Research Report

LJ EADS, RYAN CLARKE, XIAOXU SEAN LIN

SEPTEMBER 2023

There's Darkness in the Distance: The Rising Threat of China's EMP Weapons to U.S. Defenses and Critical Infrastructure

Table of Contents

Executive Summary

1. **Emerging Technologies in Defense:** The amalgamation of AI, big data, cloud computing, and others, is reshaping the military landscape, with EMP weapons standing out as a modern-day countermeasure.
2. **China's EMP Developments:** China's significant advancements in EMP weaponry portend potential vulnerabilities for U.S. defense mechanisms.
3. **Comparative Defense Analysis:** Just as Taiwan faces challenges from China's EMP threats, Israel too must strategize against regional adversaries potentially armed with China-sourced EMPs.
4. **Patent Analysis Insight:** Wang Yongfang's research unearthed key insights into high-power microwave weapon tech using patent analysis.
5. **Database & Patent Landscape:** The Derwent World Patent Database, housing 337 related patents until October 20, 2018, reveals a dynamic global competitive scene.
6. **China's Leadership in Patents:** Commencing in 2006, China saw a patent surge after 2012, now boasting 37% of total global applications, illustrating both technological and IP maturity.
7. **Focus on Pulse & Microwave Source Technologies:** China's patent focus and breakthroughs, particularly from leading institutions, hint at a long-term vision and strategy.
8. **Microwave Source Devices:** With a vast spectrum including relativistic gyrotrons, these form a bulk of patent applications and depict global competition.
9. **Magnetic Pulse Compressor:** Research on the magnetic pulse compressor reveals its ability to generate impactful electromagnetic pulses. These pulses can critically hamper intelligent military equipment, marking a significant threat to defense strategies.
10. **Silicon Micro-inertial Sensor Vulnerabilities:** Demonstrating the susceptibility of such sensors to EMPs, particularly those pivotal in exoskeleton systems, underscores that many advanced weapons may be defenseless against electromagnetic onslaughts.
11. **Microwave Active Denial System (ADS):** CETC International Co., Ltd. introduced ADS, a non-lethal countermeasure, which, using high-power microwaves, can incapacitate an array of electronic systems, emphasizing the evolution of non-contact warfare techniques.
12. **Significance for U.S. & Allies:** China's technological strides in EMP weaponry is an alarm for U.S. military and civilian assets, demanding understanding, resilience, and countermeasures.
13. **Beyond Taiwan's Defense:** The defense parallels between Israel and Taiwan underscore the need for global collaboration and shared insights in EMP defense mechanisms against common threats.

14. **Future Trends:** China's dedication to lead in high-power microwave weapon tech reveals a broader geopolitical military strategy, signaling shifts in defense paradigms.
15. **Conclusion & Recommendation:** To maintain global stability, nations under potential threat must be vigilant of these tech shifts, reinvest in defense, and advocate for international collaborative efforts against looming threats.

Abstract

The contemporary defense landscape is undergoing transformative changes, spearheaded by the integration of AI, big data, and cloud computing. A particularly compelling development within this paradigm is the rise of Electromagnetic Pulse (EMP) weapons, which present profound strategic implications. China's rapid advancement in this domain, as evidenced by their dominant presence in the global EMP patent landscape and nuanced technological innovations, indicates a potential vulnerability for U.S. and allied defense structures. High-profile research, such as Wang Yongfang's patent analysis, highlights China's concentrated efforts in pulse and microwave source technologies, pointing towards a sustained and strategic EMP weaponization roadmap. Further studies reveal specific technological threats, like the magnetic pulse compressor's capability to disrupt sophisticated military hardware and the vulnerabilities of silicon micro-inertial sensors to EMPs. Moreover, innovations like the Microwave Active Denial System introduce a new dimension to non-contact warfare. Given China's aggressive EMP-centric pursuits, U.S., and its allies, including nations like Taiwan and Israel, need a concerted, collaborative approach to understand, counteract, and potentially co-create defense mechanisms to ensure a balanced global power dynamic.

Introduction

In the modern era of warfare and defense, the confluence of artificial intelligence, big data, cloud computing, and a slew of emerging technologies has revolutionized the paradigm of military strategy and power projection. This fusion not only enables unprecedented data-driven insights and real-time response mechanisms but also introduces novel vulnerabilities in defense architectures. Central among these emergent threats are EMP weapons, which can debilitate intricate electronic systems and render state-of-the-art military equipment ineffective in moments. As EMP weapons become more sophisticated, they are seen as strategic assets, especially when confronting technologically advanced opponents. China, with its concerted efforts in military modernization and technological research, has made remarkable advancements in this field. This amplifies the urgency for the U.S. and its allies to comprehend the full spectrum of threats posed by these weapons. Delving deep into the dynamics of EMP weapons and evaluating their potential impacts is now of paramount importance in shaping U.S. defense policies and strategies.

Electromagnetic Threats & Defense: Exploring Chinese Research on EMP Weaponry

Recent studies from Chinese defense researchers provide valuable insights:

1. **High Power Magnetic Pulse Compressor**: This research elaborates on the operational mechanism of the magnetic pulse compressor. By generating strong electromagnetic pulses, it can interfere or permanently damage sensitive electronic components, presenting a considerable threat to intelligent military equipment.[1]
2. **Damage Effects of EMP on Silicon Micro-inertial Sensor**: The paper demonstrates the susceptibility of silicon micro-inertial sensors, critical components in exoskeleton assist systems, to EMPs. These findings suggest that modern weapons equipped with such sensors are vulnerable to electromagnetic attacks.[2]
3. **Technical Proposal of Microwave Active Denial System**: The CETC International Co., Ltd.'s Microwave Active Denial System (ADS) is a non-lethal technology designed to disrupt electronic control systems using high-power microwaves. Offered in both mobile and portable formats, it can incapacitate vehicle controls, jam

[1] Meng Zhipeng, Li Song, Yang Jie, Zhang Jianghua, "Design and Experimental Research of High Power Magnetic Pulse Compressor," (高功率磁脉冲压缩器的设计及实验研究), Journal of Ordnance and Equipment Engineering, Issue 7, 2020, (1. Institute of National Defense Science and Technology Innovation, Academy of Military Sciences, Beijing 100071; 2. School of Advanced Interdisciplinary Sciences, National University of Defense Technology, Changsha 410073). Published on 2020-08-05 06:32.

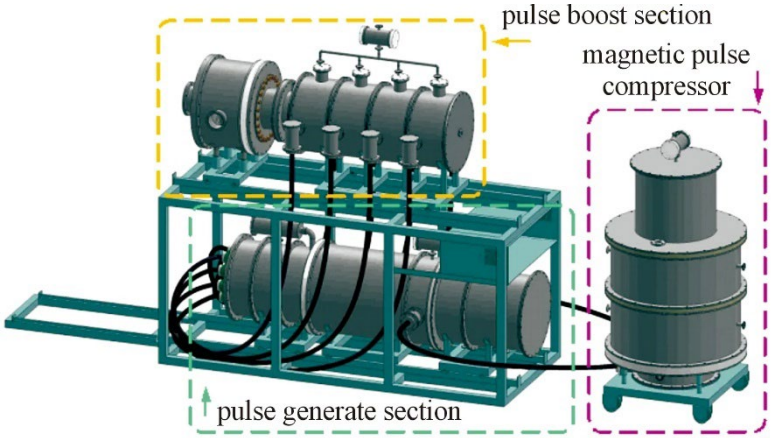
[2] Shen Jie, Pan Xuchao, Fang Zhong, He Yong, Chen Hong, Zhang Jiangnan, Shi Yunlei, "Study on the Damage Effect of Intense Electromagnetic Pulse on Silicon Micro-inertial Sensor," (强电磁脉冲对硅微惯性传感器的损伤效应研究), Journal of Military Engineering, Issue 6, 2020, (1. National Defense Key Discipline Laboratory of Intelligent Ammunition Technology, Nanjing University of Science and Technology, Nanjing, Jiangsu 210094; 2. Quality Safety Testing Center, Fifth Electronic Research Institute, Ministry of Industry and Information Technology, Guangzhou, Guangdong 510610). Published on 2020-07-21 09:44.

communication devices, and disable various electronic equipment without physical contact.[3]

High Power Magnetic Pulse Compressor[4]

In a 2020 paper titled **"Design and Experimental Research of High-Power Magnetic Pulse Compressor"** from the *Journal of Ordnance and Equipment Engineering*, researchers Meng Zhipeng, Li Song, Yang Jie, and Zhang Jianghua from the Institute of National Defense Science and Technology Innovation and the National University of Defense Technology presented their design and research on a high-power magnetic pulse compressor.

With rapid advancements in technologies like artificial intelligence, cloud computing, and autonomous control, the application and research into intelligent equipment in military operations have surged. One crucial aspect of this is the use of strong electromagnetic pulses, which can interfere with or even permanently damage electronic circuits within weapon systems. High-power pulse technology has emerged as a critical method to generate these electromagnetic pulses. Magnetic pulse compressors, in particular, are attracting significant interest because of their solid-state operation, high power capacity, reliability, and longevity.



Schematic diagram of the experimental device described in "Design and Experimental Research of High Power Magnetic Pulse Compressor"

The team's research centered on a two-stage magnetic pulse compressor that used an iron-based amorphous magnetic core. Through experimental verification, they showcased the efficiency of this compressor in generating high-power pulses. Their design showcased the ability to transform a sine wave electric pulse with a 19 μs rise time into one with about a 1 μs rising edge and a peak voltage of about 100 kV. The compressor could stably operate at a repetition frequency of 20 Hz, making it suitable for applications in high-power microwave drives, high-energy laser pumps, and plasma physics.

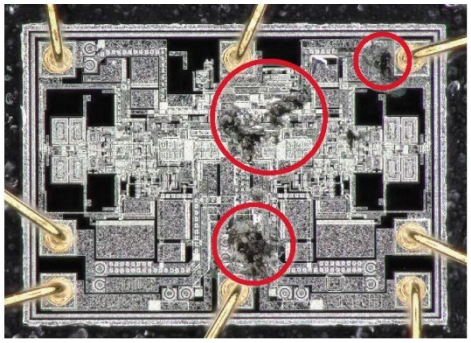
This technology holds potential military implications. If weaponized, EMP technology can disable electronic equipment, neutralize defense systems, and cripple communications. This could be particularly concerning in scenarios where an adversary could use EMPs as a preliminary strike to incapacitate defensive capabilities of a nation or an ally, like Taiwan, before launching a more conventional attack.

[3] CETC International Co., Ltd., "TECHNICAL PROPOSAL OF MICROWAVE ACTIVE DENIAL SYSTEM," June 2017. CETC Mansion, No. 5 Wulutong North Street, Xicheng District, Beijing, China 100120.

[4] Meng Zhipeng, Li Song, Yang Jie, Zhang Jianghua, "Design and Experimental Research of High Power Magnetic Pulse Compressor," (高功率磁脉冲压缩器的设计及实验研究), Journal of Ordnance and Equipment Engineering, Issue 7, 2020, (1. Institute of National Defense Science and Technology Innovation, Academy of Military Sciences, Beijing 100071; 2. School of Advanced Interdisciplinary Sciences, National University of Defense Technology, Changsha 410073). Published on 2020-08-05 06:32.

Damage Effects of EMP on Silicon Micro-inertial Sensor[5]

In another recent article titled **"Study on the Damage Effect of Intense Electromagnetic Pulse on Silicon Micro-inertial Sensor"** in the *Journal of Military Engineering, Issue 6, 2020*, Shen Jie, Pan Xuchao, Fang Zhong, He Yong, Chen Hong, Zhang Jiangnan, and Shi Yunlei from the National Defense Key Discipline Laboratory of Intelligent Ammunition Technology and the Quality Safety Testing Center presented their findings on the damage effects of intense electromagnetic pulses on silicon micro-inertial sensors.



Intense electromagnetic pulse induced burn marks on MEMS sensor described in the "Study on the Damage Effect of Intense Electromagnetic Pulse on Silicon Micro-inertial Sensor"

Modern warfare is witnessing an evolution with the advent of advanced technologies and their applications, such as individual exoskeleton booster systems, which rely heavily on MEMS sensors. These sensors are responsible for sensing real-time motion information, feeding it back to control systems, and are thus vital for the operation of these exoskeleton systems. However, their exposure to high-altitude nuclear electromagnetic pulses (HEMP) can have detrimental effects. Such pulses can introduce high-voltage, high-current instantaneous impacts through direct cable connections to the sensors, leading to transient interference or even irreversible physical damage.

This study delved into the theoretical analysis of these impacts, focusing on the silicon micro-inertial sensor. Using a transmission line model, the researchers explored how strong electric pulses could be coupled and transmitted through direct sensor connections in the event of a HEMP. By simulating and testing the damage thresholds, they found that at a pulse voltage amplitude of 780 V and a pulse current amplitude of 4.23 A, the sensor suffered irreparable physical damage. This threshold indicates the sensor's vulnerability to electromagnetic pulses in warfare scenarios.

Furthermore, the research pinpointed the primary components at risk within these sensors: the front-end capacitor and the signal amplifier. The primary modes of damage observed were high-voltage breakdown of the capacitor and high-current burnout of the amplifier.

In conclusion, this paper sheds light on the vulnerabilities of silicon micro-inertial sensors within advanced exoskeleton systems in a high-electromagnetic pulse environment. The findings underscore the need for enhanced protective measures and the reconsideration of design aspects for such sensors, given their critical role in modern military applications.

---

[5] Shen Jie, Pan Xuchao, Fang Zhong, He Yong, Chen Hong, Zhang Jiangnan, Shi Yunlei, "Study on the Damage Effect of Intense Electromagnetic Pulse on Silicon Micro-inertial Sensor," (强电磁脉冲对硅微惯性传感器的损伤效应研究), Journal of Military Engineering, Issue 6, 2020, (1. National Defense Key Discipline Laboratory of Intelligent Ammunition Technology, Nanjing University of Science and Technology, Nanjing, Jiangsu 210094; 2. Quality Safety Testing Center, Fifth Electronic Research Institute, Ministry of Industry and Information Technology, Guangzhou, Guangdong 510610). Published on 2020-07-21 09:44.

Technical Proposal of Microwave Active Denial System[6]

The Microwave Active Denial System (ADS) developed by CETC International Co., Ltd. represents a cutting-edge application of high-powered microwaves to target and disrupt electronic control systems. Available in both mobile and portable iterations, this system is designed with a broad range of applications, from incapacitating vehicle controls to jamming communication devices and deactivating various other electronic apparatus. The potential risks associated with the deployment of such technology are manifold. Foremost among these is the ability to disrupt military assets, with the system potentially being deployed to jam or disable critical communication systems, thus impeding the coordination capabilities of the U.S. and its allies. Additionally, the technology could neutralize electronic surveillance and security protocols at critical installations like military bases or checkpoints, leaving them exposed to breaches. Beyond the military spectrum, the broader economic and civilian landscape is also vulnerable. Critical infrastructure, including power grids, transportation hubs, and communication networks, could be targeted, instigating widespread chaos and significant economic repercussions.

Fig. 5 Typical Photo of Portable Microwave ADS

Portable Microwave Active Denial System (ADS) developed by CETC International Co., Ltd.

Focusing on the geopolitical theater of Taiwan, the deployment of the ADS could serve as a pivotal precursor to an invasion. By incapacitating Taiwan's communication infrastructures, defense forces would be left disoriented, leading to delayed response times. This disruption extends to Taiwan's electronic-dependent defense assets, such as missile systems and radars, which could be rendered ineffective. In tandem with military operations, the civilian domain could be thrown into disarray by disabling urban electronic systems, fostering panic and misdirection. Furthermore, this system could act as a deterrent to international intervention. The U.S. or allied forces rushing to Taiwan's defense could find their communication or transport systems compromised, causing delays and hindering mobilization efforts. Given this spectrum of risks and potential applications, it is paramount for the U.S. and its allies to prioritize the development of counterstrategies and protective measures against the impacts of such disruptive technologies.

Portable Microwave Active Denial System (ADS) developed by CETC International Co., Ltd.

Moreover, the potential deployment of Chinese spy balloons equipped with EMP devices poses a direct threat beyond the immediate vicinity of Taiwan. If launched to float over U.S.

[6] CETC International Co., Ltd., "TECHNICAL PROPOSAL OF MICROWAVE ACTIVE DENIAL SYSTEM," June 2017. CETC Mansion, No. 5 Wulutong North Street, Xicheng District, Beijing, China 100120.

territories, these balloons could act as covert delivery mechanisms for EMP detonations, severely compromising the nation's critical infrastructures and defense readiness. This elevated risk highlights the urgency for advanced surveillance, detection, and neutralization methods to safeguard against such aerial threats.[7] CETC was among the Chinese companies the Biden administration blacklisted for providing "support" to the People's Liberation Army's balloon surveillance programs.[8] [9]

ADS and CCP NeuroStrike: A New Clandestine Deployment Mode

The ADS also has implications for the Chinese Communist Party's NeuroStrike program[10]. Unknown to many, the Chinese Communist Party (CCP) and its People's Liberation Army (PLA) have established themselves as world leaders in the development of NeuroStrike weapons. These platforms directly attack, or even control, mammalian brains (including humans) with microwave/directed energy weapons via standalone platforms (i.e., handheld gun) or the broader electromagnetic spectrum.[11] NeuroStrike, as defined by McCreight, refers to the engineered targeting of warfighter and civilian brains using distinct non-kinetic technology to impair cognition, reduce situational awareness, inflict long term neurological degradation and fog normal cognitive functions.[12] The CCP views NeuroStrike and psychological warfare as a core component of its asymmetric warfare strategy against the United States and its Allies in the Indo-Pacific.

NeuroStrike is part of the CCP's standard order of battle; not an unconventional set of

---

[7] Cohen, Ariel. "Protecting America's Power Grids From EMP Attacks." FORBES BUSINESS ENERGY. https://www.forbes.com/sites/arielcohen/2023/03/20/deflating-the-emp-danger-to-americas-power-grids/?sh=68fe68f92050, 2023-03-20

[8] Andrew W. Lehren, Dan De Luce and Yasmine Salam, U.S. firm's subsidiary sold electronics to Chinese defense firm linked to spy balloon program, https://www.nbcnews.com/news/us-firms-subsidiary-sold-electronics-chinese-defense-firm-linked-spy-b-rcna72712, 2023-03-06

[9] Bureau of Industry and Security, Commerce Adds Six to Entity List for Supporting PRC Military Modernization, Intelligence, and Reconnaissance Activities, https://www.bis.doc.gov/index.php/documents/about-bis/newsroom/press-releases/3220-2023-02-10-bis-press-release-six-prc-entities-final-3/file, 2023-02-10

[10] For more information, please see Ryan Clarke, Xiaoxu Sean Lin and LJ Eads, "Enumerating, Targeting and Collapsing the Chinese Communist Party's NeuroStrike Program Aggregating Intelligence Fragments and the Power of Network Graphs', CCP BioThreats Initiative.
Enumerating, Targeting and Collapsing the Chinese Communist Party's NeuroStrike Program — The CCP BioThreats Initiative

[11] For empirical examples of such research, please see Yanyun Lin, et. al., 'Effects of Long-Term Exposure to L-Band High-Power Microwave on the Brain Function of Male Mice', *BioMed Research International*, Volume 2021, Article ID 2237370.
Wei-Jia Zhi, et. al., 'Recent advances in the effects of microwave radiation on brains', *Military Medical Research*, Volume 4, No. 29, 2017.
Mark Hodge, 'Inside China's terrifying 'brain control weapons' capable of 'paralyzing enemies'', The Sun, 31 December 2021.
Ryan Morgan, 'China creating 'brain-control weapons' and weaponizing biotech, US says', American Military News, 17 December 2021.
Similar research is also being conducted in Russia. Please see A.V. Kereya, et. al., 'Laboratory Mice are Stressed After Exposure to Nanosecond Repetitive Pulsed Microwaves', *ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ – ФИЗИКА*, Vol. 59, No. 9/2, 2016.
A.V. Kereya, et. al., 'Some biological reactions of the organism after exposure to nanosecond repetitive pulsed microwaves', 6th International Congress 'Energy Fluxes and Radiation Effects', *IOP Conf. Series: Journal of Physics*, Conference Series 1115, 2018.

[12] Robert McCreight, 'Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat', *Small Wars Journal*, 16 September 2022.

capabilities only to be used under extreme circumstances. This represents a fundamental difference in strategic thinking regarding these domains in Beijing. This is not a hypothetical point. There was a sharp statistical increase in Chinese military activity in the South China Sea, East China Sea, Taiwan Straits, and along the Sino-Indian border during the most acute phases of the COVID-19 outbreak in 2020 and 2021.[13]

However, the CCP's weaponization of neuroscience extends well beyond the scope and understanding of classical microwave weapons. Their new landscape of NeuroStrike development includes using massively distributed human-computer interfaces to control entire populations as well as a range of weapons designed to cause cognitive damage.[14] These research programs are not obscure 'moonshots'; they are core strategic focus areas that are designed to be utilized over the near-term and within current state strategic circumstances, such as in Taiwan. Any breakthrough in this research would provide unprecedented tools for the CCP to forcibly establish a new world order, which has been Xi Jinping's lifelong goal.

ADS likely represents the next generation of technological development in the NeuroStrike domain. As ADS is the size of a suitcase, it can be clandestinely deployed across a range of environments, such as outside an airfield fence or in the immediate vicinity of a critical defense or intelligence installation. ADS could be used for targeting personnel and electronic equipment and systems covertly. CETC openly states in its product report for

---

[13] For more in-depth discussions and empirical examples, please see Ryan Clarke, 'Is China Converting COVID-19 Into a Strategic Opportunity?'. EAI Background Brief No. 1545, East Asian Institute, National University of Singapore, 9 July 2020.
Ryan Clarke, 'China-India Border Conflicts: Geopolitical and Environmental Drivers and New Partnership Modalities', EAI Background Brief No. 1554, East Asian Institute, National University of Singapore, 27 August 2020.

[14] For more in-depth Chinese discussions on psychological warfare, please see Tianliang Xiao [肖天亮], eds., *The Science of Military Strategy* [战略学]. PLA National Defence University Press, Beijing, 2015.
Jieming Wu [吴杰明] and Zhifu Liu [刘志富], *An Introduction to Public Opinion Warfare, Psychological Warfare, [and] Legal Warfare* [舆论战心理战法律战概论], PLA National Defence University Press, Beijing, 2014.
Academy of Military Science Military Strategy Research Department [军事科学院军事战略研究部], eds., *The Science of Military Strategy* [战略学]. Military Science Press, Beijing, 2013.
Baocun Wang and Fei Li, "Information Warfare," *Liberation Army Daily by Federation of American Scientists*, June 1995.
For more in-depth international discussions on Chinese psychological warfare, please see Kerry Gershanek, *Political Warfare: Strategies for Combatting China's Plan to "Win without Fighting"*, Marine Corps University Press, 2020.
Michael Clarke, "China's Application of the 'Three Warfares' in the South China Sea and Xinjiang", *Orbis*, January 2019.
Matthew Brazil and Peter Mattis, *Chinese Communist Espionage: An Intelligence Primer*, Naval Institute Press, 2019.
Doug Livermore, "China's "Three Warfares" In Theory and Practice in the South China Sea", *Georgetown Security Studies Review*, 25 March 2018.
Jason Fritz, *China's Cyber Warfare: The Evolution of Strategic Doctrine,* Lexington Books, 2017.
Elsa Kania, "The PLA's Latest Strategic Thinking on the Three Warfares", *China Brief*, Vol. 16, Iss. 13, 22 August 2016.
United States Department of Defence, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2011", 2011.

For an authoritative discussion on Soviet methods of psychological warfare that formed the foundation of China's own capabilities, please see Tomas Schuman (Yuri Bezmenov), *Bezemenov World Thought Police*, Facsimile Publisher, 1986.

ADS that it is specifically designed for covert uses to target individuals and systems without physical contact.[15]

Analysis of High-Power Microwave Weapon Technology Development based on Patent Analysis[16]

In an endeavor to comprehensively understand the growth trajectory of high-power microwave weapon technology across the globe, Wang Yongfang, Yu Binkai, and Wang Lingyun undertook an exhaustive patent analysis using the **Derwent World Patent Database**. The search, which was capped on October 20, 2018, returned a total of 337 patents.

China's Dominance:
One of the most notable findings from the analysis is China's escalating dominance in the domain. The genesis of related patent applications in China can be traced back to 2006, but the explosion in numbers commenced post-2012. Accounting for an impressive 37% of the total global applications, China leads with 124 patents. This trend is indicative of two critical insights: China's technological breakthroughs in the realm of high-power microwave technology and the nations progressively refined intellectual property system.

Details on Chinese Patents:
The crux of China's patent applications revolves around high-power pulsed power sources and high-power microwave source technologies, comprising 30% and 55% of the country's total applications in this sphere, respectively. Leading the research wave are institutions such as the **China Academy of Engineering Physics** and the **University of Electronic Science and Technology of China**. They've recorded significant advancements in high-power pulse power sources and high-power microwave sources.

Breaking down the applications, the most populous subset pertains to high-power microwave source devices, totaling 124 items. These devices span a broad spectrum including relativistic gyrotrons, relativistic magnetrons, relativistic echo tubes, relativistic klystrons, magnetic insulation oscillators, and virtual cathode oscillators. Primarily, China and Russia emerge as the key players in high-power microwave source device patents. China, in particular, spearheaded by institutions like the **China Academy of Engineering Physics**, has patented technologies associated with virtual cathode oscillators and diverse relativistic microwave devices.

Global Perspective:
Globally, the major innovators hail from the U.S., Europe, and China. The top ten includes three U.S. entities: the **U.S. Army**, the **U.S. Department of Energy**, and **Raytheon**. China contributes four entities, with the **China Academy of Engineering Physics** leading with 54

[15] CETC International Co., Ltd., "TECHNICAL PROPOSAL OF MICROWAVE ACTIVE DENIAL SYSTEM," June 2017. CETC Mansion, No. 5 Wulutong North Street, Xicheng District, Beijing, China 100120.
[16] Wang Yongfang, Yu Binkai, Wang Lingyun, "Research on the development of high power microwave weapon technology based on patent analysis," (基于专利分析的高功率微波武器技术发展研究), Aviation Weapons, Issue 5, 2019, (1. China Academy of Aerospace Systems Science and Engineering, Beijing 100048; 2. Beijing Institute of Aerospace Propulsion, Beijing 100076). Published on 2019-11-22 07:47.

patent applications, closely followed by institutions like the **National University of Defense University** and **Northwest Institute of Nuclear Technology**.

Conclusion:
China's rapid rise in patent applications for high-power microwave weapon technology, particularly in high-power pulsed power source and high-power microwave source technologies, underscores its assertive move to the forefront of global technological innovation in this arena. The strategic and concentrated efforts of institutions such as the China Academy of Engineering Physics not only illuminate China's research prowess but also indicate the shifting global balance in advanced military technological capabilities.

China's Advancements in EMP Countermeasures for Systemic Protection

In a report titled **"Research on Strong Electromagnetic Pulse Protection of Hardened Computer Interface"** from the **706th Institute of the Second Academy of China Aerospace Science and Industry**, researchers highlighted the growing threat posed by strong EMPs to electronic information systems. As EMP technologies such as super tube rectifiers and relativistic magnetrons advance, the vulnerability of hardened computers, which are pivotal in these systems, is accentuated. These pulses, possessing extensive power and wide spectrums, can lead to significant damage, potentially rendering electronic information systems temporarily or permanently inoperable. A focal point of the research was on pulses like the HEMP, which has a broad spectrum threatening even hardened computers. The report underscored the importance of enhancing EMP protective measures, especially for computer interfaces such as antennas and transmission lines. Notably, among the interfaces for these computers, there's a reference to the GPS antenna interface, hinting at China's interest in shielding GPS systems from EMP disruptions.[17]

The paper titled **"Aircraft EMP Reinforcement Technology"** by **Aviation Industry Chengdu Aircraft Co., Ltd.** highlights the growing influence of electromagnetic pulse (EMP) technology on modern life and its potential detrimental effects on flight equipment. Aircraft, being crucial transportation means, have sensitive systems that can be heavily disrupted by strong electromagnetic disturbances, such as those from nuclear explosions or lightning. A significant concern is the disruption or failure of engine control, vital for aircraft operation, which can result in temporary or permanent loss of aircraft functionality. The study delves into enhancing the aircraft's defense capabilities against EMPs, with a specific focus on the engine's electronic control system. Through simulations and calculations, the paper examines disturbance waveform parameters at the device port, validating the effectiveness and feasibility of the proposed EMP reinforcement plans. These findings provide guidance for the design and operation of EMP-reinforced aircraft.[18]

---

[17] Research on Strong Electromagnetic Pulse Protection of Hardened Computer Interface (加固计算机接口的强电磁脉冲防护研究*). Ship Electronic Engineering 2020 Issue 4. The 706th Institute of the Second Academy of China Aerospace Science and Industry, Beijing 100854.

[18] Aviation Industry Chengdu Aircraft Co., Ltd., Aircraft EMP Reinforcement Technology (飞机EMP加固技术), Think Tank Times, 2018-12-01

China is proactively investing in technologies to shield its aviation assets from the detrimental effects of EMPs. By emphasizing the need for reinforced engine control systems in aircraft, China acknowledges the potential threats posed by EMP disturbances. The research underscores China's intention to ensure its aircraft remain operational in high-intensity electromagnetic environments, highlighting their commitment to advancing countermeasures for national defense and transportation security.

Implications for U.S. Defenses

Aircraft Vulnerabilities: A Deep Dive into Modern U.S. Aircraft Systems

Modern U.S. aircraft, such as the F-22 Raptor, F-35 Lightning II, and B-21 Raider, stand as epitomes of cutting-edge aerospace engineering. Central to their unparalleled capabilities are the advanced electronic systems they house. These aren't just any electronics; they are the heart and brain of these formidable flying machines, coordinating everything from precision targeting to stealth capabilities.

1. **Micro-Electro-Mechanical Systems (MEMS) Sensors:** MEMS sensors are micro-sized devices that combine mechanical and electrical components. On aircraft like the F-35, they play pivotal roles in functions such as:

- **Navigation:** MEMS gyroscopes provide information about the aircraft's orientation in space. They help ensure the aircraft is flying on the correct path and assist pilots during challenging maneuvers.[19]
- **Weapon Systems:** MEMS accelerometers can detect rapid changes in speed, crucial for missile guidance systems. A slight interference in these can lead to a significant deviation from the intended target.[20]
- **Flight Safety:** MEMS pressure sensors monitor various systems, from cabin air pressure to hydraulic systems, ensuring optimal and safe operations.[21]

2. **Advanced Radar and Stealth Systems:** These aircraft are equipped with radar systems like the AN/APG-77 (F-22) or the AN/APG-81 (F-35) that give them superior situational awareness and targeting capabilities. Disruption of these radars could blind the aircraft in combat scenarios.[22] [23]

Moreover, the aircraft's stealth capabilities rely on carefully designed electronic systems that reduce their radar cross-section. Damage or interference to these systems can compromise an aircraft's stealth, making it an easier target for adversaries.[24]

---

[19] Gardner, J. W., & Varadan, V. K. (Eds.). (2012). Microsensors, MEMS, and smart devices. John Wiley & Sons.
[20] Nguyen, C. T. C. (1999). MEMS technology for timing and frequency control. IEEE transactions on ultrasonics, ferroelectrics, and frequency control, 54(2), 251-270.
[21] Purtova, T., & Schumacher, H. (2013). Overview of RF MEMS technology and applications. In D. Uttamchandani (Ed.), Handbook of MEMS for Wireless and Mobile Applications (pp. 3-29).
[22] Skolnik, M. I. (2008). Introduction to radar systems. Tata McGraw-Hill Education.
[23] Pace, P. E. (2004). Detecting and classifying low probability of intercept radar. Artech house.
[24] Knott, E. F., Shaeffer, J. F., & Tuley, M. T. (2004). Radar cross section. SciTech Publishing.

3. **Electronic Warfare (EW) and Countermeasures:** Aircraft like the F-22 and F-35 have integrated EW systems designed to detect, deceive, and defeat enemy radar and missile systems. A malfunction in these systems due to external interference could expose the aircraft to potential threats.[25] [26]

4. **Communication Systems:** The onboard communication systems allow these aircraft to connect with ground control, other aircraft, and even satellites. Disruption in communication can isolate the aircraft, making coordinated operations with ground or naval forces impossible.[27] [28]

5. **Engine Control Systems:** Modern jet engines, like the F135 engine in the F-35, are not just about thrust. They're governed by intricate electronic systems that manage everything from fuel-air mixture to thrust vectoring. A compromised engine control system could lead to catastrophic engine failure.[29] [30]

In essence, while these advanced electronic systems provide U.S. state-of-the-art aircraft with unmatched capabilities, they also present potential vulnerabilities. Any interference, whether from electromagnetic pulses, cyber-attacks, or direct physical damage, could incapacitate these flying marvels. As military technology continues to evolve, so too will the need to safeguard these electronic components and systems from emerging threats.[31] [32]

Global Airfields: Assessing Vulnerabilities in the Face of EMP Threats

Airfields across the globe act as vital nodes in the international aviation infrastructure, enabling everything from commercial air travel to strategic military operations. Within this context, the rising concern about EMP weapons, particularly those of more compact, discreet designs like suitcase-sized variants, presents a clear and pressing threat. An EMP attack targeting an airfield could create cascading effects that extend far beyond the immediate vicinity.[33] [34] [35]

1. **Air Traffic Control Systems:** At the heart of every airfield is its Air Traffic Control (ATC) system, which ensures the safe and efficient movement of aircraft both in the air and on the ground.

---

[25] Adamy, D. (2009). EW 101: A first course in electronic warfare. Artech House.
[26] Adamy, D. (2001). EW 102: A second course in electronic warfare. Artech House.
[27] Richharia, M., & Westbrook, L. (2012). Satellite systems for personal and broadband communications. Springer Science & Business Media.
[28] Titz, D., Lapini, A., & Robertazzi, T. (2015). Wireless Communication Electronics by Example. Springer.
[29] Patterson, M. A., & Ray, A. (2001). PCA-based bounds for direct adaptive control and performance improvement. International Journal of Control, 74(18), 1773-1783.
[30] Cook, M. V. (2013). Flight dynamics principles: a linear systems approach to aircraft stability and control. Butterworth-Heinemann.
[31] Giri, D. V., & Tesche, F. M. (2004). Classification of intentional electromagnetic environments (IEME). IEEE transactions on electromagnetic compatibility, 46(3), 322-328.
[32] Radasky, W. A., & Wik, M. W. (1994). An introduction to high-power electromagnetics. IEEE Transactions on Electromagnetic Compatibility, 36(4), 311-321.
[33] Button, K. (2009). Air transport networks: Theory and policy implications. Edward Elgar Publishing.
[34] Giri, D. V. (2017). High-power electromagnetic radiators: Nonlethal weapons and other applications. Harvard University Press.
[35] Graham, W. R. (2008). Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.

- **Navigation Systems:** Modern airfields use Instrument Landing Systems (ILS) and Ground-Based Augmentation Systems (GBAS) for precision landing. An EMP strike can distort or entirely disable these systems, leading to disruptions in landings and take-offs.[36]
- **Communication:** Controllers rely on sophisticated communication systems to direct aircraft. EMP interference can lead to loss of communication, potentially causing collisions or misdirection. [37]

2. **Runway Lighting and Operations:** Illuminated runways are essential for nighttime or low-visibility operations. An EMP event could plunge runways into darkness, halting airfield operations entirely.[38]

3. **Aircraft Ground Operations:** Aircraft on the ground rely on various systems for refueling, maintenance, and cargo handling.[39]

- **Fuel Systems:** Automated systems control fuel storage and distribution. EMP damage could lead to fuel delivery issues or even potential spillages and fires.
- **Maintenance Equipment:** Modern aircraft require specialized electronic maintenance tools. EMP damage could stall essential repair and maintenance operations.

4. **Security and Surveillance Systems:** Airfields employ numerous electronic security systems, from CCTV cameras to access control systems at entry and exit points. An EMP attack can disable these, leaving airfields vulnerable to secondary physical or cyber-attacks.[40]

5. **Backup Power Systems:** While airfields often have backup power systems in case of outages, EMPs can disable both primary and backup systems, leading to a total operational shutdown.[41]

The prospect of covert EMP attacks on airfields is alarming. Disabling an airfield, even temporarily, can critically impact not only commercial aviation but also the operational readiness and response times of military forces. As such, understanding these vulnerabilities and investing in EMP-resistant infrastructure becomes paramount for nations looking to safeguard their skies and strategic interests.[42]

Critical Infrastructure: Evaluating the Risks of EMP Disruptions

The backbone of modern society, particularly in countries like the U.S., is the intricate network of critical infrastructure. These infrastructures, heavily intertwined and reliant on sophisticated electronic systems, play pivotal roles in maintaining societal order and ensuring

[36] Eurocontrol. (2019). Challenges of Growth 2018: Keeping Europe's Air Traffic in Motion. Eurocontrol.
[37] Garland, T. B., & Hopkin, V. D. (2018). Air traffic control: Human performance factors. Routledge.
[38] ICAO. (2018). Aerodrome Design Manual, Part 4 – Visual Aids. International Civil Aviation Organization.
[39] Khan, S. (2016). Ground Handling at Airports: Processes, Systems, and Strategies. Routledge.
[40] Price, J., & Forrest, J. (2016). Practical Aviation Security: Predicting and Preventing Future Threats. Elsevier.
[41] Billinton, R., & Allan, R. N. (2014). Reliability evaluation of power systems. Springer.
[42] Radasky, W. A., Wik, M. W., & Kappenman, J. G. (2017). Effects of intense electromagnetic fields on electronics, and methods of protection. IEEE Transactions on Electromagnetic Compatibility, 59(6), 1727-1741.

uninterrupted daily operations. However, the growing threat of EMP attacks could jeopardize these systems, leading to systemic failures with catastrophic consequences.[43] [44]

1. **Power Grids:** The energy sector, specifically the electrical power grid, forms the lifeblood of contemporary civilizations.

- **Generation and Transmission:** Power plants, substations, and high-voltage transmission lines rely on electronic control systems. An EMP event could destabilize power generation, leading to widespread blackouts.[45]
- **Grid Control Systems:** Advanced grid management systems maintain a balance of power supply and demand. A disruption can lead to grid overloads or underloads, causing equipment failures.[46]

2. **Communication Networks:** From emergency services to everyday communications, a functioning network is indispensable.

- **Cell Towers and Data Centers:** EMP attacks can damage cellular infrastructure and data storage hubs, crippling both mobile and wired communications.[47]
- **Satellite Communications:** While satellites might be less susceptible to ground-based EMPs, ground stations and satellite control networks can still be targeted, disrupting GPS, weather forecasts, and satellite-based communications.[48]

3. **Transportation Systems:** Modern transportation is more than just vehicles; it's about interconnected networks and automation.

- **Rail Systems:** Modern trains and subways rely on electronic signaling and automated control systems. EMP-induced failures could result in train collisions or stranded passengers.[49]
- **Air Traffic:** As previously discussed, EMP can severely impair airfields, but it can also disrupt in-flight communication and navigation for aircraft.[50]
- **Road Traffic Control:** Traffic lights, electronic signage, and vehicle communication systems ensure smooth traffic flow. Their failure could result in widespread traffic jams or accidents.

4. **Financial Institutions:** The economy hinges on the electronic processing of transactions.

[43] U.S. Congress. (2008). EMP Commission Report. Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack.
[44] Baker, D. N., & Li, X. (2018). Intense space weather storms and security of critical infrastructure. Space Weather, 16(3), 288-291.
[45] U.S. Department of Energy. (2017). Electromagnetic Pulse Resilience Action Plan.
[46] Kundur, P. (2014). Power system stability and control. McGraw-hill.
[47] Freeman, R. L. (2017). Telecommunication system engineering. John Wiley & Sons.
[48] Peuhkuri, M. (2016). A survey of network threats and defenses. ACM Computing Surveys (CSUR), 49(4), 1-32.
[49] U.S. Department of Transportation. (2016). Intelligent Transportation Systems Joint Program Office - Impacts of Electromagnetic Pulse on ITS.
[50] Ortúzar, J. D. D., & Willumsen, L. G. (2011). Modelling transport. John Wiley & Sons.

- **ATMs and Electronic Transactions:** With ATMs malfunctioning and online transactions halted, there would be a rush on physical bank locations and potential for financial panic.[51]
- **Stock Exchanges:** Electronic trading systems could be incapacitated, causing market crashes and significant economic aftershocks.[52]

5. **Emergency Services:** Reliable communication is paramount for police, fire, and medical services.

- **Dispatch Systems:** EMP can disrupt emergency dispatch centers, delaying response times during crises.[53]
- **Hospital Equipment:** Essential life-saving equipment in hospitals, from monitors to ventilators, could fail, putting countless lives at risk.[54]

The potential devastation of an EMP attack on U.S. critical infrastructure is profound. The intertwined nature of these systems means that the failure of one could cascade to others. As society becomes increasingly digitized, addressing these vulnerabilities and reinforcing infrastructure against EMP threats becomes an imperative for national security, economic stability, and the very fabric of daily life.

Beyond Taiwan and Israel: A Global Perspective on EMP Threats

In the modern era of interconnected geopolitics, the ramifications of EMP threats transcend regional boundaries and individual nation-states. Countries like Taiwan and Israel, despite being geographically distinct, face shared vulnerabilities when it comes to the proliferation of such disruptive technologies. As the global landscape shifts with emerging alliances and threats, understanding the ripple effects of localized EMP attacks becomes paramount.

While the defense of Taiwan is pressing, given its strategic location and importance in global supply chains, Israel's situation offers another lens through which to understand the global EMP threat matrix. Israel, situated in a volatile region, is surrounded by potential adversaries. The nation's strategic significance and geopolitical tensions make it a potential target for EMP attacks. Furthermore, with the increasing indications of neighboring nations acquiring advanced weaponry, potentially through collaborations or transactions with nations like China, the urgency to defend against EMP threats escalates.

For instance, a disruption in Taiwan's electronic manufacturing operations due to an EMP attack could send shockwaves through global technology markets. Similarly, an EMP-induced paralysis of Israel's critical infrastructures could further destabilize an already fragile Middle East, potentially spiraling into larger conflicts with wider-reaching implications.

---

[51] Lenz, R. (2016). IT Risks in financial services institutions. In Enterprise Risk Management Models (pp. 109-125). Springer, Berlin, Heidelberg.
[52] U.S. Securities and Exchange Commission. (2019). Strengthening Cybersecurity Controls and Infrastructure.
[53] National Fire Protection Association. (2019). NFPA 1221: Standard for the Installation, Maintenance, and Use of Emergency Services Communications Systems.
[54] Institute of Electrical and Electronics Engineers. (2018). IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture Amendment 1: Enhancements for Emergency Services Communications.

The defense alliance dynamics also play a pivotal role. While Taiwan has strong ties with the U.S., Israel's security dynamics are closely intertwined with NATO and other Western allies. An EMP attack on either nation could thereby instigate a domino effect, dragging allies into conflict, and reshaping global geopolitics.

In conclusion, while the immediate need is to bolster the defenses of both Taiwan and Israel, the overarching theme is the call for a holistic global strategy. This would involve nations collaborating on intelligence sharing, joint research and development of countermeasures, and diplomatic dialogues to control the proliferation of EMP technologies. The global stakes are high, demanding a unified and comprehensive response.

Countermeasures and Resilience[55] [56]

The threat of EMP weapons, capable of disabling vast regions of electronic infrastructure, necessitates multifaceted protective strategies. Modern aircraft, pivotal to defense, rely heavily on sensors like Micro-Electro-Mechanical Systems (MEMS) for essential functions. These sensors are inherently vulnerable to electromagnetic disturbances, making them potential targets in EMP attacks. Shielding techniques, which could include advanced materials or Faraday cages, can protect such sensors from EMP disruption. Furthermore, in mission-critical scenarios, implementing redundant systems ensures that if one is incapacitated due to an EMP strike, its counterpart can take over. Optical systems, notably fiber optics for communication, offer another avenue of defense, given their natural immunity to electromagnetic disturbances.

In the realm of research and development, there's promising work in nanostructured materials that offer enhanced EMP shielding. These materials, combined with cutting-edge circuit designs that can divert energy surges from EMPs, could be the next frontier in defense technology. Realistic EMP simulators can further enable defense agencies to test current tech resilience and refine designs for better protection.

From an intelligence perspective, proactive measures like high-altitude satellite surveillance can help in early detection of adversary EMP weapon tests or deployments. Collaborating intelligence with global allies can cast a wider surveillance net, providing a comprehensive view of emerging EMP threats. Furthermore, cyber surveillance, spanning online forums, research publications, and other digital avenues, can offer timely insights into ongoing research or imminent EMP-related threats from adversary nations. In essence, while the EMP threat looms large, a combination of advanced materials science, innovative circuitry, and exhaustive intelligence efforts can fortify the U.S.'s defenses, ensuring continued operational capability even in the face of EMP adversity.

[55] U.S. Department of Homeland Security. (2016). National Infrastructure Protection Plan.
[56] Moteff, J., & Parfomak, P. (2014). Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress. Congressional Research Service.

Conclusion

China's rapid advancements in the field of EMP weaponry have emerged as a significant concern for the strategic landscape of global security, particularly concerning the vulnerabilities of U.S. military and civilian operations. These developments are not merely theoretical exercises but tangible shifts that could recalibrate the balance of power. The risks they introduce extend beyond battlefield confrontations to potentially crippling impacts on the everyday frameworks that underpin U.S. society—from communication networks to energy grids. Furthermore, considering the increasing reliance on electronic systems in biosecurity frameworks, an EMP strike could severely compromise essential biomedical research, bio-surveillance mechanisms, and emergency healthcare responses. Disruption of these systems could exacerbate the spread of biothreats or hinder the containment of potential outbreaks, further endangering public health and national security. In light of this evolving threat matrix, it is not only essential to rigorously assess and understand the nuances of China's EMP capabilities but also to champion the development and deployment of robust countermeasures. Beyond reactive strategies, proactively building resilience into the very fabric of U.S. defense, critical infrastructure, and biosecurity systems is vital. This dual approach of preemptive defense and systemic robustness will be instrumental in ensuring that the U.S. remains at the forefront of global defense dynamics, safeguarding its assets and interests in an increasingly complex technological era.

Acknowledgements

We wish to extend our profound appreciation to Dr. Robert McCreight for his invaluable insights and expertise on the subject of advanced weapons systems, convergent technology, and neuroscience-based threats. With a distinguished career that spans roles as a US Army Special Ops officer, a treaty negotiator with the State Department, and an advisor to the Reagan White House on nuclear matters, Mr. McCreight's contributions to our understanding of this domain are unparalleled. Notably, his coining of the term "NeuroStrike" has provided a significant conceptual framework that aids in illuminating the complex nuances of technologies behind phenomena such as the Havana Syndrome. Beyond his direct contributions to this work, his vast academic pursuits, including teaching at a graduate level and authoring numerous books and articles, have undoubtedly shaped the broader discourse on topics ranging from emergency management to future technology risks. We are sincerely grateful for his guidance, which has enriched this study and, by extension, the collective knowledge on this critical subject.