performance of communication and sensor systems.

Cybersecurity:

The practice of protecting systems, networks, and data from digital attacks. In the context of EW, cybersecurity intersects with CEMA (Cyber-Electromagnetic Activities), where both cyber and electromagnetic threats can compromise civilian infrastructure, such as power grids or communication networks.

Electromagnetic Pulse:

A burst of electromagnetic radiation. EMPs can cause widespread damage to electronic equipment and

infrastructure, leading to large-scale disruptions in civilian life.

Data Privacy:

The protection of personal and sensitive information from unauthorised access. EW operations that involve interception or jamming of signals can lead to breaches in data privacy, especially in communication networks and devices used by civilians.

General Overview

Electromagnetic warfare (EW) is a crucial aspect of modern military operations, entailing the strategic use of the electromagnetic spectrum (EMS) to outmanoeuvre adversaries. EW encompasses a broad range of activities designed to impede friendly forces from utilising the EMS while impeding, deceiving, or impairing the enemy's capacity to do so. It can be divided into 3 parts. Electronic attack(EA), Electronic protection(EP), and electronic support(ES).

Furthermore, by shielding friendly forces' electronic systems from enemy attack, EW increases their operational efficacy and survivability. This includes defending radar, communications, and other vital systems against direct energy attacks, spoofing, and jamming. EW facilitates information gathering, weapon system targeting, and command and control by guaranteeing dependable access to the electromagnetic spectrum. In the end, the strategic use of EW can tip the scales in a fight, allowing troops to accomplish their goals more quickly and with less risk.

Electromagnetic warfare greatly reduces the number of feeding casualties during an operation. Access to the tool mentioned above makes it possible for swift coordinated strikes that reduce the risk of casualties. However, the number of possible civilian casualties has increased. As well as damage to both infrastructure and all electronics within range. The production and development of these weapons have been increasing and have seen the introduction of AI. This entails countless risks to data and privacy. If it were used it would cause massive problems for civilian life.

Electromagnetic warfare (EW) can have wide-ranging, significant consequences on civilians that frequently go beyond the local battlefield. There can be major societal repercussions when EW operations intentionally or unintentionally destroy civilian infrastructure, such as electricity grids, navigation systems, or communication networks. For example, blocking or jamming communication systems can make it more difficult to respond to emergencies, interfere with public services, and incite widespread fear among the general public. Because we rely on electronic devices and networks in today's heavily interconnected societies, even small-scale EW operations have the potential to have catastrophic consequences, even destroying vital services like banking, transportation, and healthcare. Furthermore, EW's involvement in cyber-electromagnetic activities may result in security lapses affecting civilian data, endangering individual privacy and safety.

A loss of public trust in military and governmental institutions can result from the psychological effects of such interruptions as well as the physical threats provided by malfunctioning infrastructure. This can intensify social unrest and make post-conflict rebuilding efforts more difficult. Therefore, even while EW is an effective weapon in military strategy, using it responsibly necessitates taking into account the possibility of harm to civilians as well as the moral ramifications of impacting or attacking civilian infrastructure.

Electromagnetic attack, protection, and support

Electronic attack (EA) can have a significant negative influence on civilian life, particularly when military operations involve deliberate or inadvertent interference with civilian electromagnetic equipment. EA strategies like electronic deception and jamming can interfere with communication networks, such as those for emergency broadcast systems, mobile phones, and the internet, which can make people anxious and confused. During emergencies, people may find it more difficult to communicate with loved ones, call for help, or get critical information if there are communication disruptions. Moreover, EA has the ability to compromise GPS and other navigation systems, affecting transportation networks, causing accidents, and disrupting the delivery of essential services. Broken

infrastructure not only poses a risk of physical harm but also has the ability to seriously disrupt people's mental health.

Electronic Protection (EP) seeks to shield friendly electromagnetic systems from enemy interference by maintaining critical infrastructure during wartime, hence giving civilians indirect benefits. By protecting communication networks, EP measures help to maintain the flow of information, enabling citizens to be informed and make informed decisions in times of emergency. This protection extends to essential services like healthcare, where consistent communication and reliable access to electronic medical records are vital. Furthermore, EP prevents possible unrest by shielding the financial and transportation industries from disruptions caused by hostile EW activities. The military's communications may, on occasion, be given priority over those on civilian networks as a result of EP deployment; this could restrict bandwidth available to the general population or degrade the quality of services offered.

Since electromagnetic emissions can affect civilians in both positive and bad ways, Electronic Support (ES) is essential to the intelligence-gathering process. Positively, by spotting hostile behaviours before they worsen, ES operations can assist prevent assaults and enhance the safety and security of civilian populations. Nevertheless, the usage of ES also prompts questions regarding privacy and civil liberties since electronic communication monitoring and interception can unintentionally lead to citizen surveillance. Public trust could be damaged by this, particularly if intelligence-gathering operations are thought to be intrusive or carried out uncontrolled. Therefore, even while the deployment of ES is necessary for military situational awareness and operational effectiveness, it must be carefully considered in light of its moral and legal implications.

Infrastructure

As a component of electromagnetic warfare, electronic attack (EA) operations that target essential systems like power grids, transportation, and communication can have a substantial effect on civilian infrastructure (EW). These systems are susceptible to malfunctioning due to jamming or other forms of interference, which can impact everything from air traffic control to emergency response. Wide-ranging service interruptions may arise from this. Such interruptions may have disastrous domino consequences on essential services, leading to accidents, monetary losses, and significant challenges in maintaining public safety and order. In today's closely interconnected world, even small disruptions can have a lasting effect, making recovery efforts more challenging and undermining public confidence in the stability of vital infrastructure.

On the other hand, infrastructure must be protected by Electronic Protection (EP) to prevent the detrimental impacts of EW. By safeguarding critical systems from threats, EP strives to preserve the continuance of essential services during times of conflict or catastrophe, including anything from financial transactions to electricity distribution. But occasionally, the focus on military EP might lead to the reallocation of resources, such as spectrum bandwidth, away from uses by the general public, which could result in a temporary drop in service quality or disruption. As a result, while EP is essential for maintaining the infrastructure's resilience, it also needs to be carefully regulated to balance military goals with the security of civilian systems.

Major Parties Involved

The United States of America

The United States is one of the main players in electromagnetic warfare (EMW) through the Department of Defense (DoD). To preserve its technological edge in combat, the DoD makes significant investments in the creation and application of EW capabilities. The U.S. military uses electronic warfare (EW), a broad strategy, to gather intelligence through electronic monitoring, defend its networks against cyberattacks, and intercept enemy communications. To develop and improve EW systems and make sure they are ready for new challenges in contemporary combat, the DoD also works with tech firms and defence contractors.

North Atlantic Treaty Organisation (NATO)

NATO is vital to standardising and coordinating EW capabilities across its member states. NATO is a military alliance that successfully integrates the EW plans and equipment of its member nations by emphasising the importance of EW in joint operations. The Electronic Warfare Working Group (EWWG) of NATO is tasked with developing common rules, technologies, and guidelines to enhance the alliance's overall EW capabilities. This cooperation allows NATO forces to operate fluidly throughout the electromagnetic spectrum during multinational missions, thereby offering a unified defence against electronic attacks.

Russia

Russia has a long history of using EW tactics, especially in recent conflicts. Their military has invested heavily in advanced EW systems, including powerful jamming devices and cyber warfare capabilities. Russia also prioritises defensive EW measures to protect its own forces and infrastructure. This includes ECM systems and cyber defence measures.

China

China's achievements in electromagnetic technology have had a big impact on its position in the world and on its own country's development. The nation has made significant investments in the study and use of electromagnetic fields, including industrial automation, defence, and telecommunications and transportation. China's application of electromagnetic technology to monitoring and surveillance shows how it might employ these advancements to tighten social control and boost security. Therefore, these achievements not only highlight China's scientific superiority but also raise questions about its ability to influence international standards and practices in electromagnetic applications, potentially changing the global competitive landscape in a number of areas.

Timeline of Events

World War I Use of radio jamming and electronic countermeasures to disrupt enemy communications.

World War II Extensive use of radar and electronic warfare techniques

1950 Development of advanced radar systems and electronic countermeasures for military aircraft and ships.

1962 Cuban Missile Crisis: Use of electronic surveillance to detect Soviet missile installations.

1973 Yom Kippur War: Extensive use of electronic warfare by both sides.

1980 Increased emphasis on electronic warfare in the context of the Cold War.

2000 Increased use of drones and unmanned aerial vehicles (UAVs) with electronic warfare capabilities.

2010 Continued development of advanced EW technologies, including directed energy weapons and cyber warfare capabilities.

2014 Russian annexation of Crimea: Russian use of electronic warfare to disrupt Ukrainian communications.

2015 Syrian Civil War: Extensive use of electronic warfare by various factions.

2022 Russian invasion of Ukraine: Russian use of electronic warfare to disrupt Ukrainian communications and infrastructure.

Possible Solutions

Establishing fundamental principles and fostering international cooperation are essential to addressing the problems caused by electromagnetic warfare (EW). Creating legally binding treaties or agreements that control the use of EW technologies—especially those with offensive potential—is one possible answer. These agreements could include codes of behaviour, restrictions on specific kinds of EW attacks, and terms and conditions for resolving conflicts. An international convention might, for instance, outlaw the employment of EW weapons against vital infrastructure or civilian targets.

Moreover, setting up global forums or organisations devoted to EW could aid in keeping an eye on things, looking at instances, and fostering openness. These groups could provide forums for discussion, compromise, and the creation of shared standards. Increasing diplomatic relations and open communication between countries can also help to lower tensions and reduce escalation in terms of electromagnetic warfare.

Technological innovation is essential for countering EW threats. Investing in research and development to create more effective electronic countermeasures (ECM) and cyber defence technologies can help mitigate the impact of EW attacks. This could involve developing new jamming techniques, encryption algorithms, and intrusion detection systems. Enhancing the resilience of critical infrastructure and systems can also make them less vulnerable to disruption. This could include hardening power grids,

communication networks, and other vital infrastructure against EW attacks. This not only helps in the prevention of external attacks but also prevents instability caused by insurgents and other terrorist organisations.

Promoting technological innovation in EW can lead to the development of new defensive capabilities that can outpace offensive threats. This could involve supporting research and development in emerging technologies such as machine learning and quantum computing.

To prevent the proliferation of EW technologies and reduce the risks associated with their use, international efforts to promote non-proliferation and arms control are essential. This could involve establishing export controls, implementing transparency measures, and promoting the development of international norms and standards. By limiting the spread of EW technologies and preventing their acquisition by non-state actors, nations can help reduce the risks of their misuse.

To solve the problems caused by electromagnetic warfare (EW), we need to work together as a world, develop new technology, and act responsibly. By doing these things, we can make the world safer and more stable.

Sources

Top 10 Northrop Grumman Government Contracts - GovCon Wire. (2022, December 27). Retrieved September 29, 2024, from GovCon Wire website: https://www.govconwire.com/articles/top-10-northrop-grumman-government-contracts/

Administrator. (2023, November 13). Electronic warfare program for Royal Navy warships achieves major milestone - Defence Equipment & Support. Retrieved September 29, 2024, from Defence Equipment & Support website: https://des.mod.uk/electronic-warfare-programme-for-royal-navy-warships-achieves-major-milestone/#:~:text=%E2%80%9CThe%20Royal%20Navy%20has%20invested,that%20will%20allow%20them%20to

ET Online. (2024, February 7). China's electromagnetic warfare game-changer: "Nowhere to hide" for enemy forces. Retrieved September 29, 2024, from The Economic Times website: https://economictimes.indiatimes.com/news/defence/chinas-electromagnetic-

warfare-game-changer-nowhere-to-hide-for-enemy-forces/articleshow/107494144.cms?from=mdr

UNODA – United Nations Office for Disarmament Affairs. (2024). Retrieved September 29, 2024, from Unoda.org website: https://disarmament.unoda.org/

ICRC | International Committee of the Red Cross. (2024, September 27). Retrieved September 29, 2024, from Icrc.org website: https://www.icrc.org/en

CCDCOE - The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary hub of cyber defence expertise. (2024). Retrieved September 29, 2024, from Ccdcoe.org website: https://ccdcoe.org/

Home Page | CISA. (2024, September 25). Retrieved September 29, 2024, from Cisa.gov website: https://www.cisa.gov/

Electronic warfare | Cybersecurity, Jamming, Countermeasures | Britannica. (2024). In *Encyclopædia Britannica*. Retrieved from https://www.britannica.com/topic/electronic-warfare

Wikipedia Contributors. (2024, September 27). Electronic warfare. Retrieved September 29, 2024, from Wikipedia website: https://en.wikipedia.org/wiki/Electronic_warfare

NATO. (2023). Electromagnetic warfare. Retrieved September 29, 2024, from NATO website: https://www.nato.int/cps/en/natohq/topics_80906.htm

What is Electromagnetic Warfare? (2022). Retrieved September 29, 2024, from BAE Systems | United States website: https://www.baesystems.com/en-us/definition/what-is-electromagnetic-warfare

EW-Sea. (2023). Retrieved September 29, 2024, from Lockheed Martin website: https://www.lockheedmartin.com/en-us/capabilities/electronic-warfare.html

adminjem. (2019, September). An Introduction to Jammers and Jamming Techniques - JEM Engineering. Retrieved September 29, 2024, from JEM Engineering website: https://jemengineering.com/blog-an-introduction-to-jammers/#:~:text=The%20two%20main%20jamming%20techniques,common%20type%20of%20repeater%20jamming.