Research Report

LJ EADS, RYAN CLARKE, XIAOXU SEAN LIN

AUGUST 2023

In the Shadows of Science: Unravelling China's Invisible Arsenals of Nanoweapons

Table of Contents

Executive Summary

1. China's invisible arsenals of nanotechnology-driven weapons encompass a range of advanced weaponry that are distinctly focused on providing the Chinese Communist Party (CCP) with a range of asymmetric warfare options. This includes the delivery of biological, biochemical and neurobiological weapons on target populations. These developments present enormous new challenges to global security that are without historical precedent in human history.

2. China's advancements in biotechnology raise concerns about potential dual-use applications, as there are fears they may be exploring genetically engineered pathogens for use in biological warfare, while obfuscating the original point of origins. While the CCP's attempts to obfuscate the Wuhan Institute of Virology's role in the SARS-CoV-2/COVID-19 pandemic were unsuccessful, nanotechnology delivery systems would make future investigations and determinations of specific attribution more challenging.

3. It is essential for the international community to closely monitor China's advancements in these areas and engage in open discussions to define the boundaries of what constitutes a chemical weapon, biological weapon, or any other type of invisible arsenals.

4. By understanding and addressing these challenges, nations can collectively work to strengthen arms control regimes and maintain global security in the face of rapidly evolving threats. If the CCP refuses to engage in these discussions, that is also information and should then generate precision targeting plans to eliminate these threats.

5. Researchers from the Hefei Institute of Physical Science, Chinese Academy of Sciences, have made a breakthrough in DNA nanotechnology, developing a smart DNA molecular nanorobot model. This model innovatively proposes a non-linear gathering 'siege' of biological targets, allowing for advanced signal amplification and intelligent targeted drug delivery.

6. The article suggests that this technology has potential applications in biosensing, bioimaging, and drug delivery. However, there are risks associated with this advancement. The ability of nanorobots to transport biological agents directly to target cells with deadly precision could be exploited by the CCP's People's Liberation Army (PLA) for harmful purposes.

7. It could be used to deliver biological agents with precision, making it a potential threat for biological warfare. Additionally, the close collaboration between the Hefei Institute of Physical Science and the PLA raises concerns about potential dual-use applications of this technology for military purposes.

8. The CCP views nanotechnology-driven warfare as a core component of its asymmetric warfare strategy against the United States and its Allies. They are part of the CCP's standard order of battle; not an unconventional set of capabilities only to be used under extreme circumstances. This represents a fundamental difference in strategic thinking regarding these domains in Beijing.

9. However, the CCP's weaponization of multiple scientific disciplines extends well beyond viruses (such as SARS-CoV-2), as well as beyond the scope and understanding of classical bioweapons. Their new landscape of nanotechnology weapons development includes the entire synthetic biology spectrum; from human genome editing of soldiers, genetic manipulation of bacteria to using human-computer interface to attack and/or control entire populations.

10. 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 dual-use research would provide unprecedented tools for the CCP to forcibly establish a new world order, which has been Xi Jinping's lifelong goal.

11. For example, these capabilities can 'fit' into the CCP's anti-access/area denial strategy in the Indo-Pacific. Imagine genetically immunized PLA troops being inserted into a geography where a specific weaponized bacterial strain has been released using nanotechnology delivery mechanisms prior to their entry to prepare the ground and eliminate points of resistance. Any remaining sources of resistance on the ground are then dealt with through neurobiological weaponry that instill intense fear and/or other forms of cognitive incoherence resulting in inaction.

12. The net result of such a scenario would be the PLA establishing absolute control over a geography such as Taiwan while simultaneously blunting any American strategic options to intervene and physically insert personnel into the theater. This would effectively negate and render inert America's overwhelming conventional superiority with very few (if any) near-term remedies. This scenario is based on known existing CCP research programs and what the clear strategic aims of those programs are.

13. What is the current state and near-term trajectories of these programs? What new strategic options would these capabilities generate for the CCP? What are the critical dependencies and acute vulnerabilities of these programs? How do we collapse these CCP programs with no options for reconstitution or regeneration?

`14. These are the types of questions that need to be directly addressed with domain expertise augmented by field-validated precision search and intelligence representation technology that are utilized by the CCP BioThreats Initiative.

In the Shadows of Innovation: China's Invisible Arsenals and the Emergence of Nanotechnology-Enabled Warfare

China's invisible arsenals encompass a wide array of advanced and covert weaponry developed using next-generation technologies, particularly nanotechnology platforms. These weapons are designed to be discreet, hard to detect, and capable of inflicting significant damage on adversaries while avoiding direct confrontation. China's invisible arsenals encompass a range of advanced weaponry that are distinctly focused on providing the Chinese Communist Party (CCP) with a range of asymmetric warfare options, including the delivery of biological, biochemical and neurobiological weapons on target populations. These developments present enormous new challenges to global security that are without historical precedent in human history.[1]

Nanotechnology-enabled weapons utilize highly sophisticated nanomaterials to enhance performance, stealth capabilities, and overall attack efficacy in military applications. Additionally, China's advancements in biotechnology raise concerns about potential dual-use applications, as there are fears they may be exploring genetically engineered pathogens for use in biological warfare, while obfuscating the original point of origins. While the CCP's attempts to obfuscate the Wuhan Institute of Virology's role in the SARS-CoV-2/COVID-19 pandemic were unsuccessful, nanotechnology delivery systems would make future investigations and determinations of specific attribution more challenging. [2] [3]

If China had in its possession a stockpile of chemical warfare agents, coupled with advancements in nanotechnology, they would be able to development advanced nano-enhanced stealth chemical weapons. Furthermore, their expertise in electromagnetic and cyber warfare allows them to disrupt critical infrastructure and defense networks without direct military engagement, making traditional countermeasures obsolete and ineffective.

China's focus on hypersonic technology and AI-driven warfare enables the delivery of their invisible arsenal with unprecedented speed and precision, further complicating defense strategies. Their emphasis on psychological and information warfare through "The Three

---

[1] For more in-depth analysis of these programs, please see the following CCP BioThreats Initiative Reports:
China's International Military-Civilian Virology Fusion: High-Risk Pathogen Research, Global Linkages and Strategic Implications: Clarke, Dr. Ryan, Lin, Dr. Xiaoxu Sean, Eads, LJ: 9789869777483: Amazon.com: Books
Guardians of the Invisible Arsenal - Weapons Research at the Research Institute of Chemical Defense — The CCP BioThreats Initiative
State-Backed Synthetic Narcotics Trafficking Syndicates and the Vectored Threat to the Five Eyes — The CCP BioThreats Initiative
The International Frontier of the CCP's Bioweapons Program — The CCP BioThreats Initiative
Precision Targeting Bioweapons Facilities in a Post-CCP Regime Collapse Scenario — The CCP BioThreats Initiative
Enumerating, Targeting and Collapsing the Chinese Communist Party's NeuroStrike Program — The CCP BioThreats Initiative

[2] Wu Xinghua, Zhao Lei, "Nanotechnology——Building the Future Battlefield "Transformers"", China Military Net, http://www.81.cn/bq_208581/10106213.html, 2021-11-09

[3] Wu Xinghua, Shang Xiaomin, "When nanotechnology meets ceramics, what kind of sparks will it collide with?", China Military Net, Zhongke Nano Industry Group, http://www.81.cn/ss_208539/10097801.html, 2021-10-11

Warfares" underscores their understanding of the power of controlling narratives and manipulating public opinion to achieve strategic goals without overt military actions.[4]

One of the most concerning aspects of China's invisible arsenals is their distributed and potentially decentralized nature, as weapons may be concealed within civilian infrastructure, posing challenges for traditional intelligence and surveillance methods. This evolving landscape necessitates a deeper understanding and awareness of these threats to devise effective countermeasures and safeguard global security.

It is essential for the international community to closely monitor China's advancements in these areas and engage in open discussions to define the boundaries of what constitutes a chemical weapon, biological weapon, or any other type of invisible arsenals. By understanding and addressing these challenges, nations can collectively work to strengthen arms control regimes and maintain global security in the face of rapidly evolving threats. If the CCP refuses to engage in these discussions, that is also information and should then generate precision targeting plans to eliminate these threats.

---

[4] Enumerating, Targeting and Collapsing the Chinese Communist Party's NeuroStrike Program — The CCP BioThreats Initiative

For additional information, please see
Robert McCreight, 'Neuro-Cognitive Warfare: Inflicting Strategic Impact via Non-Kinetic Threat', *Small Wars Journal*, 16 September 2022.

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.

Unseen Perils: Emerging Threats in Nanotechnology Warfare[5]

The convergence of nanotechnology with various scientific disciplines opens possibilities for China to develop new invisible arsenals beyond traditional chemical and biological weapons. These potential invisible arsenals include:

- **Nanoscale Electronics and Cyber Warfare**: Nanotechnology can enable the development of miniature, high-performance electronic components, and sensors. In the realm of cyber warfare, this could lead to the creation of advanced, undetectable nano-devices for surveillance, data theft, or even disrupting critical infrastructure without leaving a trace.

- **Nano-Enhanced Stealth Materials**: Nanomaterials can be engineered to manipulate light and electromagnetic waves, potentially leading to the creation of advanced stealth materials. Invisible aircraft, ships, or vehicles could be developed using these technologies, making them virtually undetectable to radar and other conventional sensors.

- **Nanomedicine as a Weapon**: While nanomedicine holds great promise for medical advancements, it could also be misused as a weapon. Nanoscale drug delivery systems could be tailored to deliver toxic agents specifically to target individuals or groups, making it challenging to trace the source of the attack.

- **Nanorobotics and Autonomous Weapons**: Nanotechnology can facilitate the development of nanorobots with various functions, such as swarm intelligence and autonomous decision-making. These tiny yet powerful machines could be weaponized for tasks like reconnaissance, infiltration, or even targeted assassinations.

- **Nano-Bioinformatics for Biowarfare**: Advanced computational techniques, combined with nanotechnology, could allow for the manipulation of biological data and the creation of synthetic pathogens or genetically modified organisms with enhanced virulence or drug resistance.

- **Nano-Scale Chemical Sensors**: Nanosensors can be used for detecting and identifying chemical substances at extremely low concentrations, making them ideal for covert monitoring or assessing the success of chemical attacks.

- **Nano-Cyber Biological Weapons**: The integration of nanotechnology with cyber and biological domains could give rise to sophisticated hybrid weapons, where nanoscale devices are deployed to infect computer systems, disrupt communication networks, or control biological agents remotely.

[5] Nicholas Winstead, The Applications and Implications of Nanotechnology, The Center for Security, Innovation, and New Technology (CSINT), American University - Washington DC, 2020-04-15

- **Nanoparticle-Enhanced Energy Weapons**: Nanoparticles could be employed to enhance the performance of directed energy weapons, such as laser systems or electromagnetic pulse (EMP) devices, enabling more precise and devastating attacks.

As these examples illustrate, the combination of nanotechnology with various fields introduces novel and complex challenges for security and non-proliferation efforts. The potential for invisible arsenals extends far beyond traditional chemical and biological weapons, making it essential for policymakers, researchers, and international communities to remain vigilant and proactive in addressing emerging threats in this rapidly advancing technological landscape.

Emerging Nanotechnology in Chemical and Biological Warfare: Unveiling the Risks of Advanced Detection and Stealth Capabilities

The report 'Core-shell quantum dot-nano-gold particle assembly for efficient detection of nerve agent mimics' discusses the development of a core-shell quantum dot-nano-gold particle assembly for the efficient detection of nerve agent mimics. The study was conducted by researchers from the Institute of Chemical Defense, Chinese Academy of Military Sciences, the State Key Laboratory of National Nuclear, Biological and Chemical Protection, and the Technical Institute of Physics and Chemistry, Chinese Academy of Sciences. The research aimed to establish a simple and fast detection method for nerve agent mimics, which are highly toxic organophosphates with potential threats to human health and security.[6]

The experimental design involved creating a composite structure of 12 layers of zinc sulfide-coated cadmium selenide core-shell quantum dots (CdSe/12ZnS QDs) and gold nanoparticles (Au NPs). The fluorescence resonance energy transfer (FRET) between QDs and Au NPs was utilized for detection purposes. The hydrolysis of thioacetylcholine chloride (ATC) by acetylcholinesterase (AChE) generated thiocholine, which replaced the quantum dots, leading to the restoration of fluorescence. The presence of the nerve agent mimic diethyl cyanophosphate (DCNP) inhibited AChE activity, resulting in reduced fluorescence recovery efficiency of QDs. By measuring the fluorescence recovery efficiency of quantum dots, DCNP could be detected within a concentration range of 5.0×10–9 to 5.0×10–4 mol/L, with a detection limit of 5.0×10-9mol/L.[7] The core-shell structure of CdSe/12ZnS QDs offered improved luminous efficiency and stability, enhancing the fluorescence recovery rate. The coordination effect between quantum dots and Au NPs improved the FRET fluorescence quenching efficiency. The system demonstrated good anti-interference properties, showing potential for practical applications in detecting nerve agent mimics. Additionally, the aggregation degree of gold particles under different DCNP concentrations caused observable color changes in the solution, providing a possibility for naked eye detection of DCNP.[8] Overall, the study presents an approach to detect nerve agent mimics using nanotechnology, showcasing the potential of core-shell quantum dot-nano-gold particle assemblies for efficient and sensitive detection of toxic agents.

[6] Li Shengsong , Zheng Yongchao , Meng Shulin, Wu Lizhu, Zhong Jinyi, Zhao Chonglin, 'Core-shell quantum dot-nano-gold particle assembly for efficient detection of nerve agent mimics (核壳型量子点-纳米金颗粒组装体高效检测神经性毒剂模拟剂)', *Journal of Inorganic Materials*, Issue 8, 2019, 2019-09-12.

[7] Ibid.

[8] Ibid.

This research has potential applications not only in defense and counterterrorism but also in offensive military capabilities. Some offensive ways this research could be utilized by the Chinese military include:

- **Advanced Chemical Warfare**: The research findings could be used to develop more efficient and sophisticated chemical weapons. By understanding the mechanisms of fluorescence quenching and recovery, the Chinese military could design chemical agents that inhibit acetylcholinesterase activity, leading to severe nerve agent-like effects on the nervous system of the targeted individuals or populations.

- **Covert Surveillance and Assassination**: The development of core-shell quantum dot-nano-gold particle assemblies could enable the creation of highly sensitive detection systems. These systems might be used for covert surveillance, detecting trace amounts of nerve agent mimics or other chemical substances associated with enemy activities. Additionally, the technology could facilitate targeted assassinations, as the detection systems might be used to identify and track specific individuals or groups exposed to toxic agents.

- **Non-Conventional Attacks**: The research's focus on nanoscale detection and advanced stealth materials could open up possibilities for unconventional attacks. Invisible delivery methods, such as drones or other nanoscale devices, could be equipped with nerve agent mimics and used to infiltrate enemy territories without detection, leading to devastating consequences.

- **Cyber-Biological Attacks**: The combination of nanotechnology with cyber and biological domains could lead to the creation of sophisticated hybrid weapons. Nanoscale devices could be deployed to infiltrate computer systems, disrupt communication networks, and remotely control biological agents, blurring the lines between traditional military and cyber warfare.

- **Targeted Biological Warfare**: While the research primarily focuses on nerve agent mimics, it could also provide insights into the manipulation of biological data and the creation of genetically modified organisms. The Chinese military might explore the development of genetically engineered pathogens with specific virulence or drug resistance profiles, allowing for targeted biological attacks against enemy forces or populations.

The research's primary intent might be focused on defense and civilian applications however, given the dual-use nature of many technologies, offensive military applications cannot be entirely ruled out. The potential misuse of such research highlights the need for international cooperation and stringent safeguards to prevent the proliferation and use of these technologies for harmful purposes.

The Rise of China's Nanoscale Electronics and Cyber Warfare Capabilities

China's military has been at the forefront of leveraging nanoscale electronics and cyber warfare, capitalizing on the convergence of nanotechnology and information warfare to gain a significant advantage in the digital realm. Nanoscale electronics allows the Chinese military, specifically the PLA's Strategic Support Force (PLASSF), to develop miniature yet high-performance electronic components and sensors, providing them with enhanced computing power, data processing, and communication capabilities.[9] The PLA Daily quoted that the members of the PLASSF should always prepare for 'tomorrow's warfare'. These nanoelectronics find applications not only in consumer electronics but also in military equipment, enabling the Chinese military to stay at the cutting edge of technological advancements thus preparing the PLA for tomorrow's war.

In the realm of cyber warfare, China's military harnesses nanotechnology to develop advanced and stealthy nano-devices with various espionage and data theft capabilities. These nano-devices are deployed covertly to infiltrate secure networks, gather sensitive information, and monitor communications without raising any suspicion. Their small size and sophisticated design allow them to evade conventional security measures, making them formidable tools for cyber-espionage.

The offensive potential of China's nanotechnology research in cyber warfare is particularly concerning. Nano-devices can be employed to carry out cyber-attacks on critical infrastructure and networks, leaving little to no traces behind. These attacks could lead to blackouts, communication failures, or financial disruptions, posing severe threats to national security and stability. Moreover, with the integration of AI into nano-devices, China's military can create autonomous AI-driven nano-weapons capable of making real-time decisions and executing cyber-attacks with unparalleled sophistication and unpredictability. This AI-nanotechnology synergy presents significant challenges for traditional defense mechanisms and raises questions about accountability in the event of cyber conflicts.

The conference paper 'Communication Modeling for Targeted Delivery under Bio-DoS Attack in 6G Molecular Networks' published by the Institute of Cyber Science and Technology at Shanghai Jiao Tong University and the State Grid Electric Power Research Institute discusses the use of molecular communication, a nanonetwork paradigm in 6G networks, for targeted delivery. However, it raises concerns about the vulnerability of this communication method to Bio-Denial of Service (Bio-DoS) attacks, where the delivery process can be compromised. The Bio-DoS attack could disrupt the biochemical reaction between the targeted molecule and the Information Molecule (IM), affecting the effectiveness of targeted delivery.[10]

The risks and implications of the Chinese military using nanotechnology-enabled weapons to conduct Bio-DoS attacks are significant. If the Chinese military gains access to nanotech capable of conducting Bio-DoS attacks, it could exploit vulnerabilities in molecular communication networks to disrupt targeted delivery systems, causing potential chaos in critical systems and services. The compromised nanotech could be used for harmful purposes,

[9] Zhao Lei, "Xi Calls New PLA Branch a Key Pillar," China Daily, August 30, 2016.
[10] Shen, Q., Wu, J., Li, J., Zhang, X., Wang, K., 'Communication Modeling for Targeted Delivery under Bio-DoS Attack in 6G Molecular Networks (Conference Paper)', 2021 IEEE International Conference on Communications, June 2021

targeting specific individuals or groups with precision and causing harm to their biological systems.

Moreover, the involvement of Shanghai Jiao Tong University, known for conducting cyber-attacks on the United States with PLA military units, raises additional concerns. It suggests a potential link between academic research and military applications, indicating the risk of dual-use technology for military purposes.[11]

Overall, the implications of the Chinese military utilizing nanotechnology-enabled weapons to conduct Bio-DoS attacks pose a serious threat to communication networks and targeted delivery systems, potentially disrupting critical services and causing harm to individuals or organizations. Close monitoring and stringent controls on the development and deployment of such technology are essential to mitigate these risks and protect against potential misuse.

The blurring line between the physical and digital realms in nanoscale electronics and cyber warfare demands robust cybersecurity measures and defense strategies. As China's capabilities in these areas continue to advance, it is crucial for other nations, organizations, and cybersecurity experts to remain vigilant and develop effective safeguards to detect, prevent, and respond to emerging threats posed by China's nanotechnology-enabled cyber weapons.

China's Advancements in Nano-Enhanced Chemical and Biological Warfare

With China's rapid strides in nanotechnologies, concerns rise over their potential use in chemical and biological warfare, posing serious risks and implications for global security. The convergence of nanotechnology with various military domains presents unprecedented challenges. China's military could exploit these technologies to enhance chemical and biological weapons to alarming levels of potency and sophistication. Meanwhile, China's military is actively researching and developing protective clothing against 'future biochemical warfare agents' with the advancements of nanotech enhanced clothing.[12] Nanoparticles integrated into traditional chemical agents could increase their stability and dispersal, while nanoscale drug delivery systems might transport biological agents directly to target cells with deadly precision. Moreover, nanorobots could navigate the human body, delivering lethal payloads while evading conventional biological defenses.[13]

Researchers from the Hefei Institute of Physical Science, Chinese Academy of Sciences, have made a breakthrough in DNA nanotechnology, developing a smart DNA molecular nanorobot model. This model innovatively proposes a non-linear gathering 'siege' of biological targets, allowing for advanced signal amplification and intelligent targeted drug delivery.

The nanorobot model consists of multifunctional robotic arms with optional accessories (such as drugs and signal tags), target validators, intelligent swarm path controllers, and self-

[11] China Defence Universities Track, Shanghai Jiao Tong University, Australian Strategic Policy Institute, https://unitracker.aspi.org.au/universities/shanghai-jiaotong-university/

[12] Li Rong, Ge Xin, Chang Liushuan, Yang Limei, Research progress of electrospun nano functional fibers for biochemical warfare agent protective clothing (用于生化战剂防护服的静电纺丝纳米功能纤维研究进展), Medical and Health Equipment Issue 9, 2015, 2015-12-27

[13] Dominik Juling, Future Bioterror and Biowarfare Threats for NATO's Armed Forces until 2030, Journal of Advanced Military Studies vol. 14, no. 1, Spring 2023

assembling motors. It responds only to specific biological targets, forming a large aggregate through cooperative operations and achieving nonlinear cascade amplification or amplification of target signals.

The article suggests that this technology has potential applications in biosensing, bioimaging, and drug delivery. However, there are risks associated with this advancement. The ability of nanorobots to transport biological agents directly to target cells with deadly precision could be exploited by the CCP's People's Liberation Army (PLA) for harmful purposes. It could be used to deliver biological agents with precision, making it a potential threat for biological warfare. Additionally, the close collaboration between the Hefei Institute of Physical Science and the PLA raises concerns about potential dual-use applications of this technology for military purposes.[14]

China's military could leverage nanosensors for covert monitoring, detecting even minute traces of chemical and biological agents to assess the success of their attacks. In the realm of cyber-biological warfare, the integration of nanotechnology with cyber capabilities might lead to the development of hybrid nanobots capable of infecting both computer systems and biological organisms, causing widespread chaos and disruption. Through genetic engineering using nanotechnology, China could create pathogens that are more virulent, resistant to treatments, or tailored to target specific genetic traits, exponentially increasing their destructive potential.

Additionally, China could employ nanomaterials to create stealth materials, rendering military equipment nearly invisible to conventional detection methods. While these advancements raise serious concerns, it is imperative to emphasize that employing nanotechnology for developing chemical and biological weapons is strictly prohibited under international law, including the Chemical Weapons Convention (CWC) and the Biological Weapons Convention (BWC). To safeguard global security and stability, robust non-proliferation efforts, strong arms control agreements, and international cooperation are essential to prevent the misuse of nanotechnologies for harmful purposes. Vigilance and collective action are crucial in ensuring that China's capabilities in this field are not utilized to undermine international security. If the CCP resists these measures, there need to be concrete discussions around offensive actions to destroy these programs.

New Safeguards Against Invisible Weapons

As the development of invisible weapons incorporating nanotechnologies progresses, there is an urgent need for innovative safeguards to detect and counter these emerging threats. Traditional methods of detecting chemical and biological weapons may prove inadequate in the face of these new capabilities, as invisible weapons are designed to avoid direct confrontation and go undetected by conventional sensors. Therefore, it is imperative to invest in cutting-edge technologies and research to stay ahead of potential adversaries.

One approach to addressing this challenge is to develop advanced nanosensors capable of detecting and identifying nanomaterials and nanodevices that may be used in these invisible arsenals. These sensors should be able to operate at the nanoscale level to ensure sensitivity

[14] China News Network, The Chinese scientific research team proposes a model of intelligent nano-robots gathered to "siege" biological targets, http://www.chinanews.com.cn/sh/2022/05-19/9758568.shtml, 2022-05-19

to minute quantities of nanomaterials, enabling real-time monitoring and early detection of potential threats.

Moreover, advancements in artificial intelligence and machine learning can play a crucial role in analyzing vast amounts of data to identify patterns and anomalies associated with invisible weapons. AI-driven surveillance systems can constantly monitor various data sources, including cyber activities, environmental samples, and communication networks, to spot any suspicious activities or emerging threats.

Furthermore, international collaboration and information sharing are paramount in tackling the global challenge of invisible weapons. Nations must work together to exchange intelligence, share best practices, and collectively develop strategies to counter these emerging threats effectively.

Lastly, policymakers and researchers must continuously assess and update existing arms control agreements to address the fast-evolving landscape of invisible arsenals. By ensuring that international treaties are adaptable and encompass novel technologies, we can strengthen the global framework for non-proliferation and deter potential actors from pursuing these dangerous weapons.

In summary, addressing the risks posed by invisible weapons requires a multifaceted and forward-thinking approach. By investing in new detection technologies, leveraging AI and machine learning, fostering international collaboration, and updating arms control agreements, the global community can enhance its ability to detect and mitigate the dangers of these new and emerging threats.

Conclusion

The CCP views nanotechnology-driven warfare as a core component of its asymmetric warfare strategy against the United States and its Allies. They are part of the CCP's standard order of battle; not an unconventional set of 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.[15]

However, the CCP's weaponization of multiple scientific disciplines extends well beyond viruses (such as SARS-CoV-2), as well as beyond the scope and understanding of classical bioweapons. Their new landscape of nanotechnology weapons development includes the entire synthetic biology spectrum; from human genome editing of soldiers, genetic manipulation of bacteria to using human-computer interface to attack and/or control entire

[15] For additional information, please see Ryan Clarke, 'Is China Converting COVID-19 into a Strategic Opportunity?', EAI Background Brief No. 1545, July 9, 2020.
Ryan Clarke, 'Post-COVID China: Core Strategic Drivers and Multi-Dimensional Asymmetric Warfare in Asia', Center for Security Policy, August 2021.

populations, the latter of which we refer to as CCP NeuroStrike.[16] 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 dual-use research would provide unprecedented tools for the CCP to forcibly establish a new world order, which has been Xi Jinping's lifelong goal.

For example, these capabilities can 'fit' into the CCP's anti-access/area denial strategy in the Indo-Pacific. Imagine genetically immunized PLA troops being inserted into a geography where a specific weaponized bacterial strain has been released using nanotechnology delivery mechanisms prior to their entry to prepare the ground and eliminate points of resistance. Any remaining sources of resistance on the ground are then dealt with through neurobiological weaponry that instill intense fear and/or other forms of cognitive incoherence resulting in inaction.

The net result of such a scenario would be the PLA establishing absolute control over a geography such as Taiwan while simultaneously blunting any American strategic options to intervene and physically insert personnel into the theater. This would effectively negate and render inert America's overwhelming conventional superiority with very few (if any) near-term remedies. This scenario is based on known existing CCP research programs and what the clear strategic aims of those programs are.

What is the current state and near-term trajectories of these programs? What new strategic options would these capabilities generate for the CCP? What are the critical dependencies and acute vulnerabilities of these programs? How do we collapse these CCP programs with no options for reconstitution or regeneration? These are the types of questions that need to be directly addressed with domain expertise augmented by field-validated precision search and intelligence representation technology that are utilized by the CCP BioThreats Initiative.

---

[16] 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.