



SINOPSIS

Blueprinting the Future: Mitigating the Risks of Chinese Hegemony in Additive Manufacturing

David Gardáš, Michal Thim, Filip Urban



Table of Contents

1. Executive Summary.....	2
2. China's Strategic Deployment of AM Across Industries	4
3. AM in China's Industrial Policy System	7
4. AM Integration into China's Defense Industrial Base.....	11
5. When the PLA Is Always Just a Step Away: the MCF Ecosystem Case Study	13
5.1. NORINCO.....	13
5.2. BLT.....	14
5.3. Bambu Lab.....	15
6. Cyber Espionage and China's Pursuit of Technological Advantage	18
6.1. AM and its Supply Chain as Emerging Targets.....	19
6.2. China-Nexus Targeting of the Technology Sector.....	22
6.3. Regulatory Weaponisation of Vulnerability Disclosure	23
7. Policy Recommendations.....	25



1. Executive Summary

Additive manufacturing (AM, 增材制造), commonly known as 3D printing (3D打印), refers to production processes that create physical objects from digital models by adding material layer by layer. Unlike traditional subtractive machining or tooling-intensive molding and casting, AM offers unprecedented manufacturing flexibility, enabling a single production system to rapidly produce components of widely different designs without dedicated tooling or production-line reconfiguration. It can also realize complex geometries and internal structures that are difficult or physically impossible to achieve through conventional manufacturing techniques.

By compressing the cycle from design to physical part from weeks or months to hours or days, AM enables rapid iteration and production at or near the point of need, reducing dependence on conventional supply chains and logistics. These characteristics make it particularly valuable in time-sensitive or supply-constrained environments, including defense, disaster response, and other crisis conditions. Its industrial value stems from the integration of software, advanced materials, precision machinery, and production data, making it an important component of next-generation manufacturing and a powerful accelerator of innovation.

Over the past three decades, AM has been incorporated into China's industrial-policy system and identified as a strategic industry, including through Made in China 2025 《中国制造2025》. Dedicated AM plans, provincial support programs, and high-level documents such as the official outline of the recently concluded 14th Five-Year Plan (FYP) have all emphasized the importance of AM. Chinese AM companies also benefit from broader non-market measures favoring localization, scale, and domestic substitution, and receive disproportionately high levels of state support relative to competitors in OECD economies, including through subsidies, preferential financing, and R&D support. The result is a significant distortion of competition, enabling rapid expansion abroad while foreign firms face more constrained access to the Chinese market. At the same time, it undermines the viability of new Western AM entrants and reduces their ability to secure venture funding.

Against this policy backdrop, China's AM industry now spans desktop 3D printers as well as industrial systems for high-performance metal and polymer components. Over the past several years, Chinese firms have rapidly expanded their global presence, with companies such as Bambu Lab carving out a dominant position in mass-market hardware, while Xi'an Bright Laser Technologies (BLT) and Farsoon Technologies have strengthened China's



position in advanced metal and polymer systems for aerospace and other high-value sectors. This expansion is increasing Chinese influence across the AM value chain while accelerating import substitution and shifting strategic manufacturing capacity and know-how into more integrated domestic supply chains.

As AM production becomes increasingly concentrated within a China-controlled ecosystem, risks related to intellectual property loss, technology transfer, and the security of sensitive data become more consequential. This is especially important because 3D printing is now a standard prototyping tool across many advanced industries, meaning AM systems often handle early-stage designs and sensitive engineering data well before products reach commercial production. Beyond prototyping, these systems also process engineering drawings, material specifications, process parameters, software, and machine settings that can embody years of R&D and provide a relatively direct path from digital design to physical production. Unauthorized access can therefore shortcut development and production cycles, facilitate reverse engineering, reduce costly trial-and-error, and accelerate domestic substitution or replication of advanced manufacturing capabilities.

These risks take on added significance because of AM's dual-use nature. Technologies used in aerospace, medical, automotive, and energy applications can also support military logistics, space systems, unmanned platforms, and weapons production. The reported use of Bambu Lab printers in Ukrainian drone-related production and by the British Army illustrates how commercially available systems can enter defense environments, raising concerns around cloud connectivity, telemetry, firmware control, remote access, and sensitive production data. In the context of military-civil fusion (军民融合), these dynamics also create risks of technology diversion and the transfer of commercially acquired capabilities into defense applications.

Taken together, these trends make China's AM ecosystem a strategic concern not only for industrial competitiveness, but also for supply-chain resilience, technology and innovation security, intellectual-property protection, and Western national security.



2. China's Strategic Deployment of AM Across Industries

Additive manufacturing is strategically important because it allows layer-by-layer fabrication of complex parts, reduces tooling dependence, shortens iteration cycles, enables lightweight structures and internal channels, and supports localized production of hard-to-machine or low-volume components. In the Chinese policy statements, these advantages are explicitly tied to aviation, aerospace, biomedicine, and other high-end sectors where performance, supply security, and time-to-deployment matter.¹

Critical Sectors:

- **Medical:** Additive manufacturing is important in medicine because it enables patient-specific implants and surgical hardware that more closely match individual anatomy than standardized parts. Applications now span a wide range of tissue types, including bones, joints, vascular and neural tissues, as well as patient-specific medical models and personalized pharmaceuticals, helping reduce surgical time and costs.² China's strongest public examples are Peking University Third Hospital's world-first 3D-printed artificial vertebra and China's first approved 3D-printed human implant.³
- **Energy:** Additive manufacturing is important in energy because it enables large, high-performance parts with complex flow paths and reduced machining burdens. Chinese examples include Dongfang Electric's use of robotic arc additive manufacturing for a 500-megawatt impulse-hydropower runner⁴ and Dongfang Turbine's use of 3D printing for hard-to-machine complex components in its G15 heavy-duty gas turbine.⁵
- **Telecommunications & Satellites:** Additive manufacturing is valuable for this sector because antennas, brackets, and payload supports benefit from lightweight

¹ 江苏省经济和信息化委员会等, “关于印发江苏省增材制造产业发展三年行动计划(2018-2020年)的通知”, August 28, 2018.

² Chensong Dong, Marko Petrovic, and Ian J. Davies, “Applications of 3D Printing in Medicine: A Review”, *Annals of 3D Printed Medicine*, February 7, 2024.

³ 北京大学, “世界首个3D打印人工椎体植入手术在北大第三医院获得成功”, June 15, 2016.

⁴ 东方电机, “东方电气集团启动‘我为大国重器命名’宣传征名活动”, November 29, 2023.

⁵ 东方电气集团东方汽轮机, “探索燃气轮机技术进步‘中国方案’”, July 10, 2024.



geometries and rapid design iteration. Recent materials development is also expanding desktop AM into space applications: Czech companies Prusa Research and TRL Space developed PC Space Grade Black for printing functional satellite and CubeSat components.⁶ China Space Technology reports that Egyptian satellite MisrSat-2 used China's first 3D-printed integrated large ultra-light star-sensor bracket,⁷ while the University of Electronic Science and Technology of China publicized award-winning research on 3D-printed high-gain millimeter-wave and terahertz lens antennas relevant to future communications hardware.⁸

- **Aerospace:** Additive manufacturing is especially important in aerospace because it reduces part count and weight while enabling large or integrated structures. High-performance polymers such as ULTEM (PEI), PEEK, and carbon-fiber-reinforced materials can replace metal in selected applications, with carbon-fiber-reinforced PEEK delivering 40–60% weight savings while matching or exceeding aluminum's mechanical performance.⁹ Northwestern Polytechnical University reports that its laser solid forming technology produced the long titanium central-wing edge member for the C919,¹⁰ while the China Aerospace Science and Technology Corporation's Sixth Academy states that additive manufacturing has been used on more than 40 liquid-rocket-engine models and over 240 typical products supporting more than 50 launches and flight tests.¹¹
- **Defense:** The war in Ukraine has demonstrated AM's value in rapid, distributed production, particularly for drones and related components. Ukrainian volunteer networks use decentralized 3D-printing capacity to supply frontline units with mounts, sights, replacement parts, and other drone components on demand, while adapting designs quickly to changing battlefield requirements.¹² Interceptor drones such as Wild Hornets' Sting further illustrate how low-cost UAVs can be produced and modified rapidly to counter larger loitering munitions.¹³ Together, these applications bring production, adaptation, and replenishment much closer to

⁶ Prusa Research, "Prusament PC Space Grade Black – ESD Safe Material Suitable for Space Applications", September 25, 2025.

⁷ 中国空间技术研究院, "‘天眼’点亮‘太空丝路’, 埃及二号卫星发射成功!", December 4, 2023.

⁸ 电子科技大学, "我校博士生获ISAP2014‘最佳学生论文奖'", n.d.

⁹ Chenwei Shen, Yanbing Guo, Zhikang Shen, Fei Yan, and Ning Zhong, "Additive Manufacturing of Aerospace Composites: A Critical Review of the Material–Process–Design Interplay and Prospects for Application", *Materials*, September 12, 2025.

¹⁰ 西北工业大学, "西北工业大学与空客公司联合开发3D打印技术在航空领域的应用", March 17, 2014.

¹¹ 中国航天科技集团, "航天科技六院7103厂增材制造创新中心发展纪实", December 13, 2021.

¹² DrukArmy, "About Us", n.d.

¹³ Wild Hornets, "Ukrainian FPV Interceptor STING", n.d.



the point of need. China is developing similar capabilities: China Aero Engine Corporation has flight-tested a micro-turbojet with more than three-quarters of its weight produced through 3D printing for potential use in UAVs, target drones, and loitering munitions,¹⁴ while the PLA has demonstrated field units scanning damaged drone parts and printing replacements locally to return aircraft to service.¹⁵ Chinese AM capabilities also extend to large aircraft components and repair of complex high-end equipment.¹⁶

¹⁴ 中国航空发动机集团有限公司, “3D打印极简轻质微型涡喷发动机完成首次单发飞行试验!”, November 17, 2025.

¹⁵ Ministry of National Defense of the People's Republic of China, “军营观察 | ‘翼次方’工作室成长记”, March 20, 2026.

¹⁶ Northwestern Polytechnical University, “科技部党组书记王志刚调研西工大无人机和金属增材制造创新成果”, May 18, 2015.



3. AM in China's Industrial Policy System

China's interest in additive manufacturing began in the 1990s, when research on rapid prototyping and related AM technologies were concentrated in a small group of universities, including Tsinghua University (清华大学), Xi'an Jiaotong University (西安交通大学), Beihang University (北京航空航天大学), Northwestern Polytechnical University (西北工业大学), and Huazhong University of Science and Technology (华中科技大学).¹⁷ Foreign technology acquisition significantly contributed to this development. Kania and Wood identify foreign design, forging, CNC, and 3D manufacturing technologies—particularly laser additive manufacturing (LAM)—as inputs into China's growing defense-industrial capability at the time.¹⁸ This approach fits a longer-standing Chinese industrial-policy model of “introduction, digestion, absorption, and re-innovation,” in which foreign technology is acquired and adapted as an input into the development of indigenous capabilities.¹⁹

These domestic research capabilities and foreign technology inputs were subsequently incorporated into China's broader industrial-upgrading agenda. *Made in China 2025*, introduced in 2015, positioned AM within a broader drive toward intelligent manufacturing, advanced equipment, industrial upgrading, and reduced dependence on foreign core technologies.²⁰ This priority was then translated into Beijing's first two nationwide AM development plans: “国家增材制造产业发展推进计划(2015-2016年)” (National Additive Manufacturing Industry Development Promotion Plan, 2015-2016)²¹ and “增材制造产业发展行动计划(2017-2020年)” (Additive Manufacturing Industry Development Action Plan, 2017-2020).²²

The 2024 Government Work Report further directed the state to “*vigorously advance a modern industrial system and accelerate new productive forces*.” It also called for upgrading industrial and supply chains, strengthening advanced manufacturing clusters, supporting specialized firms, and improving standards and quality systems. AM fits this framework

¹⁷ Pan Xuesong, “An inside perspective on China's thriving metal additive manufacturing industry”, Metal AM, April 5, 2023.

¹⁸ Elsa Kania and Peter Wood, in William C. Hannas and Didi Kirsten Tatlow, eds., “China's Quest for Foreign Technology: Beyond Espionage”, Routledge, 2021, p. 228.

¹⁹ Karen M. Sutter, in William C. Hannas and Didi Kirsten Tatlow, eds., “China's Quest for Foreign Technology: Beyond Espionage”, Routledge, 2021, p. 58–60.

²⁰ State Council of the People's Republic of China, “国务院关于印发《中国制造2025》的通知”, May 19, 2015.

²¹ 工业和信息化部, “国家增材制造产业发展推进计划(2015-2016年)”, February 28, 2015.

²² Ministry of Industry and Information Technology, “十二部门关于印发《增材制造产业发展行动计划(2017-2020年)》的通知”, January 17, 2017.



because it links high-end equipment, advanced materials, industrial software, quality control, and application-specific production knowledge.²³

The IMF estimates that the People's Republic of China (PRC) devoted the equivalent of around 4.4% of GDP to industrial-policy support in 2023, encompassing cash subsidies, tax benefits, subsidized land, and preferential credit.²⁴ Similar OECD analysis highlights China's outsized use of such support, finding that Chinese firms received on average three to eight times more subsidies than firms in OECD economies between 2005 and 2024, with below-market borrowing playing an especially important role.²⁵ The European Commission also identifies significant state influence over capital allocation, including targeted financing, special funds, procurement, and technology-upgrading programs under initiatives such as Made in China 2025. Together, these measures can reduce financing constraints and accelerate investment in strategically important manufacturing technologies, including additive manufacturing.²⁶

This national policy framework is reinforced at the provincial level. Jiangsu's "Additive Manufacturing Industry Three-Year Action Plan (2018–2020)" supported key technology breakthroughs, equipment and component R&D, commercialization, and industrialization through national R&D programs, demonstration policies, financing instruments, and capital-market access.²⁷ Guangdong—China's largest laser and AM industry cluster and a major hub for desktop 3D-printer companies such as Shenzhen-based Bambu Lab—similarly adopted an "Action Plan for Cultivating Strategic Emerging Industry Clusters of Laser and Additive Manufacturing (2021–2025)", targeting industrial scale, innovation, key technologies, and development of a more complete domestic value chain.²⁸ Together, these measures show how national AM priorities are translated into layered local support that lowers the cost and risk of moving from research to commercial production. This process is further reinforced by market-access conditions, including localization requirements, joint ventures, procurement rules, and other commercial arrangements

²³ National Development and Reform Commission, "《政府工作报告》（全文）", March 20, 2024.

²⁴ Garcia-Macia, D., Kothari, S., & Tao, Y. "Industrial policy in China: Quantification and impact on misallocation" (IMF Working Paper No. 2025/155). *International Monetary Fund*, 2025.

²⁵ Sauvage, J., "Industrial subsidies hit USD 108 billion and reshape global competition", *Organisation for Economic Co-operation and Development*, June 1, 2025.

²⁶ European Commission, "Commission Staff Working Document on Significant Distortions in the Economy of the People's Republic of China for the Purposes of Trade Defence Investigations", 10 April 2024.

²⁷ Jiangsu Provincial Economic and Information Commission et al., "江苏省增材制造产业发展三年行动计划（2018–2020年）", August 28, 2018.

²⁸ Guangdong Provincial Department of Science and Technology, "广东省培育激光与增材制造战略性新兴产业集群行动计划（2021–2025年）图解", December 8, 2020.



that have historically encouraged the transfer of foreign know-how and the development of domestic supplier capabilities.²⁹

China's 14th Five-Year Plan explicitly identified additive manufacturing as a priority area for development, reflecting its strategic role within the country's advanced-manufacturing agenda.³⁰ According to the Ministry of Industry and Information Technology (MIIT) Equipment Industry Development Center, China's AM industry grew from RMB 20.8 billion in 2021 to RMB 70 billion in 2025, ranking first globally in consumer-grade equipment output and second in overall scale. The sector includes more than 2,000 specialized firms, around 250 above-scale enterprises, and over 60 national-level "Little Giant" companies. Domestic capabilities have also strengthened, reaching 95% for specialized materials and nearly 70% domestic market share for fiber lasers, while applications have expanded across aerospace, medical, consumer electronics, automotive, low-altitude equipment, and humanoid robotics.³¹

Crealty, one of the leading desktop 3D-printer manufacturers, illustrates how China's broader industrial-policy framework translates into firm-level support. The company's revenue rose from RMB 1.88 billion in 2023 to RMB 3.13 billion in 2025, while it was recognized as a national-level "Little Giant" enterprise and subsequently as a "Key Little Giant." Its prospectus also records government grants of RMB 34.6 million in 2023, RMB 10.1 million in 2024, and RMB 16.3 million in 2025, supporting operations, R&D, and talent recruitment, alongside VAT refunds and preferential tax treatment for advanced-manufacturing enterprises.³² BLT illustrates another layer of support: its 2024 annual report records project-specific subsidies for metal AM equipment, aerospace applications, technology upgrading, and localization of key components, linking state support directly to the build-out of dual-use industrial capacity and import substitution.³³

The industrial-policy model is therefore cumulative: national policy defines AM as strategic, provincial plans build clusters, standards, financing, and demonstration applications, while firm disclosures show support for industrialization, R&D, and localization. For the 15th Five-Year Plan (2026–2030), MIIT's Equipment Industry Development Center targets an industry scale above RMB 150 billion, with priorities

²⁹ Karen M. Sutter, in William C. Hannas and Didi Kirsten Tatlow, eds., *"China's Quest for Foreign Technology: Beyond Espionage,"* Routledge, 2021, p. 60–64.

³⁰ State Council of the People's Republic of China, *"中华人民共和国国民经济和社会发展第十四个五年规划和2035年远景目标纲要,"* March 13, 2021.

³¹ MIIT Equipment Industry Development Center, *"为制造强国注入新动能：增材制造产业‘十四五’答卷与‘十五五’展望,"* January 8, 2026.

³² Shenzhen Crealty 3D Technology Co., Ltd., *"Global Offering Prospectus,"* Hong Kong Stock Exchange, May 29, 2026.

³³ Xi'an Bright Laser Technologies Co., Ltd. (BLT), *"2024 Annual Report,"* April 29, 2025.



including high-performance materials, core technology autonomy, AI integration, intelligent manufacturing, regional coordination, and supply-chain resilience.³⁴ Although AM is not mentioned explicitly, it intersects with advanced materials, industrial software, AI, high-end equipment, supply-chain security, and intelligent manufacturing. This suggests that AM is becoming embedded within a wider advanced-manufacturing system.³⁵

Across the region, AM is likewise increasingly treated as a strategic manufacturing technology, although national priorities differ. Japan's 2025 industrial strategy sets an explicit target of increasing its share of the global metal-AM market from below 10% to 20% by 2040, while expanding its use in aerospace and other high-value manufacturing sectors.³⁶ India's 2022 National Strategy presents AM as a technology with the potential to reshape industrial production through digital design and engineering, while promoting indigenous technologies, local supply chains, skills development, and reduced dependence on imported capabilities.³⁷ Taiwan links intelligent metal AM more directly to civil-military technology development and defense-industrial resilience,³⁸ while also seeking to strengthen diversified, "non-red" supply chains that reduce reliance on PRC-linked suppliers and connect domestic firms more closely with international partners.³⁹

The regional comparison indicates that the key difference lies not in strategic interest in AM itself, but in the scale and integration of the system supporting it. What matters, therefore, is less whether China leads in every AM technology than whether the Party-state can coordinate materials, software, equipment, finance, standards, certification, industrial clusters, and downstream users into a self-reinforcing ecosystem. The available evidence suggests that this is the direction of Chinese policy. The resulting distortion affects not only established Western manufacturers, but also the formation of new firms: if Chinese state-supported scale and pricing undermine the economics of market entry, they also make Western AM startups harder to finance. The risk, therefore, is not only erosion of the existing Western production base, but a gradual concentration of the next generation of AM companies and capabilities in China.

³⁴ MIIT Equipment Industry Development Center, op. cit.

³⁵ Michael Petch, "China's 15th Five-Year Plan: What It Means for Additive Manufacturing in China and What Has Changed Since 2021", *3D Printing Industry*, March 31, 2026.

³⁶ Ministry of Economy, Trade and Industry of Japan, "FY2025 Vision for the Machine Parts and Tooling Industries Formulated", March 28, 2025.

³⁷ Press Information Bureau, Government of India, "National Strategy on Additive Manufacturing", February 24, 2022.

³⁸ Ministry of National Defense, Republic of China (Taiwan), "2025 National Defense Report", 2025.

³⁹ Ministry of National Defense, Republic of China (Taiwan), "Securing Defense Supply Chain", 2025.



4. AM Integration into China's Defense Industrial Base

Like other emerging technologies, AM is being widely adopted by major global military powers. The PRC is no exception to the trend. The People's Liberation Army (PLA) and Chinese defense conglomerates utilize AM to manufacture components for military aerospace use,⁴⁰ on-battlefield 3D printing of weapons parts⁴¹ as well as for on-board repair of damaged warships while deployed at sea.⁴² The Chinese government's recognition of AM's dual-use potential led to significant investment and support for R&D, effectively blurring the line between its civilian and military side.

First link between the civilian AM research and the PLA date back to 2001, when research into titanium alloy laser rapid forming was sponsored by the predecessors of the Equipment Development Department of Central Military Commission (军委装备发展部) and State Administration of Science, Technology and Industry for National Defense (SASTIND, 国防科工局). These two institutions are PLA-linked civilian governmental bodies tasked with defense procurement and military R&D.⁴³ The state support bore fruit and led to one of the first major successes of Chinese AM around 2012, when the research team headed by Wang Huaming (王华明) produced world's largest 3D printed titanium aircraft component.⁴⁴ The team's achievement was rewarded by the prestigious State Technological Invention Award (国家技术发明奖) and, arguably, brought the central government's attention to AM.⁴⁵

In 2015 and 2017, respectively, Beijing issued its first two nationwide AM development plans: 《国家增材制造产业发展推进计划（2015 - 2016年）》 and 《增材制造产业发展行动计划（2017 - 2020年）》. These plans explicitly highlighted a need for the military application of technological breakthroughs achieved through AM. While the 2015 plan specifically targeted national defense aerospace projects,⁴⁶ the 2017 plan demanded the "vigorous" application of AM across defense industry as well as the accelerated

⁴⁰ Eric Anderson, "Additive Manufacturing in China: Aviation and Aerospace Applications (Part 2)", May 9, 2013.

⁴¹ SCMP, "China's military tests remote 3D printed parts and drone delivery for battlefield: report", December 27, 2024.

⁴² Global Times, "中国战舰配备3D打印方舱 战时可极大提升生存力", January 8, 2015.

⁴³ China Aviation News, "中国首创3D打印造飞机钛合金大型主承力构件", January 21, 2013

⁴⁴ Eric Anderson, "Additive Manufacturing in China: Aviation and Aerospace Applications (Part 2)", May 9, 2013, 1, 3-4.

⁴⁵ Eric Anderson, "Additive Manufacturing in China: Threats, Opportunities, and Developments (Part 1)", May 1, 2013, 2-3.

⁴⁶ Cyberspace Administration of China, "国家增材制造产业发展推进计划（2015-2016年）", March 2, 2015, 3, 15.



development of dual-use technology under the framework of Military-Civil Fusion policy (MCF, 军民融合).⁴⁷

MCF aims to boost the PRC's economic and military power through maximizing ties and cooperation between civilian and defense R&D.⁴⁸ Overseen by SASTIND, the policy connects at least 60 civilian universities with the PLA and defense companies through on-campus defense laboratories. MCF grants military bodies a cover which gives them access to civilian talent and know-how. The policy also allows them to engage in foreign exchanges or in rare cases to conduct espionage and cyberattacks.⁴⁹

After the US sanctioned multiple MCF-affiliated entities, overt mentions of defense-related work became much rarer in governmental, business, and academic documents.⁵⁰ Nonetheless, links between Chinese AM companies and the PLA persist, as demonstrated by the following examples.

⁴⁷ China Association of Automobile Manufacturers, “关于印发《增材制造产业发展行动计划（2017-2020年）》的通知”, December 15, 2017.

⁴⁸ Audrey Fritz, “The foundation of innovation under military-civil fusion: The role of universities”, *Sinopsis*, October 8, 2021.

⁴⁹ Alex Joske, *The China Defense Universities Tracker*, November 25, 2019, 4, 9-10, 12, 25-26.

⁵⁰ Aaron McNicholas, “China's Military-Civil Defusion”, September 22, 2024.



5. When the PLA Is Always Just a Step Away: the MCF Ecosystem Case Study

5.1. NORINCO

The giant defense conglomerate NORINCO Group, which operates its own Additive Manufacturing Technology Research and Application Center (中国兵器工业增材制造技术研究应用中心), perfectly embodies the MCF state-academia-business nexus. The center is funded by a defense SOE and their academic partners include not only a SASTIND supervised university, but also the Nanjing University of Science and Technology (南京理工大学), which is part of the Seven Sons of National Defense (国防七子).⁵¹ These, together with the Seven Sons of National Arms Industry (兵工七子) are the most deeply embedded civilian universities in the Chinese defense sector.⁵²

NORINCO's AM research center is led by Xu Hong (徐宏), who has headed more than 30 defense-related research projects, including programs for SASTIND, the Central Military Commission Science and Technology Commission, and the CMC Equipment Development Department. His work spans additive manufacturing, advanced materials, and equipment development, and he has received multiple national-defense science and technology awards.⁵³ Xu framed the center's commercialization logic explicitly in 2016, stating that "3D printing + traditional manufacturing has already demonstrated its strengths in the weapons sector, and it will also become a 'sharp sword' in the civilian sector."⁵⁴

That logic remains visible in Beifang Hengli Technology Development Co. (北京北方恒利科技发展有限公司), the center's lead organization, which opened a new Xiong'an production base in 2025 for industrial AM equipment serving defense, aerospace, automotive, and other sectors.⁵⁵ Xiong'an authorities are simultaneously building an AM ecosystem spanning R&D, pilot production, industrialization, and supplier development,

⁵¹ 3D Printing World, "3D打印聚焦军工！中国兵器工业增材制造技术研究应用中心在京揭牌", October 14, 2015.

⁵² Alex Joske, [The China Defense Universities Tracker](#), November 25, 2019.

⁵³ School of Material Science and Engineering, 徐宏, March 26, 2010.

⁵⁴ 3D Printing World, "恒利科技：揭秘中国首家军工3D打印企业", July 18, 2016.

⁵⁵ 澎湃新闻, "北方恒利雄安生产基地，正式投产运营！", April 19, 2025.



bringing defense-linked capabilities into closer contact with civilian firms, research teams, and local industrial policy.⁵⁶

5.2. BLT

BLT (Xi'an Bright Laser Technologies, 铂力特) is China's largest metal AM company⁵⁷ which focuses on industrial metal AM. Unlike NORINCO, its English website gives the impression of a purely civilian enterprise, containing merely one subtle and possibly accidental mention of the fact that the company provides services to clients in the defense sector.⁵⁸ However, upon closer examination, multiple ties to the PLA emerge.

First, BLT's founder and chairman Huang Weidong (黄卫东) works as a professor at the Northwestern Polytechnical University (NPU, 西工大), which is among the Seven Sons of National Defense. Even among the Seven Sons, NPU has particularly strong links to the defense sector. For example, in 2017, 41.3% of NPU graduates ended up working in defense.⁵⁹ Huang also directs NPU's State Key Laboratory of Solidification Technology (凝固技术全国重点实验室), which according to its website assists in the development and manufacturing of national defense equipment.⁶⁰

Aside from having personal links to MCF-linked institutions, Chinese consultancy AVIC Securities also describes BLT as a participant in key national defense programs and SASTIND commissioned projects.⁶¹ Finally, the company's Chinese language website mentions partnership with SASTIND supervised company (西安航天发动机有限公司)⁶² and the PLA Air Force Medical University (空军军医大学).⁶³ Despite its civilian image, BLT seems to be interlinked with the MCF ecosystem in similar ways as NORINCO's AM research center.

This institutional overlap also complicates attempts to firewall civilian cooperation from military applications, particularly where the same firms, laboratories, universities, and

⁵⁶ Xiong'an New Area, “未来之城 ‘御风前行’”, November 11, 2025.

⁵⁷ AMPulse, “BLT reports 2025 revenue growth amid ongoing SEC investigation for disclosure violations”, May 1, 2026.

⁵⁸ BLT, “110 Units of Systems, BLT Reveals 3D Printing Innovation Power”, July 10, 2018.

⁵⁹ Alex Joske, *The China Defense Universities Tracker*, November 25, 2019, 6-7.

⁶⁰ State Key Laboratory of Solidification Processing, “实验室概况”, n.d.

⁶¹ Avic Securities, “铂力特 (688333.SH) 深度报告: 国内航空航天金属增材制造龙头”, June 29, 2021, 8.

⁶² BLT, “用户故事 | 西安航天发动机有限公司: 3D打印助力航天液体动力研制生产释放新动能!”, February 20, 2021.

⁶³ BLT, “铂力特参与项目荣获陕西省科学技术奖, 助力口腔修复数字化升级”, September 2, 2025.



personnel participate across both ecosystems.⁶⁴ Regardless of its apparent proximity to the Chinese defense sector, a few cutting-edge European tech companies still cooperate with BLT, including Siemens⁶⁵ and Airbus,⁶⁶ which even runs a trilateral joint R&D effort with BLT and NPU. Against the backdrop of the Pentagon recently banning all Chinese AM hardware and software from defense procurement over security concerns, these partnerships might turn out to be problematic in future.⁶⁷

5.3. Bambu Lab

Although industrial-grade AM companies (such as BLT) produce the most sophisticated form of the technology, it has been the entry-level 3D printers that have driven the sector's growth lately. Chinese companies dominate this segment, reportedly holding over 90% market share in 2025.⁶⁸ The market is also highly concentrated: in the first quarter of 2026, Bambu Lab, Creality, Elegoo, and Anycubic collectively accounted for 88% of global entry-level shipments.⁶⁹ While it only takes a computer and a few hundred euros to operate the entry-level printers, they still have a significant dual-use potential. 3D-printed guns, weapon components, and drones are now a common sight at the battlefields in Ukraine, Yemen,⁷⁰ and Myanmar.⁷¹ This combination of market concentration and dual-use diffusion increases the significance of vendor-controlled software, authentication, and cloud infrastructure as entry-level printers move further into professional prototyping and distributed production.

⁶⁴ Elsa Kania and Peter Wood, in William C. Hannas and Didi Kirsten Tatlow, eds., *“China’s Quest for Foreign Technology: Beyond Espionage”*, pp. 228–230. Routledge, 2021.

⁶⁵ BLT, *“BLT and Siemens Join Forces to Drive Forward the Development of Metal Additive manufacturing, open a new chapter of strategic cooperation”*, May 15, 2023.

⁶⁶ BLT, *“From Supplier to Joint R&D Partners, BLT to gether with Airbus Enter a New Era of Aerospace Application with Metal Additive Manufacturing”*, December 27, 2018.

⁶⁷ Anier Tenorio Lara, *“U.S. blocks additive manufacturing systems tied to China, Russia, Iran, and North Korea from defense procurement”*, January 6, 2026.

⁶⁸ Context, *“Quarterly Industrial 3D Printer Shipments Rebound Amid Continued Record-Breaking Entry-Level Growth”*, April 15, 2026.

⁶⁹ Context, *“Quarterly Global Industrial 3D Printer Shipments Surge on the Back of Strong Defence and 3C Sector Demand”*, July 9, 2026.

⁷⁰ Michael Horton, *“Yemen’s drone doom loop: A model of instability for fragile states Yemen’s drone doom loop: A model of instability for fragile states”*, November 17, 2023.

⁷¹ Manuel Nicola Primitivi, *“Anti-Junta Rebels Resort to 3D-Printed Weapons in Myanmar”*, June 5, 2024.



At the very top of the desktop printer food chain sits the Shenzhen-based Bambu Lab (拓竹), which holds 37% of the global market.⁷² The company was founded by five engineers who previously worked for DJI, a leading drone manufacturer,⁷³ which is designated by the Pentagon and American courts as a MCF-linked company.⁷⁴ The same goes for one of Bambu Lab's first investors IDG Capital⁷⁵ which the US classified as a military-linked enterprise for almost a year before removing it from the list.⁷⁶

Additionally, Bambu Lab established the "2026 Alma Mater Fund" (2026母校基金), which supports the universities attended by firm's employees. Out of the ten universities, six are supervised by SASTIND.⁷⁷ Amongst them is the Harbin Institute of Technology (HIT, 哈工大) one of the Seven Sons of National Defense. Given that 36,5% of HIT graduates end up working in defense,⁷⁸ it is reasonable to assume that personal connections exist between the current Bambu Lab staff and their former classmates working in MCF linked entities.

Finally, at least three of Bambu Lab's Chinese distributors provide services to clients in the defense sector⁷⁹ such as the SOEs that produce PLA military aircraft⁸⁰ or run the PRC space and missile programs.⁸¹ One of them also supplies the National University of Defense Technology (国防科技大学), which is directly subordinate to the CCP's Central Military Commission (CMC).⁸²

Bambu Lab printers have also been used by the U.S. Air Force,⁸³ the British Army,⁸⁴ and, increasingly, Czech defence institutions. In 2023, the Ministry of Defence purchased a Bambu Lab X1 Carbon for the 102nd Reconnaissance Battalion to support the

⁷² Context, "Quarterly Industrial 3D Printer Shipments Rebound Amid Continued Record-Breaking Entry-Level Growth", April 15, 2026.

⁷³ BrandsFactory, "海龟博士从大疆离职创业，拓竹科技Bambu Lab案例分享", June 18, 2024

⁷⁴ Mike Scarcella, "Drone maker DJI loses lawsuit to exit Pentagon's list of firms with Chinese military ties", September 26, 2025.

⁷⁵ IDG, IDG Capital, n.d.

⁷⁶ Private Equity Wire, "IDG Capital removed from Pentagon's Chinese military ties list", December 18, 2024.

⁷⁷ 界面新闻, "深圳一公司向员工母校捐赠超1亿元，2025年营收已破百亿", January 28, 2026.

⁷⁸ Alex Joske, "The China Defense Universities Tracker", November 25, 2019, 7.

⁷⁹ GYD 3D, "从开模等待到按需打印，3D打印如何架起航空航天轻资产之路", May 22, 2025.

⁸⁰ JBEOS, "装备制造行业（含军工制造行业）信息化整体解决方案", n. d.

⁸¹ 运通智造, "湖南云通：合作伙伴", n.d.

⁸² Hunan Today, "湖南云通：三载深耕结硕果 双证加持启新程", March 13, 2026.

⁸³ Alex Tyler Jones, "USAF Leverages Bambu Lab 3D Printers for Attack Drone Maintenance", February 27, 2025.

⁸⁴ Ada Shaikhmag, "MOD Probes Security Risks of Chinese 3D Printers in Military Exercises", April 30, 2026.



“acceleration of repairs of materiel and equipment.”⁸⁵ In 2024, it acquired another X1C for “minor repairs, production of prototypes, equipment accessories and fixtures.”⁸⁶ The Ministry also procured Bambu Lab equipment for the University of Defence’s Faculty of Military Technology to “develop capabilities and knowledge in additive technologies,” including 3D printing and improving the properties of printed parts.⁸⁷

Unlike its industrial-level counterpart BLT, Bambu Lab is likely not directly linked to China’s defense sector. However, it operates within a broader Chinese technology ecosystem in which MCF-linked institutions and actors are often closely connected to commercial innovation. Given the dual-use nature of Bambu Lab’s products, this proximity does not in itself establish a defense relationship, but it does make the company’s growing presence in Western military environments increasingly sensitive. Fears of potential cooperation between the company and Chinese authorities is the reason why the British MoD currently conducts a security inquiry into Bambu Lab printers used by the British Army.⁸⁸

⁸⁵ Hlídač státu, “[Nákup 3D tiskárny a gravírovacího stroje s příslušenstvím](#)”, November 3, 2023.

⁸⁶ Hlídač státu, “[NS 229800 – 3D Tiskárny](#)”, October 29, 2024.

⁸⁷ Hlídač státu, “[24041/2024-SED – Nákup 3D tiskárny a příslušenství](#)”, July 8, 2024.

⁸⁸ Ada Shaikhmag, op. cit.



6. Cyber Espionage and China's Pursuit of Technological Advantage

Cyber espionage is one of the principal instruments through which the PRC pursues technological self-reliance and competitive advantage, closely coupled with published industrial policy. For over a decade the Ministry of State Security (MSS) and, since 2015 to a lesser extent, the People's Liberation Army (PLA) have sponsored or directed intrusions to acquire foreign intellectual property and strategic information. The seminal 2013 Mandiant APT1 report first tied a PLA-affiliated unit's targeting directly to China's 12th Five-Year Plan.⁸⁹ Analysts have since continued to characterize state-aligned cyber espionage as a means of accelerating development in sectors Beijing considers strategically important.⁹⁰

The line between state direction and private contracting is diminishing. The leaked materials from the contractor i-Soon revealed a commercial "APT-as-a-service" business model,⁹¹ and groups such as APT41 blend espionage with financially motivated cybercrime.⁹² U.S. Cybersecurity and Infrastructure Security Agency (CISA) assessed in 2020 that PRC actors continue to pursue intellectual property and personal data to advance the country's competitive position.⁹³ The activity and focus of Chinese state-linked threat actors has only increased.

China's Five-Year Plans (FYPs) are the country's principal economic-policy guidance, and threat-intelligence practitioners increasingly treat them as a leading indicator of future cyber targeting: cyber-enabled IP theft has repeatedly followed declared FYP priorities within a few years of publication.⁹⁴

- 12th FYP (2011–2015): Mandiant found that APT1 targeted at least four of the seven strategic emerging industries identified in the plan.⁹⁵
- 13th FYP (2016–2020): Beijing prioritized 5G development and commercialization; China-linked cyber-espionage groups subsequently

⁸⁹ Mandiant, "APT1: Exposing One of China's Cyber Espionage Units", 2013.

⁹⁰ Jack Evans, "Wondering Where China's Cyber Effort Will Go Next? Just Read the Five-Year Plan", *The Strategist* (ASPI), 2026.

⁹¹ CybelAngel, "Cyber Espionage and APTs: Chinese Threat Groups in 2026", April 26, 2026.

⁹² Google Cloud Blog (Mandiant), "APT41, A Dual Espionage and Cyber Crime Operation", August 7, 2019.

⁹³ CISA, "Potential for China Cyber Response to Heightened U.S.–China Tensions" (Advisory AA20-275A), October 20, 2020.

⁹⁴ Jack Evans, "Wondering Where China's Cyber Effort Will Go Next? Just Read the Five-Year Plan", *The Strategist* (ASPI), March 31, 2026.

⁹⁵ Mandiant, op. cit.



targeted global telecommunications providers, including campaigns seeking 5G-related technical information.⁹⁶

- 14th FYP (2021–2025) & Made in China 2025: elevated semiconductors, new-energy vehicles, biotech, and advanced materials; CrowdStrike observed rising operational tempo as trade friction intensified.^{97 98}
- 15th FYP (2026–2030): priorities include semiconductors, AI, industrial software, advanced materials, and high-end manufacturing, with AM implicitly included and likely to influence future targeting.⁹⁹

Governments and vendors increasingly use these industrial-policy documents as a predictive input for threat modeling rather than waiting for intrusions to surface.¹⁰⁰

6.1. AM and its Supply Chain as Emerging Targets

The scale of the technology-transfer risk extends beyond conventional cyber espionage. U.S. assessments have estimated annual losses from IP theft at \$225–600 billion, with China responsible for an estimated 50–80 percent.¹⁰¹ Documented cases have involved proprietary source code, engineering drawings, material specifications, manufacturing know-how, and sensitive blueprints for advanced military technologies.^{102 103 104} In digitally enabled manufacturing, access to such assets can substantially shorten the path from R&D to replication.

AM makes this risk particularly acute because valuable IP increasingly resides within connected printers, slicers, and cloud infrastructure. Bambu Lab's own security documentation acknowledges that its cloud services may process design models, printing parameters, usage records, and other potentially sensitive information.¹⁰⁵ The company has also introduced tighter authorization controls over printing, remote functions, and

⁹⁶ Jack Evans, op. cit.

⁹⁷ CSO Online, "[China's Next Five-Year Plan Offers Preview of Cybersecurity Targets](#)" (citing CrowdStrike's Adam Meyers), April 2, 2019.

⁹⁸ QuoIntelligence, "[China's Five-Year Plan: A Pursuit for GDP Growth and Technological Self-Sufficiency](#)", March 17, 2021.

⁹⁹ Jack Evans, op. cit.

¹⁰⁰ SecAlliance, "[China's Five-Year Plan and Its Implications for the Cyber Threat Landscape](#)", October 27, 2021.

¹⁰¹ U.S.-China Economic and Security Review Commission, "[2022 Annual Report to Congress](#)", November 2022.

¹⁰² U.S. Department of Justice, "[Chinese National Pleads Guilty to Economic Espionage and Theft of a Trade Secret From U.S. Company](#)", May 19, 2017.

¹⁰³ U.S. Department of Justice, "[Former GE Engineer and Chinese Businessman Charged with Economic Espionage and Theft of GE's Trade Secrets](#)", April 23, 2019.

¹⁰⁴ U.S. Department of Justice, "[Engineer Pleads Guilty to Stealing for Chinese Government's Benefit Trade Secret Technology Designed for Missile Launch and Detection](#)", July 21, 2025.

¹⁰⁵ Bambu Lab, "[Security White Paper](#)", September 2025.



third-party software access, illustrating the degree of control increasingly embedded in the software layer.¹⁰⁶

Recent disclosures show that vendor software and authentication can themselves create security exposure. In 2025, a vulnerability in Bambu Studio that could allow malicious code to run on a user's computer was fixed roughly a year after it was first reported to the vendor.¹⁰⁷ Bambu Connect's embedded authentication certificate and private key were also extracted, creating a potential route for unauthorized commands to be accepted by printers.¹⁰⁸ A separate vulnerability in the Creality Cloud Android application could allow a malicious app to interfere with the login process and potentially obtain user credentials.¹⁰⁹

These developments have generated broader concern within the AM and open-source communities over cloud dependence, vendor control, and the ability to independently audit software handling sensitive manufacturing data. In 2026, Software Freedom Conservancy concluded that Bambu Studio did not provide complete corresponding source code for its networking component.¹¹⁰ Broader discussion across the AM community has also raised concerns about the growing dependence on vendor-controlled software, authentication systems, and cloud infrastructure.¹¹¹ Patent litigation involving Bambu Lab further underscores the growing commercial stakes around proprietary AM technologies, although such disputes do not themselves establish IP theft.¹¹²

These issues are particularly relevant in aerospace, defense, and automotive supply chains, which recur throughout China's industrial priorities and increasingly depend on digitally connected manufacturing systems. Reliance on digital design files (CAD/STL) and networked printers creates cyber-physical exposures that are distinct from conventional manufacturing and represent a concern formally recognized by standards bodies such as the America Makes/ANSI AM Standardization Collaborative.¹¹³

¹⁰⁶ Bambu Lab, "[Firmware Update Introducing New Authorization Control System](#)", January 16, 2025.

¹⁰⁷ Gianluca Palma, "[CVE-2025-57521: Arbitrary Code Execution Vulnerability in Bambu Studio](#)", GitHub, June 26, 2025.

¹⁰⁸ Maya Posch, "[Bambu Connect's Authentication X.509 Certificate And Private Key Extracted](#)", Hackaday, January 19, 2025.

¹⁰⁹ National Vulnerability Database, "[CVE-2025-10716](#)", September 19, 2025.

¹¹⁰ Software Freedom Conservancy, "[Comprehensive Response to Bambu's AGPLv3 Violations](#)", May 18, 2026.

¹¹¹ Ars Technica, "[Bambu Lab Pushes a 'Control System' for 3D Printers, and Boy, Did It Not Go Well](#)", January 21, 2025.

¹¹² *Stratasys, Inc. v. Shenzhen Tuozhu Technology Co. Ltd. et al.*, U.S. District Court for the Eastern District of Texas, "[Case No. 2:24-cv-00644](#)", filed August 8, 2024.

¹¹³ Metal AM, "[Cybersecurity in Additive Manufacturing: Securing the Industry's Future](#)", 2023.



Connected AM equipment should therefore be treated not only as manufacturing machinery but also as networked computing infrastructure. Modern desktop printers can combine vendor-cloud access, remote command functions, cameras and other sensors with direct connectivity to engineering networks. The resulting exposure extends beyond theft of design files to remote manipulation of print jobs, cyber-physical sabotage, and use of the printer as a foothold for wider network compromise.

AM technologies are specifically vulnerable to following:

- Design-file theft: weakly protected CAD/STL files enable illicit replication of proprietary parts; research has demonstrated exfiltration via acoustic and optical side-channel emissions from printers.¹¹⁴
- Digital-thread exposure: the data trail spanning design, scanning, and production can reveal process and material specifications of high intelligence value.¹¹⁵
- File tampering and sabotage: undetected manipulation of fill patterns or build parameters can introduce latent defects in safety-critical parts.¹¹⁶
- In one experiment, researchers altered a 3D-printed drone propeller so that it appeared visually intact but failed during flight.¹¹⁷
- Service-bureau¹¹⁸ exposure: outsourced printing expands the attack surface to third-party vendors with weaker security, mirroring the China-nexus preference for supply-chain compromise.¹¹⁹

This maps directly onto observed China-nexus interest in the defense industrial base, where Google Threat Intelligence Group (GTIG) reports persistent targeting of “force-multiplying” entities such as managed service providers and supply-chain nodes,¹²⁰ a category that already includes AM service bureaus and is likely to grow as AM adoption deepens.¹²¹

¹¹⁴ Seyed Ali Ghazi Asgar and Narasimha Reddy, “[QuietPrint: Protecting 3D Printers Against Acoustic Side-Channel Attacks](#)”, February, 2026.

¹¹⁵ Deloitte Insights, republished by Supply Chain Navigator, “[Cyber Risks in Additive Manufacturing Threaten to Unravel the Digital Thread](#)”, April, 2018.

¹¹⁶ Inside Metal Additive Manufacturing, “[Comprehensive Threat Landscape in Additive Manufacturing: Understanding Cyber-Physical Vulnerabilities](#)”, 2024.

¹¹⁷ USENIX, “[drOwned – Cyber-Physical Attack with Additive Manufacturing](#)”, August 2017.

¹¹⁸ A service bureau is a third-party company that specializes in 3D printing and produces parts for other businesses on demand.

¹¹⁹ Mahender Kumar, Gregory Epiphaniou, and Carsten Maple, “[Comprehensive Threat Analysis in Additive Manufacturing Supply Chain: A Hybrid Qualitative and Quantitative Risk Assessment Framework](#)”, *Production Engineering*, May 9, 2024.

¹²⁰ Google Cloud Blog (Google Threat Intelligence Group), “[Threats to the Defense Industrial Base](#)”, February 10, 2026.

¹²¹ Industrial Cyber, “[Google Flags Sustained Cyber Pressure on Defense Industrial Base from Russia, China-Linked Actors](#)”, February 11, 2026.



6.2. China-Nexus Targeting of the Technology Sector

China-nexus groups sustain a high tempo of intrusions against the technology sector — software vendors, Software-as-a-Service (SaaS) providers, semiconductor firms, and even security vendors — both for IP value and as a stepping-stone into downstream customers. This threat model is directly relevant to AM, where software platforms, cloud services, machine-control systems, and digital manufacturing files create similar opportunities for IP theft and supply-chain compromise.

- SaaS/IT-supply-chain compromise: Google reported actors breaching technology and SaaS firms with the BRICKSTORM backdoor before pivoting into customer networks, comparable to Russia's SolarWinds campaign.¹²²
- Cloud/virtualization targeting: CrowdStrike's Warp Panda cluster has focused on VMware vCenter and Azure, harvesting credentials and replaying session tokens to reach Microsoft 365 data.¹²³
- Trusted-relationship abuse: Murky Panda / Silk Typhoon exploits trust between SaaS providers and downstream tenants, alongside rapid n-day/zero-day weaponization.¹²⁴
- Security-vendor targeting: a China-nexus cluster reconnoitered SentinelOne's infrastructure and compromised a logistics provider servicing the company.^{125 126}
- Semiconductor-specific operations: three China-aligned clusters ran parallel 2025 campaigns against Taiwanese semiconductor and supply-chain firms using fake job-applicant lures.¹²⁷

Major incidents in 2024–2025 point to a growing pattern of stealthy cyber-espionage targeting technology manufacturers and their supply chains. China-aligned actors targeted Taiwan's semiconductor sector through fake job applications and phishing, putting sensitive technical and commercial information at risk.¹²⁸ Other campaigns, such as PurpleHaze, exploited vulnerable internet-facing gateways to gain and maintain access

¹²² Eric Geller, "China-Linked Groups Are Using Stealthy Malware to Hack Software Suppliers", Cybersecurity Dive, September 24, 2025.

¹²³ TechRepublic, "CrowdStrike Identifies New China-Nexus Espionage Actor (Warp Panda)," December 5, 2025.

¹²⁴ Ravie Lakshmanan, "Chinese Hackers Murky, Genesis, and Glacial Panda Escalate Cloud and Telecom Espionage", The Hacker News, August 22, 2025.

¹²⁵ Ravie Lakshmanan, "Over 70 Organizations Across Multiple Sectors Targeted by China-Linked Cyber Espionage Group", The Hacker News, June 9, 2025.

¹²⁶ Aleksandar Milenkoski and Tom Hegel, "Follow the Smoke: China-nexus Threat Actors Hammer At the Doors of Top Tier Targets", SentinelLABS, June 9, 2025.

¹²⁷ Ravie Lakshmanan, "Chinese Hackers Target Taiwan's Semiconductor Sector with Cobalt Strike, Custom Backdoors", The Hacker News, July 17, 2025

¹²⁸ Proofpoint, "Phish and Chips: China-Aligned Espionage Actors Ramp Up Taiwan Semiconductor Industry Targeting", July 16, 2025.



inside manufacturers and technology providers.¹²⁹ BRICKSTORM followed a similar pattern, using long-lived backdoors on poorly monitored devices and raising the risk that one compromised provider could expose customers further down the supply chain.¹³⁰

Two broader themes recur across these incidents: a preference for compromising supply-chain and managed-service providers rather than attacking hardened targets directly, and the use of the technology sector both as an end target and as a pathway into downstream victims.

6.3. Regulatory Weaponisation of Vulnerability Disclosure

More broadly, even nominally private technology firms in the PRC, including those in AM, operate under a legislative framework requiring cooperation with the Party-state. This is particularly relevant given AM's dependence on sensitive CAD files, machine telemetry, process parameters, materials data, and customer information. The National Intelligence Law of the PRC (2017, amended 2018), Article 7, requires all organizations and citizens to "support, assist, and cooperate with national intelligence efforts,"¹³¹ while the Cybersecurity Law (2016) obliges network operators to provide technical support and assistance to public and state security organs (Art. 28).¹³² The Data Security Law (2021) mandates cooperation when authorities lawfully seek data for national security or criminal investigation purposes.¹³³ In parallel, the revised Company Law of the PRC requires Communist Party organizations to be established in companies and obliges firms to provide necessary conditions for their activities (Art. 18 & 19).¹³⁴

This legal co-optation extends beyond mere data access to the active capture of software security research for state offensive capabilities. Under the Regulations on the Management of Network Product Security Vulnerabilities (RMSV), companies in China must report software vulnerabilities to the MIIT within 48 hours.¹³⁵ ¹³⁶ These rules prohibit public disclosure before a patch is issued and restrict sharing information with overseas

¹²⁹ SentinelOne, "[Top Tier Target: What It Takes to Defend a Cybersecurity Company from Today's Adversaries](#)" April 28, 2025.

¹³⁰ Google Threat Intelligence Group and Mandiant, "[Another BRICKSTORM: Stealthy Backdoor Enabling Espionage into Tech and Legal Sectors](#)", September 24, 2025.

¹³¹ China Law Translate, "[PRC National Intelligence Law \(as amended in 2018\)](#)", June 27, 2017.

¹³² China Law Translate, "[2016 Cybersecurity Law](#)", November 7, 2016.

¹³³ China Law Translate, "[Data Security Law of the PRC](#)," June 10, 2021.

¹³⁴ Lexis China, "[Company Law of the People's Republic of China \(Revised in 2023\)](#)", December 29, 2023.

¹³⁵ CAC, "[工业和信息化部 国家互联网信息办公室 公安部关于印发网络产品安全漏洞管理规定的通知](#)", July 13, 2021.

¹³⁶ The Record, "[Chinese government lays out new vulnerability disclosure rules](#)", July 14, 2021.



entities. The MIIT channels this data to the Ministry of Public Security (MPS) and the National Computer Network Emergency Response Technical Team (CNCERT/CC). Furthermore, the Ministry of State Security (MSS) operates China's national vulnerability database (CNNVD) through the Information Technology Security Evaluation Center (CNITSEC), also known as the MSS's 13th Bureau, requiring participating private-sector companies to provide annual quotas of critical vulnerabilities and, depending on their tier, detailed exploit code.¹³⁷

By centralizing vulnerability collection and barring participation in global hacking competitions,¹³⁸ the Party-state treats these discoveries as a "strategic resource," effectively forcing the private sector to stock a state-run arsenal of zero-day exploits. Public vulnerability databases may therefore be subject to delay or manipulation: for instance, reported industrial control system (ICS) vulnerabilities in China's voluntary database (CNVD) plummeted following the RMSV's implementation.¹³⁹ The MSS routinely delays high-threat listings, often backdating entries to conceal windows where state-sponsored hackers exploited flaws before patches were released. Thus, a relatively low volume of reported vulnerabilities in Chinese-origin hardware and software is not a reliable indicator of security, but rather a reflection of state hoarding of exploitable vulnerabilities.¹⁴⁰

These concerns are increasingly translating into procurement and risk-management measures abroad. Under the U.S. FY2026 NDAA, the Department of Defense will be prohibited from December 2026 from procuring covered AM equipment from companies based in, or subject to unmitigated control or influence from, China and several other covered countries.¹⁴¹ In the Czech Republic, NÚKIB warned in September 2025 that transferring system or user data to China, or allowing technical assets to be remotely administered from there, can constitute a cybersecurity threat.¹⁴² The Confederation of Industry subsequently applied this concern specifically to cloud-connected 3D printers, recommending scrutiny of printer origin and data flows, limits on unnecessary outbound data, and regular monitoring of network communications.¹⁴³

¹³⁷ Atlantic Council, "[Sleight of hand: How China weaponizes software vulnerabilities](#)", September 6, 2023.

¹³⁸ SCMP, "[China discourages its hackers from foreign competitions so they don't help others](#)", March 21, 2018.

¹³⁹ Intrinsec, "[China: Vulnerabilities as strategic resource](#)", p. 18. October 24, 2024.

¹⁴⁰ Bitsight, "[Red Vulns Rising: Examining Chinese National Vulnerability Databases](#)", February 18, 2026.

¹⁴¹ U.S. Congress, "[National Defense Authorization Act for Fiscal Year 2026](#)", Public Law 119-60, §849, December 18, 2025.

¹⁴² National Cyber and Information Security Agency (NÚKIB), "[NÚKIB Warns Against the Transfer of the Data to and Remote Administration from People's Republic of China](#)", September 3, 2025.

¹⁴³ Confederation of Industry of the Czech Republic, "[3D tisk pod dohledem: SP ČR a NÚKIB varují před únikem dat do Číny](#)", November 3, 2025.



7. Policy Recommendations

- **Classify additive manufacturing systems as sensitive technology:** Apply targeted export controls and procurement safeguards where systems rely on cloud connectivity, extensive sensor integration, remote administration, or vendor-controlled authorization mechanisms that can create operational and data-security risks in critical applications.
- **Raise awareness of technology-transfer risks and protect critical AM data and IP:** Treat design files, process parameters, materials recipes, machine telemetry, and production data as sensitive industrial assets, with stronger access controls, clear restrictions on vendor or third-party access, and targeted awareness for employees and partners.
- **Require secure operational protocols:** Mandate air-gapped or local-network-only deployments, disabled cloud functionality, controlled software updates, and strict firmware management for government, defense-related, research, and other high-sensitivity industrial environments to reduce outage, remote-access, and authorization vulnerabilities.
- **Promote diversification and independent audits:** Encourage organizations to avoid single-vendor dependence and conduct third-party cybersecurity, binary, licensing, and data-flow reviews of AM software, firmware, and connected hardware, while maintaining interoperable or open-source workflows where feasible to reduce security risks, IP exposure, and ecosystem lock-in.
- **Strengthen screening of investments and technology transfers:** Apply rigorous review to acquisitions, joint ventures, research partnerships, and supplier relationships involving firms closely connected to foreign industrial-policy programs, state-backed financing, or advanced-manufacturing clusters.
- **Coordinate technology-security measures with allies:** Share information on sensitive AM technologies, high-risk transactions, research links, and transfer intermediaries to reduce the risk that controls in one jurisdiction simply redirect acquisition activity to another.
- **Invest in competitive open innovation ecosystems:** Support domestic and allied R&D, technical education, and workforce expertise in industrial software, materials, secure digital workflows, and transparent hardware architectures to reduce strategic dependence and preserve critical AM know-how.