



# BIETA: A Technology Enablement Front for China's MSS

The Beijing Institute of Electronics Technology and Application (BIETA) is almost certainly affiliated with the Ministry of State Security (MSS), likely being a front for its First Research Institute.

This internationally active, Beijing-based institute and its subsidiary company are providing steganographic and counterintelligence capabilities for China's intelligence and security organizations.

BIETA's discovery offers new evidence for the MSS's very likely technology enablement role in supporting human intelligence and cyber operations conducted by provincial state security departments.

*Note: The author, Devin Thorne, thanks Alex Joske for his support in developing this research. More information about the author can be found at the end of this report.*

## Executive Summary

The Beijing Institute of Electronics Technology and Application (BIETA), a communications technology and information security research organization previously unexplored in public reporting, is almost certainly affiliated with China's principal civilian intelligence service, the Ministry of State Security (MSS). Based on publicly available sources, it is very likely led by MSS and likely a public front for the MSS First Research Institute. BIETA and its subsidiary, Beijing Sanxin Times Technology Co., Ltd. (CIII), research, develop, import, and sell technologies that almost certainly support intelligence, counterintelligence, military, and other missions relevant to China's national development and security. Their activities include researching methods of steganography that can likely support covert communications (COVCOM) and malware deployment; developing and selling forensic investigation and counterintelligence equipment; and acquiring foreign technologies for steganography, network penetration testing, and military communications and planning.

BIETA and CIII almost certainly form part of the very likely vast but underexplored (in public sources) network of front organizations contributing to the modernization of the MSS and wider Chinese state security apparatus, which challenges the interests of both foreign governments and private businesses. BIETA's almost certain MSS affiliation supports assessments of how the MSS very likely supports cyber-enabled intelligence operations by developing tools for use by intelligence officers and their proxies. Neither BIETA nor CIII are known to engage in illicit activity, but foreign export control authorities, academic institutions, and businesses should consider restricting transactions and other engagements with both BIETA and CIII. Engagement risks contributing to the capabilities of the MSS and People's Liberation Army (PLA), and could arise through joint research opportunities, overlap at international academic conferences, and product sales channels. Conducting due diligence investigations on any party interested in technologies discussed in this report is vital.

## Key Findings

- BIETA's almost certain ties to the MSS are inferable from the background of four BIETA personnel (three of which are almost certainly or very likely MSS personnel), its relationship with an MSS-run university (the University of International Relations in Beijing), and the scope of its research and other activities.
- BIETA's research almost certainly contributes to the MSS's steganographic capabilities that Chinese intelligence officers and contractors likely use to covertly communicate or deploy malware, while other products from BIETA and CIII almost certainly enable MSS and wider state and public security counterintelligence investigations.
- BIETA's almost certain MSS affiliation offers clarity into the very likely enablement role that the MSS plays with regard to Chinese cyber-espionage and cyber-enabled intelligence operations, wherein the MSS and subordinate state security departments develop and distribute technologies to operational actors.
- Discovery of BIETA also offers new insight into the MSS's organizational structure: BIETA was likely part of the MSS's former 13th Bureau, the remit of which was likely much broader than commonly recognized in connection to CNITSEC; it is also plausible that BIETA was part of the former 9th Bureau, which is now 14th Bureau.
- BIETA's research likely benefits from collaboration with international academics and exposure to international academic conferences, and very likely from foreign steganography technology acquired by CIII. CIII has attempted to support China's military modernization with foreign software for simulating and modeling communication networks and battlefield environments.

## Table of Contents

<b>Organizational Overview</b>	<b>4</b>
BIETA	4
Ties to the MSS	7
Personnel	7
Activities	12
CIII	12
Ties to the MSS	14
<b>Support to the MSS and Wider Security Apparatus</b>	<b>14</b>
Steganography	14
Steganography in Chinese Cyber Operations	17
Security Products	18
Technology Transfer	20
BIETA's Academic Activities	20
CIII's Imports	21
Steganography Software	21
Military Simulation and Modeling	21
Network Simulation and Penetration	22
Other Applications	23
<b>Implications for Understanding the MSS</b>	<b>24</b>
<b>Outlook</b>	<b>25</b>

## Organizational Overview

The Beijing Institute of Electronics Technology and Application (北京电子技术应用研究所) is a research organization primarily engaged in applied research of communication technology, multimedia information processing, and multimedia information security technology.<sup>1</sup> It has at least one wholly owned subsidiary: Beijing Sanxin Times Technology Co., Ltd. (CIII; 北京三信时代科技有限公司).<sup>2</sup> The activities of BIETA and CIII almost certainly contribute to the capabilities of the MSS and, likely, to those of China's wider security apparatus and military. The MSS (国家安全部) oversees a nationwide system of semi-autonomous units that constitute a domestic police force and China's primary civilian intelligence service responsible for human-source and cyber-enabled political and domestic security, counterintelligence and counterespionage, non-military foreign strategic intelligence, and foreign economic and technological intelligence.<sup>3 4 5</sup> BIETA and CIII are profiled below.

### BIETA

BIETA was established no later than 1990, almost certainly existing in some form as early as 1983 — the year the MSS was created.<sup>6 7 8 9</sup> It is located, per its website, at No. 15 Xinjian Gongmen Road, Haidian District, Beijing (北京市海淀区新建宫门路15号).<sup>10</sup> As shown in **Figure 1**, this address is adjacent to or within the MSS's almost certain headquarters compound at Xiyuan (West Garden).<sup>11</sup> BIETA is almost certainly state-owned, given that the website of BIETA's subsidiary, CIII, describes itself (CIII) as an "enterprise that is owned by the whole people" (全民所有制企业).<sup>12 13 14</sup> BIETA is almost certainly affiliated with the MSS, very likely led by the MSS, and likely a front for the MSS First Research Institute.

<sup>1</sup> 公司介绍 ["Company Introduction"], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20230605232400/http://www.bieta.cn/aboutus.htm>.

<sup>2</sup> Source held by Recorded Future.

<sup>3</sup> *Hearing before the U.S.-China Economic and Security Review Commission on China's Intelligence Services and Espionage Operations*, 114th Cong. (2016), pp. 6, 9–10 (opening statement and prepared statement of John Costello, Congressional Innovation Fellow, New America), <https://www.uscc.gov/sites/default/files/transcripts/June%2009,%202016%20Hearing%20Transcript.pdf>.

<sup>4</sup> Samantha Hoffman and Peter Mattis, "Managing the Power Within: China's State Security Commission," *War on the Rocks*, July 18, 2016, <https://warontherocks.com/2016/07/managing-the-power-within-chinas-state-security-commission/>.

<sup>5</sup> *United States of America v. Ding Xiaoyang et al.* (California: US District Court for the Southern District of California, March 28, 2021), p. 12, <https://www.justice.gov/opa/press-release/file/1412916/download>.

<sup>6</sup> Source held by Recorded Future.

<sup>7</sup> "Company Introduction," Beijing Institute of Electronics Technology and Application.

<sup>8</sup> 人才队伍 ["Talent Team"], 上海交通大学 [Shanghai Jiao Tong University], No Date, <https://web.archive.org/web/20221201213028/https://zias.sjtu.edu.cn/info/1267/1398.htm>.

<sup>9</sup> Peter Mattis and Matthew Brazil, *Chinese Communist Espionage: An Intelligence Primer* (Naval Institute Press, 2019), 53.

<sup>10</sup> 联系我们 ["Contact Us"], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20230605231433/http://www.bieta.cn/contact.htm>.

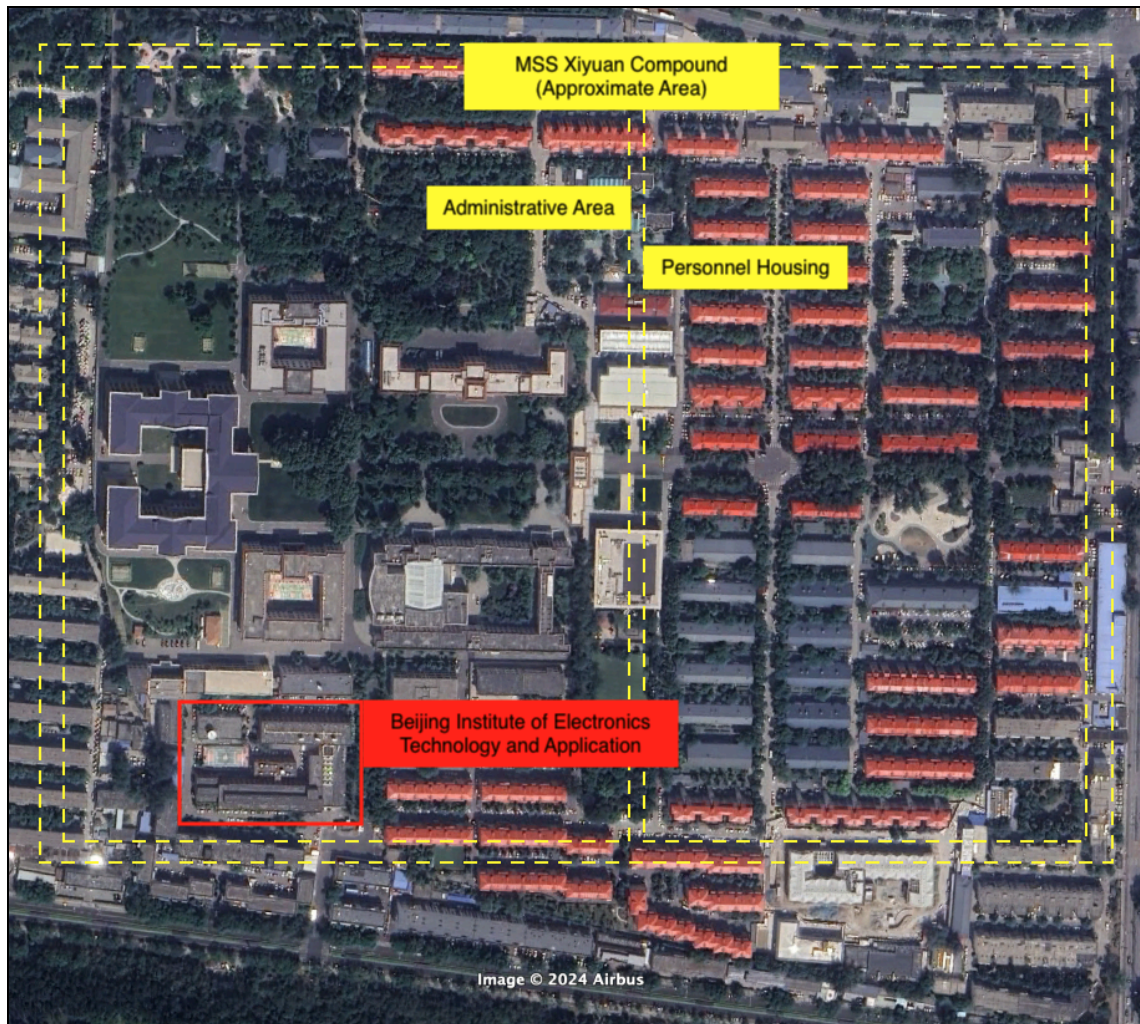
<sup>11</sup> "Ministry of State Security Headquarters Xiyuan [Western Garden]," Federation of American Scientists, November 26, 1997, <https://irp.fas.org/world/china/facilities/xiyuan.htm>.

<sup>12</sup> "Beijing Sanxin Times Information Co.," Network Security.

<sup>13</sup> 公司介绍 ["Company Introduction"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922113309/http://ciii.com.cn/1/>.

<sup>14</sup> 全民所有制企业改革 ["Reform of Enterprises Owned by the Whole People"], 中国关键词 [China Keywords], October 30, 2018, [https://web.archive.org/web/20231027203418/http://keywords.china.org.cn/2018-10/30/content\\_69094500.html](https://web.archive.org/web/20231027203418/http://keywords.china.org.cn/2018-10/30/content_69094500.html).





**Figure 1:** BIETA's location in relation to the approximate location of the MSS's Xiyuan headquarters compound  
(Source: Baidu Maps, Google Earth)

BIETA comprises at least four laboratories and one testing center. Its laboratories include the Communication Technology Research Lab, Multimedia Information Security Technology Research Lab, Electromagnetic Compatible Technology Research Lab, and the Hybrid Integrated Circuits Development Research Lab.<sup>15</sup> BIETA's Quality Testing Center (质量检测中心) is further composed of the Integrated Circuits Testing Experimental Lab, the Network Technology Testing Experimental Lab, the Multi-Media Technology Testing Experimental Lab, the Audio-Visual Subjective Evaluation Room, and the Product Integrated Testing Center Experimental Lab.<sup>16</sup>

BIETA asserts that its "primary research directions," among others, include:<sup>17</sup>

- Wireless, satellite, spread spectrum, and microwave communication technologies
- Information processing and multimedia information security technologies
- Computer vulnerability, information security, signal positioning, and signal jamming technologies

Steganography is another of BIETA's "primary research directions," and a major focus based on the organization's publicly visible academic activities. This line of research is discussed in the **Steganography** section. Other areas of research by BIETA and its researchers include forensics technology (including methods of identifying video files that have been tampered with, text forgeries, fabricated images, source cameras, and source printers), cryptography, networking, and technology miniaturization (of antennas, for example).<sup>18</sup> In 2016, for example, as China's counter-terrorism campaign in Xinjiang began escalating to include mass detentions of Uyghur and ethnic minorities, BIETA researchers co-authored an academic article on Uyghur text recognition.<sup>19 20</sup> These areas of research support the assessment that BIETA is almost certainly affiliated with the MSS.

Given BIETA's almost certain affiliation with the MSS, as well as the remit of the MSS and wider state security apparatus to investigate and mitigate domestic and foreign threats to the Chinese Communist Party (CCP) and China, it is almost certain that the organization's research directly or indirectly enables MSS operations across a range of activities. It is noteworthy in this context that BIETA contracted

<sup>15</sup> 首页 ["Main Page"], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20191025031531/http://www.bieta.cn/main.htm>.

<sup>16</sup> 质量检测中心 ["Quality Testing Center"], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20230606000823/http://www.bieta.cn/tixi.htm>.

<sup>17</sup> 研究机构 ["Research Institutions"], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20230606001559/http://www.bieta.cn/jigou.htm>.

<sup>18</sup> Sources held by Recorded Future.

<sup>19</sup> United Nations Office of the United Nations High Commissioner for Human Rights, *OHCHR Assessment of Human Rights Concerns in the Xinjiang Uyghur Autonomous Region, People's Republic of China* (Office of the United Nations High Commissioner for Human Rights, 2022), 17, <https://www.ohchr.org/sites/default/files/documents/countries/2022-08-31/22-08-31-final-assesment.pdf>.

<sup>20</sup> Li Pengchao et al., "RNN Based Uyghur Text Line Recognition and Its Training Strategy," IEEE Xplore, June 13, 2016, <https://ieeexplore.ieee.org/document/7490087>.



project(s) with NSFocus (北京神州绿盟信息安全科技股份有限公司) between 2013 and 2017.<sup>21 22 23 24</sup> The nature of the project or projects is unknown, but NSFocus is among China's leading cybersecurity companies and the first founded by early patriotic hackers (specifically those associated with the "Green Army").<sup>25</sup>

## ***Ties to the MSS***

The assessment that BIETA is almost certainly affiliated with the MSS, very likely led by the MSS, and likely a front for the MSS First Research Institute is primarily supported by evidence that several of BIETA's personnel (with varying degrees of certainty) are MSS officers, research staff, or otherwise affiliated with China's principal intelligence service. The assessment is also supported by BIETA's engagement with an MSS-subordinate university, the University of International Relations (UIR; 国际关系学院).<sup>26 27</sup>

## **Personnel**

Though the MSS is a highly secretive organization, at least four BIETA personnel have clear or potential links to the MSS, based on publicly available information. This supports the assessment that BIETA itself is almost certainly affiliated with China's principal civilian intelligence service. Of more than twenty individuals currently or formerly affiliated with BIETA, at least three individuals are almost certainly or very likely MSS personnel. There is evidence that points to one other BIETA employee having a possible MSS affiliation. The evidence linking these personnel to the MSS is surveyed below.

<sup>21</sup> 北京神州绿盟信息安全科技股份有限公司 2017 年半年度财务报告 ["Beijing Shenzhou Lvmeng Information Security Technology Co., Ltd. 2017 Semi-Annual Financial Report"], 巨潮资讯 [CN Info], August 26, 2017, <https://web.archive.org/web/20231027194645/http://static.cninfo.com.cn/finalpage/2017-08-26/1203873380.PDF>.

<sup>22</sup> 北京神州绿盟信息安全科技股份有限公司 2014 年半年度财务报告 ["Beijing Shenzhou Lvmeng Information Security Technology Co., Ltd. 2014 Semi-Annual Financial Report"], 巨潮资讯 [CN Info], April 25, 2015, [https://web.archive.org/web/20231030194642/http://file.finance.sina.com.cn/211.154.219.97:9494/MRGG/CNSESZ\\_STOCK/2015/2015-4/2015-04-25/1747706.PDF](https://web.archive.org/web/20231030194642/http://file.finance.sina.com.cn/211.154.219.97:9494/MRGG/CNSESZ_STOCK/2015/2015-4/2015-04-25/1747706.PDF).

<sup>23</sup> 自选股资讯 [Selected Stock Information], 绿盟科技: 2016 年年度报告 ["Lvmeng Technology: 2016 Annual Report"], 搜狐 [Sohu], April 21, 2017, [https://web.archive.org/web/20231030204429/https://www.sohu.com/a/135552306\\_545697](https://web.archive.org/web/20231030204429/https://www.sohu.com/a/135552306_545697).

<sup>24</sup> 北京神州绿盟信息安全科技股份有限公司 2015 年半年度财务报告 ["Beijing Shenzhou Lvmeng Information Security Technology Co., Ltd. 2015 Semi-Annual Financial Report"], 巨潮资讯 [CN Info], August 25, 2015, [https://web.archive.org/web/20231030204659/http://file.finance.sina.com.cn/211.154.219.97:9494/MRGG/CNSESZ\\_STOCK/2015/2015-8/2015-08-25/1942932.PDF](https://web.archive.org/web/20231030204659/http://file.finance.sina.com.cn/211.154.219.97:9494/MRGG/CNSESZ_STOCK/2015/2015-8/2015-08-25/1942932.PDF).

<sup>25</sup> Eugenio Benincasa, *Before Vegas: The "Red Hackers" Who Shaped China's Cyber Ecosystem* (ETH Zurich, July 18, 2025), 50, <https://css.ethz.ch/en/center/CSS-news/2025/07/before-vegas-the-red-hackers-who-shaped-chinas-cyber-ecosystem.html>.

<sup>26</sup> "University of International Relations," Australian Strategic Policy Institute, November 25, 2019, <https://unitracker.aspi.org.au/universities/university-of-international-relations/>.

<sup>27</sup> "浙江省人事厅、公安厅、国家安全厅关于从公安、安全系统院校应届毕业生中录用人民警察有关问题的通知" ["Notice from the Zhejiang Provincial Department of Personnel, the Public Security Department, and the State Security Department on Issues Related to the Recruitment of People's Police Officers from Fresh Graduates of Public Security and Security Colleges"], 宁波市人力资源和社会保障局 [Ningbo City Human Resources and Social Security Bureau], June 23, 1997, <https://archive.fo/3HRE4>.



**Wu Shizhong (吴世忠)**

**Figure 2:** Wu Shizhong (Source: Cyberspace Administration of China<sup>28</sup>)

Multiple public profiles identify Wu Shizhong as a BIETA researcher, one profile from as early as 2011.<sup>29</sup>

<sup>30</sup> In 2009, and likely as late as 2016, Wu Shizhong was the head of the "MSS Science and Technology Bureau" (国家安全部科技局).<sup>31 32</sup> Between 2005 and 2013, Wu was also the director of the China Information Technology Security Evaluation Center (CNITSEC; 中国信息安全测评中心).<sup>33 34</sup> Wu was further the secretary of CNITSEC's CCP committee between 2014 and 2018.<sup>35 36</sup> CNITSEC is almost certainly a public face of the MSS's former 13th Bureau that specialized (in part) in network security and exploitation.<sup>37 38 39</sup> According to one profile, Wu was employed at BIETA while also holding directorship of CNITSEC.<sup>40</sup> Wu's background supports the assessment that BIETA is almost certainly affiliated with the MSS.

<sup>28</sup> 谭树森 [Tan Shusen] et al, 中国信息安全测评中心书记 吴世忠 ["Secretary of China Information Security Evaluation Center Shizhong Wu"], 中央网络安全和信息化委员会办公室 [Office of the Central Cyberspace Affairs Commission], December 17, 2015, [https://web.archive.org/web/20220404020217/http://www.cac.gov.cn/2015-12/17/c\\_1117487279.htm](https://web.archive.org/web/20220404020217/http://www.cac.gov.cn/2015-12/17/c_1117487279.htm).

<sup>29</sup> 双周要闻荟萃 ["Bi-Weekly News Roundup"], 华文融媒云 [Nuawen Newspapers Cloud], April 15, 2011, [https://web.archive.org/web/20231025194742/http://wx.ihwrm.com/baokan/article/info.html?doc\\_id=563986](https://web.archive.org/web/20231025194742/http://wx.ihwrm.com/baokan/article/info.html?doc_id=563986).

<sup>30</sup> Source held by Recorded Future.

<sup>31</sup> 关于成立国家标准化体系建设工作机构的通知 (国标委综合[2009]42号) ["Notice on the Establishment of a National Standardization Systems Construction Work Organization Standardization Administration of China Comprehensive [2009] No. 42"], 民政科技与标准化信息平台 [Civil Affairs Technology and Standardization Information Platform], June 2, 2011, <https://web.archive.org/web/20190720013714/http://kjbz.mca.gov.cn/article/mzbzhzcwj/201106/20110600157934.shtml>.

<sup>32</sup> Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3," Recorded Future, May 17, 2017, <https://www.recordedfuture.com/chinese-mss-behind-apt3>.

<sup>33</sup> 中国信息安全产品测评认证中心深圳、西南、云南测评中心正式揭牌 ["China Information Security Product Evaluation and Certification Center Shenzhen, Xinan, and Yunnan Evaluation Centers are Officially Inaugurated"], 中国信息安全测评中心 [China Information Technology Security Evaluation Center], March 8, 2005, [https://web.archive.org/web/20221102002419/http://www.itsec.gov.cn/zxxw/200503/t20050308\\_15173.html](https://web.archive.org/web/20221102002419/http://www.itsec.gov.cn/zxxw/200503/t20050308_15173.html).

<sup>34</sup> "27号文"发布十年回顾暨2013《信息安全与通信保密》编委会在京成功举办 ["The Ten-Year Review of 'Document No. 27' and the 2013 'Information Security and Communication Secrecy' Editorial Committee was Successfully Held in Beijing"], 搜论 [Soolun], January 2014, <https://web.archive.org/web/20240112184719/https://www.syhms.com/periodical/ded636ef1ef9a57fc89f307b86b9b186.html>.

<sup>35</sup> 中国信息安全测评中心党委书记吴世忠: 在网络空间治理中落实依法治国精神 ["China Information Technology Security Evaluation Center Party Committee Secretary Wu Shizhong: Implement the Rule by Law Spirit in Cyberspace Governance"], 新华网 [Xinhuanet], November 5, 2014, [https://web.archive.org/web/20240112205813/http://www.xinhuanet.com/politics/2014-11/05/c\\_127182332.htm](https://web.archive.org/web/20240112205813/http://www.xinhuanet.com/politics/2014-11/05/c_127182332.htm).

<sup>36</sup> 李玲 [Li Ling] and 裘萍 [Qiu Ping], 政协委员吴世忠: 企业获取数据的便捷性与能力 已超过政府部门 ["CPPCC member Wu Shizhong: The convenience and ability of enterprises in obtaining data has surpassed that of government departments"], 安全内参 [Security Internal Reference], March 21, 2018, <https://web.archive.org/web/20240105204145/https://www.secrss.com/articles/1551>.

<sup>37</sup> Mattis and Brazil, *Chinese Communist Espionage*, p. 56.

<sup>38</sup> Jon R. Lindsay, "Introduction: China and Cybersecurity: Controversy and Context," *China and Cybersecurity: Espionage, Strategy, and Politics in the Digital Domain*, ed. Jon R. Lindsay, Tai Ming Cheung, and Derek S. Reveron (Oxford University Press, 2015), 9.

<sup>39</sup> Alex Joske and YunGeun Jeon, "Redesigning State Security: The 2018 Reorganisation of the Ministry of State Security," *Deserepi* no. 1 (2025), 4-6, [https://deserepi.org/1/joske-jeon\\_mss.pdf](https://deserepi.org/1/joske-jeon_mss.pdf).

<sup>40</sup> Source held by Recorded Future.

**He Dequan (何德全)****Figure 3:** He Dequan (Source: Shanghai Jiao Tong University<sup>41</sup>)

Beginning in 1983 — the year the MSS was created<sup>42</sup> — He Dequan was almost certainly employed as a senior engineer at BIETA.<sup>43 44</sup> Academic publications indicate that, as late as 2009, He still used a BIETA affiliation.<sup>45</sup> He was almost certainly a career intelligence officer in China, prior to and after the MSS's establishment. In 1983, He was also deputy bureau chief (副局长) for "some security department" (某安全部) and a researcher with and director of the Beijing Information Technology Research Institute (BITRI; 北京信息技术应用研究所).<sup>46 47 48</sup> Although public profiles do not explicitly say that from 1983 to 2000, He was employed with the MSS, he won a "Ministry of State Security Science and Technology Advancement Award" (国家安全部科技进步奖) in 1989, supporting this conclusion.<sup>49</sup> He's links to the MSS are also seen in his consulting position with CNITSEC.<sup>50 51 52</sup> Further, he has had an advisory role with the China International Public Relations Association (中国国际公共关系协会), an outwardly Ministry of Foreign Affairs-affiliated organization that is reportedly run by the MSS and used by MSS officers to interact with multinational corporations.<sup>53</sup> Moreover, He's BITRI affiliation is notable because this research organization has had other employees associated with the MSS. Specifically, BITRI appears in the work history of former Huawei executive Sun Yafang (孙亚芳), who worked for the MSS in a role related to communications after college.<sup>54 55</sup> He's background supports the assessment that BIETA is almost certainly affiliated with the MSS and that BIETA is very likely led by the MSS.

<sup>41</sup> "Talent Team," Shanghai Jiao Tong University.

<sup>42</sup> Mattis and Brazil, *Chinese Communist Espionage*, 53.

<sup>43</sup> 何德全 [He Dequan], 清华大学档案信息网 [Archives of Tsinghua University], May 21, 2009, [https://web.archive.org/web/20230215074738/http://thdag.cic.tsinghua.edu.cn/docinfo\\_out/board/boarddetail.jsp?columnId=001060104&parentColumnId=0010601&itemSeq=4852](https://web.archive.org/web/20230215074738/http://thdag.cic.tsinghua.edu.cn/docinfo_out/board/boarddetail.jsp?columnId=001060104&parentColumnId=0010601&itemSeq=4852).

<sup>44</sup> "Talent Team," Shanghai Jiao Tong University.

<sup>45</sup> Source held by Recorded Future.

<sup>46</sup> He Dequan, Archives of Tsinghua University.

<sup>47</sup> "Talent Team," Shanghai Jiao Tong University.

<sup>48</sup> Source held by Recorded Future.

<sup>49</sup> Source held by Recorded Future.

<sup>50</sup> Source held by Recorded Future.

<sup>51</sup> Mattis and Brazil, *Chinese Communist Espionage*, 56.

<sup>52</sup> 中国防伪行业协会质量追溯研究中心建设方案 ["China Trade Association for Anti-counterfeiting Quality Tracing Research Center Construction Plan"], 中国防伪行业协会 [China Trade Association for Anti-counterfeiting], No Date, <https://web.archive.org/web/20231025163907/http://www.ctaac.org.cn/class/view?id=128>.

<sup>53</sup> Alex Joske, *Spies and Lies: How China's Greatest Covert Operations Fooled the World* (Hardie Grant Books, 2022), 123-124.

<sup>54</sup> 华为巾帼孙亚芳 ["Huawei Heroine Sun Yafang"], 电子科技大学校友会总会 [University of Electronic Science and Technology of China Alumni Association], April 3, 2006, <http://web.archive.org/web/20070607165123/http://www.alumni.uestc.edu.cn/ListNews.aspx?ID=484>.

<sup>55</sup> 2015年年度报告 ["2015 Annual Report"], 华为投资控股有限公司 [Huawei Investment & Holding Co., Ltd.], March 22, 2016, 85, [https://web.archive.org/web/20240115150359/https://www.huawei.com/-/media/CORPORATE/PDF/annual-report/AnnualReport2015\\_cn.pdf?la=z](https://web.archive.org/web/20240115150359/https://www.huawei.com/-/media/CORPORATE/PDF/annual-report/AnnualReport2015_cn.pdf?la=z)h.

## You Xingang (尤新刚)

You Xingang has published academic research using a BIETA affiliation since at least 2001.<sup>56</sup> You was the head of BIETA between 2008 and 2023.<sup>57 58 59 60 61 62</sup> You is very likely an MSS officer. In 2012, You was described as a CNITSEC deputy director.<sup>63</sup> References from 2018 and 2019 continue to affiliate You with CNITSEC in an unspecified capacity.<sup>64 65</sup> Furthermore, in 2003, an individual named You Xingang was awarded a China Youth Science and Technology Innovation Award (中国青年科技创新奖) and identified as a researcher with the MSS First Research Institute (国家安全部第一研究所).<sup>66</sup> This You is likely BIETA's You Xingang. Having reportedly graduated from university in 1984, BIETA's You would likely have been around the age of 39 at the time of the award and therefore eligible for it.<sup>67 68</sup> Evidence supporting the assessment that BIETA is likely a front for MSS First Research Institute are indications that the MSS First Research Institute's activities overlap with those of BIETA. A patent filed in 2007 references the MSS First Research Institute as having tested an "MT-type nickel-based conductive coating ... used for electromagnetic wave shielding."<sup>69</sup> Correspondingly, BIETA has an Electromagnetic

<sup>56</sup> Source held by Recorded Future.

<sup>57</sup> 李新玲 [Li Xinling], 从官员学者的退养之地到最有活力的学术团体 一个学会的民主改革之路 ["From a Retreat for Officials and Scholars to the Most Dynamic Academic Group A society's path to democratic reform"], 中国青年报 [China Youth Online], December 27, 2008, [https://web.archive.org/web/20231025193618/https://zqb.cyol.com/content/2008-12/27/content\\_2487886.htm](https://web.archive.org/web/20231025193618/https://zqb.cyol.com/content/2008-12/27/content_2487886.htm).

<sup>58</sup> 我校联合承办“2017年全国通信理论与技术学术会议暨通信产业创新发展论坛” ["Our School Jointly Hosted the '2017 National Academic Conference on Communication Theory and Technology and Communication Industry Innovation and Development Forum'"], 南京邮电大学 [Nanjing University of Posts and Telecommunications], August 27, 2017, <https://web.archive.org/web/20231025191815/http://www.njupt.edu.cn/2017/0827/c53a111619/pagem.htm>.

<sup>59</sup> 中国电子学会2018年全国通信理论与技术学术会议暨通信领域创新发展论坛 ["China Electronics Society 2018 National Academic Conference on Communication Theory and Technology and Communication Field Innovation and Development Forum"], 南京邮电大学 [Nanjing University of Posts and Telecommunications], July 27, 2018, <https://web.archive.org/web/20231025192016/https://webcache.googleusercontent.com/search?q=cache:o7tcsmn004YJ:https://www.scopesea.com/KBYgmIDdHm/2018/0727/c75a131580/page.htm&hl=en&gl=us>.

<sup>60</sup> 2019年全国通信理论与技术学术会议暨通信领域创新发展论坛 ["China Electronics Society 2019 National Academic Conference on Communication Theory and Technology and Communication Field Innovation and Development Forum"], 南京邮电大学 [Nanjing University of Posts and Telecommunications], September 9, 2019, <https://web.archive.org/web/20231025192428/http://www.wxchengbaijia.com/2019/0909/c75a154155/page.htm>.

<sup>61</sup> 硕果满枝！政产学研多方协同共筑集群创新高地 ["Fruitful achievements! Government, Industry, Academia, and Research Collaborate to Build a Cluster of Innovation Hubs"], 无锡物联网创新促进中心 [Wuxi IoT Innovation Promotion Center], August 8, 2023, <https://www.wiotipc.org.cn/nd/jsp?id=198> (<https://archive.ph/o9Y05>).

<sup>62</sup> There is some uncertainty about You's directorship as other sources published during this period sometimes name another person as BIETA's director.

<sup>63</sup> 周舒 [Zhou Shu], 江苏省网络监控工程中心2012年度学术委员会会议在南京召开 ["The 2012 Academic Committee Meeting of the Jiangsu Provincial Network Monitoring Engineering Center was Held in Nanjing"], 天际新闻网 [The Skyline], November 20, 2012, <https://web.archive.org/web/20231025172316/https://news.nuist.edu.cn/2012/1120/c1147a73507/page.htm>.

<sup>64</sup> 南京信息工程大学团委 [Nanjing University of Information Science and Technology Youth League Committee], 第四届云计算与安全国际会议 (ICCCS2018) ["Fourth International Conference on Cloud Computing and Security (ICCCS2018)"], 搜狐 [Sohu], January 5, 2018, [https://web.archive.org/web/20231025203842/https://www.sohu.com/a/214889517\\_702989](https://web.archive.org/web/20231025203842/https://www.sohu.com/a/214889517_702989).

<sup>65</sup> 征文通知 ["Call for Papers"], ACM 中国图灵大会 2019 [ACM TURC 2019], No Date, <https://web.archive.org/web/20231025204724/https://www.acmturc.com/2019/cn/cfp.html>.

<sup>66</sup> 共青团中央 [Chinese Communist Youth League Central Committee] and 全国青联 [All-China Youth Federation], 中青联发[2003]49号 关于表彰第六届“中国青年科技创新奖”获得者的决定 ["Zhongqing Lianfa [2003] No. 49 Decision on Commending the Winners of the 6th "China Youth Science and Technology Innovation Award"], 中国共青团 [Chinese Communist Youth League], November 5, 2003, [https://web.archive.org/web/20231025205100/https://www.gqt.org.cn/documents/zqlf/200705/t20070521\\_27792.htm](https://web.archive.org/web/20231025205100/https://www.gqt.org.cn/documents/zqlf/200705/t20070521_27792.htm).

<sup>67</sup> 尤新刚 ["You Xingang"], 百度百科 [Baidu Baike], No Date, <https://web.archive.org/web/20240111143646/https://baike.baidu.com/item/%E5%B0%A4%E6%96%B0%E5%88%9A/9987984?fromModule=disambiguation>.

<sup>68</sup> China Youth Science and Technology Innovation Awards are awarded to people under the age of 40, or up to the age of 45 in the case of outstanding talents. See 关于开展第四届“中国青年科技创新奖”评选活动的通知 ["Zhongqing Lianfa [1999] No. 64 Notice on the Launch of the 4th "China Youth Science and Technology Innovation Award" Selection Activity"], 中国共青团 [Chinese Communist Youth League], No Date, <https://www.gqt.org.cn/search/zuzhi/documents/1999/zqlf/tlf64.htm> (<https://archive.ph/UHD8W>).

<sup>69</sup> 曹宏 [Cao Hong], 一种无机非金属磁性导电涂料及其制备方法 ["An Inorganic Non-Metallic Magnetic Conductive Coating and Its Preparation Method"], China Patent CN101037555A, filed on March 29, 2007, granted on May 19, 2010, <https://patents.google.com/patent/CN101037555A>.

Compatible Technology Research Lab (电磁兼容技术研究室) and conducts research into electromagnetic signal security protection technology.<sup>70 71</sup> You's background supports the assessment that BIETA is almost certainly affiliated with the MSS, very likely led by the MSS, and likely a public front for the MSS First Research Institute.

#### Zhou Linna (周琳娜)



**Figure 4.** Zhou Linna (Source: UIR School of Cyber Science and Engineering<sup>72</sup>)

Zhou Linna reportedly worked at BIETA between 1999 and approximately 2017, publishing academic research under this affiliation at least as late as 2011.<sup>73 74 75</sup> Evidence supports an assessment that Zhou may also be an MSS officer or otherwise affiliated with the intelligence service. First, Zhou is a professor with the MSS-subordinate UIR.<sup>76 77 78 79 80</sup> As early as 2017, she was, more specifically, identified as the dean of UIR's School of Information Science and Technology (信息科技学院; now the School of Cyber Science and Engineering [网络空间安全学院]).<sup>81 82</sup> An individual named Zhou Linna was also recognized in 2017 among the recipients of the Central State Institutions Ninth National Five Good Civilized Household Award (中央国家机关第九届全国五好文明家庭获奖) and identified as a member of

<sup>70</sup> "Quality Testing Center," Beijing Institute of Electronics Technology and Application.

<sup>71</sup> "Company Introduction," Beijing Institute of Electronics Technology and Application.

<sup>72</sup> 信息科技学院教师介绍 ["School of Cyber Science and Engineering Teacher Introductions"], 国际关系学院信息科技学院 [University of International Relations School of Cyber Science and Engineering], No Date, [https://web.archive.org/web/20231222024335/https://xinke.uir.cn/xwdt\\_jsjs/541594.shtml](https://web.archive.org/web/20231222024335/https://xinke.uir.cn/xwdt_jsjs/541594.shtml).

<sup>73</sup> Source Held by Recorded Future.

<sup>74</sup> 中国开发者网络 [Chinese Software Developer Network], AI 女神是如何炼成的? ["How is the AI goddess made?"], 腾讯网 [Tencent Net], March 7, 2022, <https://web.archive.org/web/20231026145850/https://new.qq.com/rain/a/20220307A0AAZD00>.

<sup>75</sup> Source Held by Recorded Future.

<sup>76</sup> 周文柏 [Zhou Wenbai], 2019年网络空间媒体安全与取证技术研讨会顺利召开 ["The 2019 Cyberspace Media Security and Forensics Technology Seminar Successfully Held"], 中国科学技术大学网络空间安全学院 [University of Science and Technology of China School of Cyber Science and Technology], May 20, 2019, <https://web.archive.org/web/20231026151234/https://cybersec.ustc.edu.cn/2019/0520/c15751a381075/page.htm>.

<sup>77</sup> 国家重点研发计划第四课题 年度研讨会顺利召开 ["National Key R&D Program Fourth Subject Annual Seminar Successfully Held"], 北京交通大学数字媒体信息处理研究中心 [Beijing Jiaotong University Center of Digital Media Information Processing], No Date, <https://web.archive.org/web/20231026145910/http://mepro.bjtu.edu.cn/newsdetail.html?id=125>.

<sup>78</sup> "China Trade Association for Anti-counterfeiting Quality Tracing Research Center Construction Plan," China Trade Association for Anti-counterfeiting.

<sup>79</sup> "University of International Relations," Australian Strategic Policy Institute.

<sup>80</sup> "Teacher Introductions," University of International Relations School of Cyber Science and Engineering.

<sup>81</sup> 全国“信息隐藏未来发展”专题研讨会召开 ["National seminar on 'Future Development of Information Hiding' was Held"], 景德镇陶瓷大学机械电子工程学院 [Jingdezhen Ceramic University School of Mechanical and Electronic Engineering], April 10, 2017, <http://jdxu.jcu.edu.cn/info/1042/1186.htm>.

<sup>82</sup> 国际关系学院网络空间安全学院简介 ["University of International Relations School of Cyber Science and Engineering Introduction"], 圣才考研网 [Kaoyan.100xuexi], February 4, 2023, <https://web.archive.org/web/20240115171015/https://kaoyan.100xuexi.com/WebSpecF/EnrolDetail.aspx?id=220455>.



the MSS (国家安全部干部).<sup>83</sup> As of writing, however, this potential direct reference to BIETA's Zhou as an MSS member cannot be corroborated through other publicly available information. Zhou's background supports the assessment that BIETA is almost certainly affiliated with the MSS.

## Activities

BIETA's organizational links and activities in relation to the MSS-subordinate UIR also support the assessment that BIETA is almost certainly affiliated with the MSS.<sup>84</sup> UIR promotional materials for prospective graduate students assert "year-round" and "very close cooperation" between the university and BIETA.<sup>85</sup> Between at least 2011 and 2018, BIETA was a "joint training" partner for the university's Communications and Information Systems (通信与信息系统) discipline. Specifically, BIETA supported modern communications technology and information security as areas of study.<sup>87</sup> UIR's School of Cyber Science and Engineering further asserts that it has an "intern base" at BIETA where graduates can attain practical industry experience.<sup>90</sup> UIR's School of Cyber Science and Engineering only publicly names intern bases at two other organizations, one of which is CNITSEC.<sup>91</sup>

## CIII

CIII, also known as Beijing Sanxin Times Technology Co., Ltd., and formerly known as Beijing Sanxin Times Information Company (北京三信时代信息公司), is a technology company established in 1994.<sup>92</sup> CIII is a state-owned enterprise and a subsidiary of BIETA.<sup>94</sup> It is located in Beijing and has offices in Shanghai and Hangzhou (incorporated in October 2023), a likely office in Hong Kong, and former offices (now closed) in Xinjiang.<sup>96</sup> CIII claims its clients include party-state government and military

<sup>83</sup> 全国五好文明家庭(标兵)获奖名单 ["List of Winners of National Five Good Civilized Families (Modern Model)"], comment on 中央国家机关推荐妇女十一大代表和全国妇联十一届执委候选人 ["Central State Agencies Recommend Candidates for the 11th Women's Congress and the 11th Executive Committee of the All-China Women's Federation"], 氧分子网 [YangFenZi], September 14, 2013, <https://web.archive.org/web/20170708043801/http://www.yangfenzi.com/zimeiti/3907.html>.

<sup>84</sup> "University of International Relations," Australian Strategic Policy Institute.

<sup>85</sup> 研究生 ["Graduate Students"], 国际关系学院 [University of International Relations], No Date, <https://web.archive.org/web/20230326080514/https://www.uir.edu.cn/c/2015-12-01/522490.shtml>.

<sup>86</sup> 新增政治学理论、国家安全学两个专业——访国际关系学院研究生部主任李文良 ["Two New Majors: Political Science Theory and National Security Studies—Interview with Li Wenliang, Director of the Graduate Department of the University of International Relations"], 国际关系学院 [University of International Relations], No Date, <https://web.archive.org/web/20180207192824/https://yz.chsi.com.cn/kyzx/kyft/201709/20170922/1630312182.html>.

<sup>87</sup> 国际关系学院通信与信息系统2011年考研大纲 ["University of International Relations Communication and Information Systems 2011 Postgraduate Entrance Examination Syllabus"], 考研帮 [Kaoyanbang], May 10, 2014, <https://web.archive.org/web/20171231003932/https://yz.kaoyan.com/uir/dagang/536dbd3a76c21.html>.

<sup>88</sup> 国际关系学院2017年硕士研究生招生专业目录 ["University of International Relations 2017 Master's Degree Admissions Major Catalog"], 国际关系学院研究生招生信息网 [University of International Relations Graduate Student Admissions Information Net], No Date, <https://web.archive.org/web/20231027183125/https://webcache.googleusercontent.com/search?q=cache:4W5iOfH2n6gJ:https://yjszs.uir.cn/maganager/contentcore/resource/download%3FID%3D127036&hl=en&gl=us>.

<sup>89</sup> 2018国际关系学院硕士研究生招生专业目录 ["2018 University of International Relations Master's Degree Admissions Major Catalog"], 考研帮 [Kaoyanbang], September 10, 2017, <https://web.archive.org/web/20231027183113/https://m.kaoyan.com/yanzhao/uir/zhuanye/59b4fca96cfcc.html>.

<sup>90</sup> 招生就业 ["Enrollment and Employment"], 国际关系学院信息科技学院 [University of International Relations School of Cyber Science and Engineering], No Date, <https://web.archive.org/web/20230805153057/https://xinke.uir.cn/c/2016-02-26/541674.shtml>.

<sup>91</sup> "Enrollment and Employment," University of International Relations School of Cyber Science and Engineering.

<sup>92</sup> 北京市2022年度第一批拟更名高新技术企业名单 ["Beijing's First Batch of High-Tech Enterprises Renamed in 2022"], 北京市科学技术委员会 [Beijing Municipal Science and Technology Committee], No Date, [hxxps://kw\[.\]beijing\[.\]gov\[.\]cn/attach/0/附件:北京市2022年度第一批拟更名高新技术企业名单\[.docx\]](https://archive.ph/ogCzN) (<https://archive.ph/ogCzN>).

<sup>93</sup> Source held by Recorded Future.

<sup>94</sup> "Company Introduction," Beijing Sanxin Times Information Co.

<sup>95</sup> "Beijing Sanxin Times Information Co.," Network Security.

<sup>96</sup> Source Held by Recorded Future.

organizations as well as organizations in the broadcasting, finance, environment, insurance, electricity, transport, and oil industries.<sup>97</sup> While CIII has shared several employees with BIETA, publicly available information does not identify links between CIII employees and the MSS.<sup>98</sup> Nevertheless, CIII is also almost certainly affiliated with the MSS through its relationship to BIETA.

On its website, the company claims to be engaged in several disparate activities that include operating an internet data center (IDC) in Beijing; maintaining Beidou Satellite Navigation-enabled platforms for police and campus security organizations; developing enterprise and social applications for Windows, Android, and iOS — including those for uploading files to Baidu Cloud and OneDrive and for genealogy, photography, voice recording, and locating and communicating with friends<sup>99 100 101 102</sup> — and conducting network simulations and penetration testing against websites, mobile applications, enterprise systems, servers, databases, cloud platforms, and internet-of-things equipment.<sup>103 104 105 106 107</sup> How recently CIII's website has been updated is unknown, but software copyright registrations indicate activities since 2020 (see **Table 1**). CIII also registered a copyright for a “mesh detection system” (网眼检测系统) in 2017 and a “penetration testing analysis system” (渗透测试分析系统) in 2013.<sup>108</sup>

Software Copyright Name	Latest Registration Date
Intelligent Discussion Android App (慧议通安卓版应用软件)	November 29, 2021
Secure Instant Communication Software (安全即时通讯软件)	June 15, 2020
Beidou Satellite Communication Software (BD卫星通信软件)	June 14, 2020

**Table 1:** Select software developed by CIII since 2020 (Source: Insikt Group)

Limited information is publicly available on most of these activities and whether or how they may support the MSS. Most are likely aimed at generating income for BIETA, commercializing state-funded research, and supporting state-led technology initiatives. For example, CIII likely contributed to the development of “Time Capsule” (时间舱), a mobile application that claims to be China’s “first smart information rights protection certificate ledger” (智慧信息权益保全存证) platform.<sup>109</sup> “Time Capsule” was

<sup>97</sup> “Company Introduction,” Beijing Sanxin Times Information Co.

<sup>98</sup> Source Held by Recorded Future.

<sup>99</sup> Datacrypt蜂鸟网盘上传 [“Datacrypt Hummingbird Network Disk Uploader”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102170348/http://www.ciii.com.cn/49/13.html>.

<sup>100</sup> 家谱 [“Family”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102151252/http://www.ciii.com.cn/48/11.html>.

<sup>101</sup> 有声相机 [“Camera with Sound”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102151250/http://www.ciii.com.cn/48/10.html>.

<sup>102</sup> 即时通信软件 [“Where”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102151255/http://www.ciii.com.cn/48/9.html>.

<sup>103</sup> “IDC/ISP,” 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922113319/http://ciii.com.cn/5/>.

<sup>104</sup> “Company Introduction,” CIII.

<sup>105</sup> 南宮警务平台系统 [“Nangong Police Platform System”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922113339/http://www.ciii.com.cn/26/>.

<sup>106</sup> 北斗校园安全平台 [“Beidou Campus Security Platform”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922113426/http://www.ciii.com.cn/27/>.

<sup>107</sup> 产品中心 [“Product Center”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922113217/http://ciii.com.cn/11/>.

<sup>108</sup> Source held by Recorded Future.

<sup>109</sup> 北京领锋九霄科技有限公司 [“Beijing Lingfeng Jiuxiao Technology Co., Ltd.”], 时间舱 [“Time Capsule”], Apple App Store, No Date, <https://web.archive.org/web/20240208161055/https://apps.apple.com/my/app/%E6%97%B6%E9%97%B4%E8%88%B1/id1620815717>.

developed by a joint laboratory established by CIII, other companies, and various government agencies and research institutes. CIII's ownership of an IDC and publication of user applications as recently as 2021 suggests the MSS may have, or once have had, easy access to user data via CIII. The extent to which the public adopted CIII's applications is unknown.

CIII also sells a wide range of security products, services, and solutions that are relevant to the facility and operational security needs of the MSS and other Chinese military and security services. These are further discussed in the **Security Products** section. CIII further claims to be an "agent [or representative; 代理] for network testing, network monitoring, cybersecurity, network communications simulation, and other software and hardware products developed by the United States [US], Europe, and other countries."<sup>110</sup> CIII's acquisition of foreign technologies (whether as an agent or through other means) almost certainly enables the company's activities related to network simulation, penetration testing, and various Chinese military needs. The **Technology Transfer** section discusses this aspect of CIII's business in more detail.

### *Ties to the MSS*

Publicly available information does not reveal direct links between CIII and the MSS. In describing its work related to Beidou navigation, CIII refers to CNITSEC as a "related unit" (关系单位) that provides information security services for CII's Beidou platform and terminals. Whether this language has any additional meaning or significance with regard to institutional ties between CIII and the MSS is unclear.<sup>111</sup> Since at least 2017, CIII has been a CNITSEC-recognized "unit [that has] passed the national information security evaluation/information security service qualification (security engineering level 1) evaluation" (通过国家信息安全测评/信息安全服务资质(安全工程类一级)测评的单位). The potential significance of this qualification in relation to CIII's potential ties to the MSS is also unclear.<sup>112</sup>

## Support to the MSS and Wider Security Apparatus

In addition to other support, BIETA and its subsidiary, CIII, almost certainly facilitate the MSS's and state security system's missions by developing steganographic capabilities and selling security equipment. CIII claims to further support the PLA (人民解放军) with its products and services. It is likely that technologies developed or sold by BIETA and CIII also support public security operations. Notably, both BIETA and CIII almost certainly constitute a vector for technology transfer from the US and Europe that directly or indirectly benefits the MSS and PLA.

### Steganography

Publicly available information demonstrates that steganography (信息隐藏; 数据隐藏; 隐写术) is a major focal point of BIETA's research efforts. Steganography is the practice of hiding information within

<sup>110</sup> "Product Center," CIII.

<sup>111</sup> 北斗导航 ["Beidou Navigation"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922113446/http://www.ciii.com.cn/6/>.

<sup>112</sup> 测评公告(2018年第1号) ["Evaluation Announcement (2018 No. 1)"], 中国信息安全测评中心 [China Information Technology Security Evaluation Center], February 1, 2018, [https://web.archive.org/web/20231114213105/http://www.itsec.gov.cn/fwzz/fcpagg/201802/t20180201\\_23618.html](https://web.archive.org/web/20231114213105/http://www.itsec.gov.cn/fwzz/fcpagg/201802/t20180201_23618.html).

otherwise ordinary data, such as secret messages embedded in text, photo, audio, or video files. Of 87 academic publications with at least one BIETA-affiliated author between 1991 and 2023, at least 40 (46%) are related to steganography, based on keyword searches of their titles and abstracts.<sup>113</sup> Various government funding programs, including the National Natural Sciences Fund (国家自然科学基金), 973 Program (973计划), and 863 Program (863计划), have supported BIETA's steganography research as recently as 2019.<sup>114</sup> UIR interns have also worked on steganography issues.<sup>115</sup> In addition to academic publishing, BIETA has also sponsored or participated in related conferences, such as a national conference on "the future development of information hiding" in 2017 and the "18th national information hiding and multimedia information security" conference in October 2024.<sup>116</sup> <sup>117</sup> Based on BIETA's almost certain affiliation with the MSS and evidence that Chinese state security intelligence officers have "received malware from the MSS to be used against foreign victims" in known cyber espionage cases,<sup>118</sup> BIETA's research almost certainly contributes to the MSS's technical capabilities for detecting hidden information and communicating covertly that are likely to be shared with other actors in the state security system.

CIII has also received copyrights for software related to steganography. Examples include an "audio-visual-to-voice conversion secrets deep analysis system" (音图转换语音隐密深度分析系统) and a "JPEG image forensics differentiation method based on characteristics optimization" (基于特征优化选择的JPEG图像取证鉴别方法软件), both registered in 2017.<sup>119</sup>

BIETA and CIII's steganography work almost certainly has the potential to support defensive and offensive MSS operational activities. Defensively, access to effective steganalysis methods across mediums and file types could aid the state security system in detecting hidden information that threatens CCP political power and national security, such as among would-be dissidents and foreign intelligence services. Offensively, the MSS, state security departments and bureaus, and their contractors or proxies could use steganography to covertly transmit information of value in support of their operations. Chinese advanced persistent threats (APTs) have been observed doing so and have also used steganography to deploy malware (see **Steganography in Chinese Cyber Operations** below). Officers from the Shanghai State Security Bureau (SSSB) also provided former US intelligence officer Kevin Mallory a mobile phone with COVCOM capabilities and trained him how to embed documents within images as part of a scheme in which Mallory sold the SSSB classified information.<sup>120</sup> <sup>121</sup>

BIETA's steganography research covers a range of topics across different media: text, image (such as JPEG), audio (such as MP3), and video (HEVC). Public BIETA-affiliated academic articles almost

<sup>113</sup> Source Held by Recorded Future.

<sup>114</sup> Source Held by Recorded Future.

<sup>115</sup> Source Held by Recorded Future.

<sup>116</sup> "National Seminar on 'Future Development of Information Hiding'," Jingdezhen Ceramic University School of Mechanical and Electronic Engineering.

<sup>117</sup> 第十八届全国信息隐藏暨多媒体信息安全学术大会在京成功举办 ["The 18th National Information Hiding and Multimedia Information Security Academic Conference was successfully held in Beijing"], 国际战略与安全研究中心 [Center for International Strategy and Security Studies], October 22, 2024, [hxxps\[://\]ciss\[.\]cn/info/1071/6811\[.\]htm](https://www.ciss[.]cn/info/1071/6811[.]htm) (<https://archive.ph/2gCaa>).

<sup>118</sup> United States of America v. Ding Xiaoyang et al., 12.

<sup>119</sup> Source held by Recorded Future.

<sup>120</sup> Mattis and Brazil, Chinese Communist Espionage, 239.

<sup>121</sup> United States of America v. Kevin Patrick Mallory (Virginia: US District Court for the Eastern District of Virginia June 21, 2017), 9-11, <https://www.justice.gov/opa/press-release/file/975671/download>.



certainly cover topics that are relevant to both defensive and offensive applications, such as the detection of messages within MP3 files and preventing the detection of information hidden in images.<sup>122</sup> BIETA's research also includes developing methods of covertly transmitting information. **Figure 5** provides examples of methods explored by BIETA researchers for coding messages into seemingly ordinary digital online communications. During a 2019 conference panel on steganography and artificial intelligence (AI), an associate researcher with BIETA introduced Generative Adversarial Networks (GAN), suggesting this is another area of research for the organization.<sup>123</sup>



**Figure 5:** Steganographic methods researched by BIETA personnel; left: mis-ordered letters in an ostensible internet chat message communicate a message disguised as a typo (2009); right: iconographic library used to communicate secret messages (2019) (Source: Insikt Group)

<sup>122</sup> Sources Held by Recorded Future.

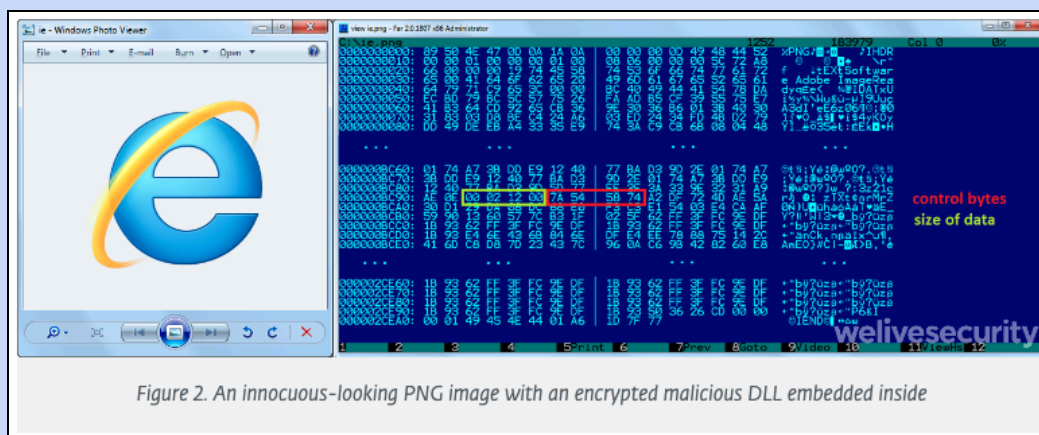
<sup>123</sup> AI学会造假, 我们该如何应对 [“AI Learns to Fake, How Should We Deal with It?”], 中央电视台网站 [CCTV.com News], April 16, 2019, <https://web.archive.org/web/20231026143814/http://news.cctv.com/2019/04/16/ARTI5p1mGY4iTGK2F63SIE97190416.shtml>.

## Steganography in Chinese Cyber Operations

Several Chinese APTs have used steganography in their operations. APT40, which operates under the direction of the Hainan State Security Department (海南国家安全厅), used this technique to transmit "stolen trade secrets and proprietary hydroacoustic data" via innocuous images (**Figure 6**).<sup>124 125</sup> APT15, which has been tentatively attributed to Xi'an Tianhe Defense Technology Co., Ltd. (西安天和防务技术股份有限公司), has used steganography to stealthily deploy malware while avoiding detection (**Figure 7**).<sup>126</sup> APT1, attributed to PLA Unit 61398 (61398部队), likely also used steganographic techniques.<sup>127</sup>



**Figure 6:** Images used by APT40 to transmit trade secrets (Source: US Department of Justice<sup>128</sup>)



**Figure 2.** An innocuous-looking PNG image with an encrypted malicious DLL embedded inside

**Figure 7:** Image used by APT15 to deliver the payload of the Okrum malware (Source: ESET Digital Security<sup>129</sup>)

<sup>124</sup> "Tactics, Techniques, and Procedures of Indicted APT40 Actors Associated with China's MSS Hainan State Security Department," Cybersecurity and Infrastructure Security Agency, July 20, 2021, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa21-000a>.

<sup>125</sup> United States of America v. Ding Xiaoyang et al., 27.

<sup>126</sup> Zuzana Hromcová, "Okrum: Ke3chang Group Targets Diplomatic Missions," We Live Security, <https://www.welivesecurity.com/2019/07/18/okrum-ke3chang-targets-diplomatic-missions/>.


<sup>127</sup> APT1: Exposing One of China's Cyber Espionage Units (Mandiant, February 19, 2013), 10, 60, <https://www.mandiant.com/sites/default/files/2021-09/mandiant-apt1-report.pdf>.

<sup>128</sup> United States of America v. Ding Xiaoyang et al., 27.

<sup>129</sup> Hromcová, "Okrum."

## Security Products

CIII advertises numerous security and forensic investigation products, services, and solutions relevant to the MSS's missions and those of the wider state security and public security apparatus. These devices cover use cases including conducting forensic or counterintelligence investigations of a given venue; preventing electronics from entering a given area; preventing data (in the form of signals and recordings) from being collected; and identifying, intercepting, and jamming mobile phones across the spectrum (2G-5G). Examples of these devices are listed in **Table 2**. Most are likely devices that CIII resells from other developers and manufacturers, but at least two are CIII- or BIETA-developed devices. Another product almost certainly developed by CIII or BIETA, but not advertised on CIII's website, is a fingerprint-secured USB drive, which BIETA certified with CNITSEC in 2006.<sup>130</sup>

Product(s)	Image	Additional Notes
Laptop Computer Information Protection Device		These devices were developed by CIII or BIETA. An older version of the device (shown left) was certified by CNITSEC in 2001. <sup>132</sup>
Desktop Computer Signal Protection Device (shown right)		These devices protect against information theft and leaks by interfering with signals emitted by a laptop or desktop computer. <sup>133</sup>



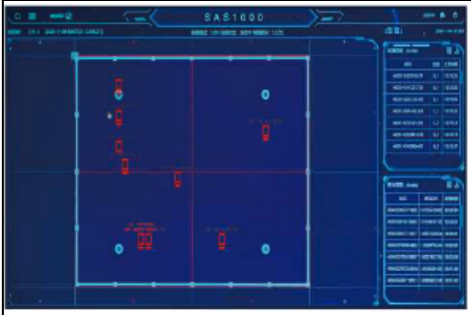
<sup>130</sup> 信息安全产品认证公告 (2007年第1号) ["Information Security Product Certification Announcement (2007 No. 1)"], 中国信息安全测评中心 [China Information Technology Security Evaluation Center], January 23, 2007, [https://web.archive.org/web/20240111001045/http://www.itsec.gov.cn/cp/cpgg/200701/t20070123\\_14786.html](https://web.archive.org/web/20240111001045/http://www.itsec.gov.cn/cp/cpgg/200701/t20070123_14786.html).

<sup>131</sup> 台式计算机信息保护机 (CNS-2) ["Desktop Computer Signal Protection Device (CNS-2)"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102201729/http://www.ciii.com.cn/12/5.html>.

<sup>132</sup> 关于通过产品认证年度监督的公告 ["Announcement on Passing the Annual Supervision of Product Certification"], 中国信息安全测评中心 [China Information Technology Security Evaluation Center], April 1, 2004, [https://web.archive.org/web/20240111001044/http://www.itsec.gov.cn/cp/cpgg/200404/t20040401\\_14805.html](https://web.archive.org/web/20240111001044/http://www.itsec.gov.cn/cp/cpgg/200404/t20040401_14805.html).

<sup>133</sup> 笔记本电脑信息保护机 (BGR-3) ["Laptop Computer Information Protection Device (BGR-3)"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102201728/http://www.ciii.com.cn/12/8.html>.

<sup>134</sup> "Desktop Computer Signal Protection Device (CNS-2)," CIII.

Product(s)	Image	Additional Notes
Environment Security Inspection Kit	 <span>135</span>	The kit includes an infrared thermal imaging detector, wireless environment analysis and warning system, handheld counter-surveillance detector, and camera detector for "security examination of general confidential places." <sup>136</sup>
3D Portable X-Ray Inspection Instrument	 <span>137</span>	
Large-Venue Cell Phone Positioning System	 <span>138</span>	A security solution for identifying, monitoring, positioning, and blocking mobile phones within large venues (such as within a conference room or building), including the ability to capture text messages and calls from controlled phones. <sup>139</sup>

<sup>135</sup> 环境安全检查套装 ["Environment Security Inspection Kit"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102190820/http://www.ciii.com.cn/64/50.html>.

<sup>136</sup> "Environment Security Inspection Kit," CIII.

<sup>137</sup> 3D便携式X射线检查仪 SXSD-XRAY ["3D Portable X-Ray Inspection Instrument SXSD-XRAY"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102192556/http://www.ciii.com.cn/64/45.html>.

<sup>138</sup> 大型环境信息安全防护-解决方案 ["Large-Scale Environment Information Security Protection-Solution"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102194345/http://www.ciii.com.cn/53/62.html>.

<sup>139</sup> "Large-Scale Environment Information Security Protection-Solution," CIII.



Product(s)	Image	Additional Notes
Recording Interference Briefcase	 140	

Table 2: Select security products advertised by CIII (Source: CIII)

Technology Transfer

Through BIETA and CIII, the MSS and PLA almost certainly benefit from access to international expert communities and foreign technology. BIETA and CIII’s activities are likely legal or were legal at the time the evidence described below was created — much of which comes from CIII’s website and likely dates to approximately 2017 or earlier. Nevertheless, BIETA and CIII’s operations likely continue to create technology transfer risks.

BIETA’s Academic Activities

BIETA’s researchers likely benefit directly or indirectly from international collaboration with other academics. Articles co-authored by BIETA personnel and others have been presented at various international conferences since at least 2012. Topics include “high capacity coverless image steganography,” models for studying network worms targeting social media users, and “audio signal authentication.”<sup>141 142 143</sup> A limited number of BIETA-affiliated articles presented internationally have further included co-authors at foreign academic institutions, specifically Deakin University in Australia and State University of New York at Buffalo in the US.<sup>144 145 146</sup>

<sup>140</sup> 录音干扰箱 SXSD-FLY05 [“Recording Interference Box SXSD-FLY05”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102194847/http://www.ciii.com.cn/53/56.html>.

<sup>141</sup> “Technical Program for Tuesday October 19, 2021,” 2021 IEEE International Conference on Systems, Man, and Cybernetics, No Date, [https://web.archive.org/web/20240110174402/https://webcache.googleusercontent.com/search?q=cache:nyfy-WHvgDsJ:https://conf.papercept.net/conferences/conferences/SMC21/program/SMC21\\_ContentListWeb\\_3.html&hl=en&gl=us](https://web.archive.org/web/20240110174402/https://webcache.googleusercontent.com/search?q=cache:nyfy-WHvgDsJ:https://conf.papercept.net/conferences/conferences/SMC21/program/SMC21_ContentListWeb_3.html&hl=en&gl=us).

<sup>142</sup> Tianbo Wang et al., “SADI: A Novel Model to Study the Propagation of Social Worms in Hierarchical Networks,” *IEEE Transactions on Dependable and Secure Computing*, vol. 16, no. 1 (January-February 2019), <https://ieeexplore.ieee.org/document/7814256>.

<sup>143</sup> Wei Zhong et al., “Electric Network Frequency Estimation Based on Linear Canonical Transform for Audio Signal Authentication,” 2017 25th European Signal Processing Conference (October 26, 2017), <https://ieeexplore.ieee.org/document/8081214>.

<sup>144</sup> Tianbo Wang et al., “SADI: A Novel Model to Study the Propagation of Social Worms in Hierarchical Networks.”

<sup>145</sup> Mengnan Zhao et al., “Source Camera Identification Based on Coupling Coding and Adaptive Filter,” *IEEE Access*, vol. 8 (December 13, 2019), <https://ieeexplore.ieee.org/document/8932363>.

<sup>146</sup> Guowen Zhang et al., “Source Camera Identification for Re-Compressed Images: A Model Perspective Based on Tri-Transfer Learning,” *Computers & Security*, vol. 100 (January 2021), <https://web.archive.org/web/20231030175829/https://www.sciencedirect.com/science/article/abs/pii/S0167404820303497>.

Whether BIETA researchers personally attend international conferences, such as the 2017 European Signal Processing Conference and those hosted by the Institute of Electrical and Electronics Engineers (IEEE), is unknown.<sup>147 148</sup> Given BIETA's almost certain affiliation with the MSS, if they do, these conferences very likely enable BIETA — and therefore China's primary intelligence service — to elicit feedback from foreign experts on topics of interest. Direct participation abroad would also very likely enable BIETA to spot experts working on similar issues that could be approached for collaboration or targeted by state security agents at a later date. Even if BIETA researchers do not travel abroad, BIETA can likely still benefit from international exposure in expert circles that legitimizes the organization if it reaches out to foreign universities or individuals. Past research into MSS tactics has found the intelligence service almost certainly relies "on genuine and internationally recognised academics to open doors, make introductions and gather intelligence."<sup>149</sup> In this context, the Chinese and foreign co-authors who work with BIETA could become conduits between the MSS and foreign expert communities.

### **CIII's Imports**

As noted, CIII claims it acts as an agent for US and European network testing, security, and simulation software products.<sup>150</sup> A variety of foreign software is advertised on its website, suggesting (in some cases even stating) that these are the products CIII resells — and those that it almost certainly works with — in providing services related to network environment simulation, penetration testing, and military equipment and operations modeling. Note that CIII may not have direct relationships with any of the foreign companies named on its website or mentioned below; its claims of having relationships with various products or companies are not independently verified. As indicated above, the information on CIII's website may not be current.

### **Steganography Software**

One of the technologies CIII advertises is WetStone Technologies's StegoHunt, which enables the discovery of steganography in a range of file types.<sup>151 152</sup> StegoHunt as allegedly sold by CIII almost certainly includes WetStone's StegoAnalyst and StegoBreak programs. These enable further analysis of and information extraction from investigated files. BIETA very likely benefits from CIII's access to this suite of foreign steganography tools.

### **Military Simulation and Modeling**

CIII advertises a range of foreign software and services related to communication simulation, 3D modeling, and operational planning for military and defense-industry use cases. These include "consulting and development" for third-party applications using Systems Tool Kit (STK) and Orbit

<sup>147</sup> "Technical Program," 25th European Signal Processing Conference 2017, No Date, <https://web.archive.org/web/20240110175412/https://www.eusipco2017.org/technical-program/>.

<sup>148</sup> "Technical Program," 2021 IEEE International Conference on Systems, Man, and Cybernetics.

<sup>149</sup> Joske, *Spies and Lies*, 138.

<sup>150</sup> "Product Center," CIII.

<sup>151</sup> StegoHunt™可疑文件探查工具 ["StegoHunt™ Suspicious Document Exploration Tool"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102204946/http://www.ciii.com.cn/40/23.html>.

<sup>152</sup> "StegoHunt™ MP Steganalysis and Steganography Detection Tool," WetStone Technologies, No Date, <https://www.wetstonetech.com/products/stegohunt-steganography-detection/>.

Determination Tool Kit (ODTK), programs developed by the US-based Ansys Government Initiatives (AGI).<sup>153 154 155 156</sup> As stated above, we have no evidence that CIII has a direct relationship with either AGI or the other foreign companies named on its website.<sup>157</sup>

Atoll, OPNET, RCS-Analyzer, WRAP, VEGA Prime, and MAK VR-Forces are other foreign software advertised on CIII's website.<sup>158</sup> CIII also offers a "3D digital electronic sand table," claiming "full military simulation production technology."<sup>159</sup> If the digital sand table referred to on CIII's website is not itself a foreign product, it almost certainly benefits from the foreign software to which CIII has access and for which CIII develops applications.

In about 2010, and no earlier than 2009, CIII very likely gave a presentation to the PLA or China's defense industry on QualNet and EXata.<sup>160</sup> Developed by the US-based Scalable Network Technologies (SNT), these software enable simulation, emulation, and analysis of communication networks.<sup>161 162 163</sup> The almost certain purpose of the presentation was to sell the value of these and related software programs — such as VisNet Defense, Network Centric Forces, and VR-Forces — for China's military and defense industry modernization. One slide in the presentation is titled "Start Our Complex Network — LandWarNet," which explains how the US Army's LandWarNet is structured.<sup>164</sup> According to the presentation, CIII's clients include PLA Electronic Engineering Institute (解放军电子工程学院; now part of the National University of Defense Technology [国防科技大学]);<sup>165</sup> several of the group of universities known as the "Seven Sons of National Defense" (国防七子);<sup>166</sup> and the state-owned defense contractor China Electronics Technology Group Corporation (CETC; 中国电子科技集团公司).<sup>167</sup>

## Network Simulation and Penetration

CIII advertises a number of "network functionality testing tools" and a "network offense-defense electronic range" from foreign providers. CIII almost certainly uses these products in its penetration testing activities and sells them to others engaged in similar activities. Products in the former category

<sup>153</sup> "Product Center," CIII.

<sup>154</sup> "About AGI: Ansys Government Initiatives," Ansys Government Initiatives, No Date, <https://www.agi.com/about>.

<sup>155</sup> "Ansys STK: Software for Digital Mission Engineering and Systems Analysis," Ansys, No Date, <https://www.ansys.com/products/missions/ansys-stk>.

<sup>156</sup> "Ansys Orbit Determination Tool Kit (ODTK)," Ansys, No Date, <https://www.ansys.com/products/missions/ansys-odtk>.

<sup>157</sup> Per communications from AGI, AGI does not conduct business in China, and Ansys has not identified any records of any sales, shipments, or authorized end use of its software products by BIETA or its CIII affiliate.

<sup>158</sup> 通信网络系统的仿真与开发 ["Communication Network Systems Simulation and Development"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102203617/http://www.ciii.com.cn/13/2.html>.

<sup>159</sup> 三维数字电子沙盘 ["3D Digital Electronic Sand Table"], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102211539/http://www.ciii.com.cn/42/26.html>.

<sup>160</sup> Source Held by Recorded Future.

<sup>161</sup> "SCALABLE Releases New Versions Of QualNet And EXata Modeling And Simulation Products," Wireless Networks Online, June 7, 2017, <https://www.wirelessnetworksonline.com/doc/scalable-releases-new-versions-qualnet-exata-modeling-simulation-products-0001>.

<sup>162</sup> "QualNet Network Simulator," Keysight Technologies, No Date, <https://www.keysight.com/us/en/assets/3122-1395/technical-overviews/QualNet-Network-Simulator.pdf>

<sup>163</sup> "EXata Network Modeling," Keysight Technologies, No Date, <https://www.keysight.com/us/en/product/SN100EXBA/exata-network-modeling.html>.

<sup>164</sup> Source Held by Recorded Future.

<sup>165</sup> Kenneth Allen and Mingzhi Chen, The People's Liberation Army's 37 Academic Institutions (China Aerospace Studies Institute, June 11, 2020), 42, [https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2020-06-11%20PLA%20Academic\\_Institutions.pdf](https://www.airuniversity.af.edu/Portals/10/CASI/documents/Research/Other-Topics/2020-06-11%20PLA%20Academic_Institutions.pdf).

<sup>166</sup> Marcel Angliviel de la Beaumelle, Benjamin Spevack, and Devin Thorne, *Open Arms: Evaluating Global Exposure to China's Defense-Industrial Base* (C4ADS, October 17, 2019), 21, <https://c4ads.org/reports/open-arms/>.

<sup>167</sup> Source Held by Recorded Future.

include a “network application layer functionality testing tool” called IxChariot that was developed by the US-based business Ixia, which was acquired by Keysight Technologies in 2017.<sup>168 169</sup> Among other products, CIII also advertises equipment from Spain’s ALBEDO Telecom, including Net.Storm “network imparer,” Net.Hunter “network monitor and analyzer,” and Ether.Giga “gigabit ethernet tester.”<sup>170</sup>

In the latter category — “network offense-defense electronic range” — CIII advertises Ixia’s (now Keysight’s) BreakingPoint cyber range.<sup>171</sup> Cyber ranges have legitimate defensive applications, such as simulating cyberattacks to strengthen an organization’s cybersecurity posture. They can also be used for training capabilities related to “‘target scouting, information theft, network intrusion ... information or service destruction, and other attack methods’, as well as for evaluating the ‘attack effects’ of various attacks,” according to authoritative Chinese military sources.<sup>172</sup>

### Other Applications

In 2016, CIII registered a “Datacrypt Hummingbird online storage upload software” (Datacrypt蜂鸟网盘上传软件) for copyright.<sup>173</sup> “Hummingbird” is likely a reference to “a lightweight encryption and message authentication” base-level algorithm (a “primitive”) first published during a 2009 conference organized by the Research Institute for Symbolic Computation in Austria.<sup>174</sup>

According to CIII’s website, the IDC it operates in Beijing makes use of these open-source and US technologies: a Cacti “network traffic monitoring platform,” Multi Router Traffic Grapher (MRTG) “network traffic monitoring,” and a SolarWinds “network load monitoring platform.”<sup>175</sup>

In addition to the aforementioned lines of business, BIETA and CIII also have or once had production lines for producing thick film circuits, micro-circuits, surface mounts, and bare chip mounts that relied on imported foreign machines from the US and Japan.<sup>176 177 178 179</sup> BIETA and CIII claim to produce communication equipment interface circuits, automobile ignition circuits, process-controlled switching and military-use analogue-digital/digital-analogue (AD/DA) converters, and “public security security

<sup>168</sup> IxChariot网络应用层性能测试工具 [“IxChariot Network Application Layer Functionality Testing Tool”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102204810/http://www.ciii.com.cn/15/22.html>.

<sup>169</sup> “Keysight Technologies Announces Closing of Acquisition of Ixia,” Keysight Technologies, April 18, 2017, <https://about.keysight.com/en/newsroom/pr/2017/18apr-nr17032.shtml>.

<sup>170</sup> 网络性能测试工具 [“Network Functionality Testing Tool”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20170922061416/http://www.ciii.com.cn/15/>.

<sup>171</sup> 网络攻防电子靶场 [“Network Offense-Defense Electronic Range”], 北京三信时代信息公司 [CIII], No Date, <https://web.archive.org/web/20231102204944/http://www.ciii.com.cn/40/24.html>.

<sup>172</sup> Devin Thorne and Zoe Haver, “From Coercion to Invasion: The Theory and Execution of China’s Cyber Activity in Cross-Strait Relations” (Recorded Future, November 23, 2022), 8, <https://www.recordedfuture.com/research/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity>.

<sup>173</sup> Source held by Recorded Future.

<sup>174</sup> Kai Zhang, Lin Ding and Jie Guan, “Cryptanalysis of Hummingbird-2,” Cryptology ePrint Archive, April 16, 2012, <https://web.archive.org/web/20120509144611/https://eprint.iacr.org/2012/207>.

<sup>175</sup> “IDC/ISP,” CIII.

<sup>176</sup> 简介 [“Introduction”], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20230605234119/http://www.bieta.cn/jgmore.htm>.

<sup>177</sup> “Research Institutions,” Beijing Institute of Electronics Technology and Application.

<sup>178</sup> “Company Introduction,” Beijing Sanxin Times Information Co.

<sup>179</sup> 微电路 [“Microcircuits”], 北京电子技术应用研究所 [Beijing Institute of Electronics Technology and Application], No Date, <https://web.archive.org/web/20170922113349/http://www.ciii.com.cn/7/>.



inspection circuits" (公安安检电路) among other items.<sup>180 181</sup> All of the machines and images related to this activity on BIETA's and CIII's websites are older, likely dating at least to the 1990s or early 2000s. How active these production lines are as of this writing is unknown.

## Implications for Understanding the MSS

Discovery of BIETA's almost certain affiliation with the MSS brings additional clarity to the MSS's role in offensive Chinese cyberspace and cyber-enabled intelligence activities, and to the MSS's organizational structure. The MSS — which sits atop a network of sub-national, semi-autonomous state security organizations — very likely plays a supporting role in cyberspace operations. BIETA's research is almost certainly used to create technologies that enable the MSS's mission. The MSS then likely makes capabilities benefiting from BIETA's achievements available to subordinate state security departments, bureaus, and officers, which in turn provide them to their contractors or proxies. In the field of steganography, these technologies likely include programs to covertly transmit information and programs to detect information covertly transmitted by the CCP's adversaries.

This model, wherein the MSS's research institutions or partners very likely support the development of technology that is distributed to others throughout the state security apparatus, is supported by prior research and evidence. First, the MSS very likely evaluates vulnerabilities submitted to national vulnerability databases, including one run by the MSS-subordinate CNITSEC, for their utility in cyber espionage, almost certainly to distribute these to Chinese APTs.<sup>182 183</sup> Second, as mentioned, state security intelligence officers have reportedly "received malware from the MSS to be used against foreign victims" in known cyber espionage cases.<sup>184</sup> Third, state security intelligence officers have provided malware to cyber threat actors<sup>185</sup> and provided recruited foreign assets with COVCOM devices and steganography training.<sup>186</sup> Cyber talent at the provincial level of the state security system — which is more directly involved in managing offensive cyber operations<sup>187 188</sup> — likely also develops tools for operational use.<sup>189</sup>

Additionally, the overlap between BIETA and CNITSEC personnel likely indicates that both organizations were organized under the former 13th Bureau, and that this bureau's remit was likely much broader than just network security as most public attention to CNITSEC suggests. Aligning with the aforementioned references to former CNITSEC Director Wu Shizhong as the head of the "MSS Science and Technology

<sup>180</sup> "Introduction," Beijing Institute of Electronics Technology and Application.

<sup>181</sup> "Company Introduction," Beijing Sanxin Times Information Co.

<sup>182</sup> Dakota Cary and Kristin Del Rosso, "Sleight of hand: How China weaponizes software vulnerabilities," Atlantic Council, September 6, 2023, <https://www.atlanticcouncil.org/in-depth-research-reports/report/sleight-of-hand-how-china-weaponizes-software-vulnerability/>.

<sup>183</sup> Priscilla Moriuchi and Dr. Bill Ladd, "China's Ministry of State Security Likely Influences National Network Vulnerability Publications," Recorded Future, November 16, 2017, <https://www.recordedfuture.com/blog/chinese-mss-vulnerability-influence>.

<sup>184</sup> United States of America v. Ding Xiaoyang et al., 12.

<sup>185</sup> United States of America v. Zhang Zhang-gui et al. (California: US District Court for the Southern District of California, October 25, 2018), 14-15, <https://www.justice.gov/archives/opa/press-release/file/1106491/dl?inline=>.

<sup>186</sup> United States of America v. Kevin Patrick Mallory, 9-11.

<sup>187</sup> United States of America v. Zhang Zhang-gui et al.

<sup>188</sup> Insikt Group, "Recorded Future Research Concludes Chinese Ministry of State Security Behind APT3."

<sup>189</sup> *Hearing before the U.S.-China Economic and Security Review Commission on "China's Cyber Capabilities: Warfare, Espionage, and Implications for the United States,"* 117th Cong. (2022), p. 2 (testimony of John Chen, Lead Analyst at the Center for Intelligence and Analysis), [https://www.uscc.gov/sites/default/files/2022-02/John\\_Chen\\_Testimony.pdf](https://www.uscc.gov/sites/default/files/2022-02/John_Chen_Testimony.pdf).

Bureau,"<sup>190</sup> the MSS's former 13th Bureau likely also oversaw the development of various technologies relevant to the MSS's intelligence, counterintelligence, and investigative responsibilities, likely to include some biomedical research.<sup>191</sup> <sup>192</sup> However, the remit of the MSS's former 9th Bureau likely covered communications surveillance and security, surveillance and forensic technology, and cybersecurity research through the Nanjing Institute of Information Technology (南京信息技术研究院).<sup>193</sup> It is, therefore, also plausible that BIETA was organized under the 9th Bureau. The MSS's organizational structure has changed since 2018; the former 13th Bureau's new number is unknown, and the former 9th Bureau has become the 14th Bureau, though it is unconfirmed whether the new 14th Bureau retains a cybersecurity remit.<sup>194</sup>

## Outlook

Public evidence of the MSS's very likely vast network of front organizations and co-optation of entities for intelligence activities is increasing. This evidence includes cybersecurity companies engaged in offensive operations, universities leveraged for intellectual property theft, non-profit organizations used for social influence, and now — almost certainly — research institutes and their subordinate firms established to provide technology enablement.

BIETA and CIII almost certainly pose technology transfer risks. How often BIETA and CIII conduct business outside of China or collaborate with foreign experts is unknown. However, foreign export control authorities concerned about the Chinese intelligence community and military's access to COVCOM technologies like steganography, network simulation, penetration testing, and 3D and communications modeling technologies should review these entities. They should consider warning government and military officials in their countries about these organizations' assessed links to the MSS and PLA and potentially add them to lists of organizations for which approval is needed to export sensitive technology.

Foreign academic institutions and businesses with activities related to COVCOM, network penetration, network simulation, advanced modeling, and forensic technologies should, during security training, advise staff about risks stemming from engagement with anyone asserting a BIETA or CIII affiliation to avoid inadvertently contributing to the capabilities of the MSS, PLA, and wider Chinese party-state security apparatus. Academics or staff who are approached by either organization should be instructed to report this to appropriate security contacts. More generally, before agreeing to any transaction involving sensitive or potentially sensitive technologies, academic institutions and businesses should attempt to thoroughly investigate their would-be partners or clients.

<sup>190</sup> "Notice on the Establishment of a National Standardization Systems," Civil Affairs Technology and Standardization Information Platform.

<sup>191</sup> 崔承彬 ["Cui Chengbin"], 沈阳药科大学校友会 [Shenyang Pharmaceutical University Alumni Association], May 20, 2017, <https://archive.ph/LqL6p>.

<sup>192</sup> Mattis and Brazil, *Chinese Communist Espionage*, 56.

<sup>193</sup> Joske and Jeon, "Redesigning State Security," 6-7.

<sup>194</sup> Joske and Jeon, "Redesigning State Security," 6-7, 11.

Recorded Future reporting contains expressions of likelihood or probability consistent with US Intelligence Community Directive (ICD) 203: Analytic Standards (published January 2, 2015). Recorded Future reporting also uses confidence level standards employed by the US Intelligence Community to assess the quality and quantity of the source information supporting our analytic judgments.

#### About the Author

Devin Thorne is a Principal Threat Intelligence Analyst on Insikt Group's Global Issues Team at Recorded Future, where he covers China's security strategies, national defense mobilization system, propaganda work, and aspects of military modernization. He has previously conducted research for the US Naval War College China Maritime Studies Center, Center for Advanced Defense Studies (C4ADS), and other organizations. He has also testified before the U.S.-China Economic and Security Review Commission. Thorne has a bachelors from the University of Alabama at Birmingham and a masters from the Hopkins-Nanjing Center for Chinese and American Studies. He speaks Mandarin.

#### About Insikt Group®

Recorded Future's Insikt Group, the company's threat research division, comprises analysts and security researchers with deep government, law enforcement, military, and intelligence agency experience. Their mission is to produce intelligence that reduces risk for customers, enables tangible outcomes, and prevents business disruption.

#### About Recorded Future®

Recorded Future is the world's largest intelligence company. The Recorded Future Intelligence Operations Platform provides the most complete coverage across adversaries, infrastructure, and targets. By combining precise, AI-driven analytics with the Intelligence Graph® populated by specialized threat data, Recorded Future enables cyber teams to see the complete picture, act with confidence, and get ahead of threats that matter before they impact your business. Headquartered in Boston with offices around the world, Recorded Future works with more than 1,900 businesses and government organizations across 80 countries.

[Learn more at recordedfuture.com](https://www.recordedfuture.com)