LAWRENCE
LIVERMORE
NATIONAL
LABORATORY

LLNL-TR-593952

More Than Meets the Eye: Clandestine Funding, Cutting-Edge Technology and China's Cyber Research & Development Program

C. Conklin, B. W. Bahney

October 23, 2012

Disclaimer

This document was prepared as an account of work sponsored by an agency of the United States government. Neither the United States government nor Lawrence Livermore National Security, LLC, nor any of their employees makes any warranty, expressed or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States government or Lawrence Livermore National Security, LLC. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States government or Lawrence Livermore National Security, LLC, and shall not be used for advertising or product endorsement purposes.

This work performed under the auspices of the U.S. Department of Energy by Lawrence Livermore National Laboratory under Contract DE-AC52-07NA27344.

More Than Meets the Eye: Clandestine Funding, Cutting-Edge Technology and China's Cyber Research & Development Program

Kit Conklin
Mentor: Benjamin Bahney

Over the course of the last decade the central government of the People's Republic of China has utilized a national grant system to invest in the research and development of new dual-use cyber capabilities. In order to understand the defense implications of these investments, this research will examine how China is investing resources to develop new cyber capabilities for national security applications. Through the collection of publicly available sources in Mandarin and English, this research will analyze how the Chinese leadership views information technology research and development (R&D), as well as the role cyber R&D plays in China's various strategic development plans. This work also explores the organizational structure of China's cyber R&D base. The paper will conclude with a projection of how China might field new cyber capabilities for intelligence platforms, advanced weapons systems, and systems designed to support asymmetric warfare operations.

Introduction

Grants and Cyber Capabilities: A Civil-Military Cocktail

In order to advance national security and economic interests, the government of the PRC is using a national grant system to not only strengthen civil-military cooperation, but also to develop new cyber capabilities. The State High-Technology Research and Development Program (国家高技术研究发展), widely referred to as the 863 Program, is a nation-wide grant system that the central government uses to fund a variety of research and development (R&D) projects deemed to be of critical importance to the country. Through the analysis of how this grant system is being used to R&D inherently dual-use cyber capabilities, it is possible to interpret what types of information technology the Chinese may be seeking to field for C4ISR platforms and advanced weapons systems. However, before an in-depth analysis of these programs can take place, it is necessary to analyze how the Chinese leadership generally approach cyber capabilities.

Strategic Development Plans and Cyber R&D

China's various strategic development plans provide broad outlines that describe what the country's IT R&D priorities are for a given period of time. However, the strategies stop short of explicitly stating what technologies should be developed or how R&D funding should be allocated. The highest level versions of these strategies are known as Five-Year Plans (FYP), currently in its 12th iteration (2011-2016). Under the auspices of these FYPs, the Ministry of Science and Technology has released a number of cyber development plans that provide specific details as to which technologies should be developed. Other plans, like the 2006 National Outline for Medium and Long-Term Science and Technology Development Plan (zhongwen), signal the leadership's strategic vision for cyber capability development and implementation. Although sometimes bureaucratically isolated, these strategies share two primary objectives: improving indigenous technology innovation and strengthening civilian-military cooperation in the field of cyber research and development.

Medium and Long-Term Science and Technology Development Plan (MLP)

In 2006 the 16th National Congress of the Chinese Communist Part commissioned the MLP in order to outline a medium-term (2006-2020) development strategy aimed at increasing the country's technological capabilities. The backbone of the MLP is a prioritized R&D hierarchy that emphasizes eleven 'key' research areas and eight types of 'frontier technologies. These areas and frontier technologies range from laser and aeronautics to national defense and public security applications. That said, Chinese policy makers are heavily emphasizing information technology R&D in the MLP. IT is one of only three technologies listed in both 'key research areas' and 'frontier technologies,' the other two being advanced energy and manufacturing systems.

The MLP goes into incredible detail when discussing how the central government should enhance technical research and development capabilities. Measures advocated include industry-university technology sharing programs, preferential laws for small-medium sized companies developing relevant technologies, and long-term central government financial support for R&D projects. The MLP also states that China's central government should "vigorously support" university-based frontier technology development, which helps explain why universities are the primary benefactors of government IT R&D grants.

Even though the MLP was published in 2006, the majority of cyber systems currently being researched and developed in China closely relate to the IT research priorities outlined in the MLP. Research areas listed in the frontier technologies' IT section include advanced computing, network and communication systems, virtual reality systems for military applications, and microelectronics.[1] Capabilities that fall under these four categories are also prioritized in China's other development strategies, including two consecutive Five-Year Plans.

Five-Year Plans (FYPs)

China's Five-Year Plans (中国五年计划) are comprehensive strategies designed to communicate the leadership's development priorities to the country's bureaucracies. Historically FYPs have focused on broad economic and infrastructure development. However since the 11th FYP (2006-2010), China's industrial policy has become more focused and now primarily

[1] "National Outline for Medium and Long Term Science and Technology Development Planning (2006–2020)," Ministry of Science and Technology of the People's Republic of China, February 9, 2006, www.most.gov.cn

emphasizes scientific development and ways the central government can support 'strategic emerging industries,' which includes next-generation information technology.[2]

Both the 11th and 12th (2011-15) FYPs emphasize a development strategy centered around the theory of informationization (信息化) and indigenous innovation (自主创新) of high-technologies. Informationization focuses on modernizing China's IT infrastructure, including industry, military and university capabilities. The FYPs also reemphasize IT R&D priorities outlined in the MLP. Advanced computing, network and communication systems, virtual reality systems, and microelectronics are all discussed. The 12th FYP promotes these MLP priorities by listing capabilities the country should develop from 2011-2015. These technologies include network monitoring and controlling systems, microelectronics for aviation and spaceflight, and cloud computing systems. However, the 12th FYP stops short of listing highly detailed technologies the country should develop. These broadly defined guidelines allow the country's leadership to evolve and adapt specific R&D priorities each year.

Internet Armies: The PLA & Cyber R&D Strategy

High-ranking officials of the Chinese Communist Party and the People's Liberation Army (PLA) have identified the electromagnetic spectrum as a "fifth domain of battlespace."[3] Furthermore, the PLA identifies advancements in information warfare as a revolution in military affairs (军事革命).[4] By doing so the Chinese leadership signaled that operations within cyberspace are to be considered as important to national security as the four physical domains: land, sea, air and space. Chinese state-run media have even called for the central government to fund the PLA's efforts to develop a cyber warfare unit capable of rivaling any of the "world's [most] advanced Internet armies."[5] In order to accomplish this mission, media reports indicate that the PLA should focus on recruiting cyber warfare specialists from civilian organizations like universities and research institutes. In this regard Hu Jintao, president of the PRC and chairman of the Central Military Commission, stated that the recruitment and cultivation of talent is a "pillar for the scientific development of China's defense and military."[6]

As the PLA attempts to advance its capabilities for this new 5th domain, they are receiving support from a variety of organization and entities throughout the country, including the Ministry of Science and Technology. During an interview coinciding with the 2006 release of the MLP, Ma Songde, then the Vice Minister of the Ministry of Science and Technology[7], stated that research grants should be used to "further strengthen military-civilian interaction and the

[2] Joseph Casey, Katerhine Koleski, "Backgrounder: China's 12th Five-Year Plan," US-China Economic and Security Review Commission, 24 June 2011

[3] Bryan Krekel, Patton Adams, George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage," Prepared for the US-China Economic and Security Review Commission by Northrop Grumman Corporation, 7 March 2012, www.uscc.gov

[4] 王稚, "军事革命/转型的定义和内涵," August 2003, www.china.org.cn

[5] Li Hong, "China's Cyber Squad if for Defense," People's Daily, 31 May 2011

[6] Li Hong, "China's Cyber Squad if for Defense," People's Daily, 31 May 2011

[7] And currently the 863 Program's Director

sharing of resources…especially in conjunction and implementation of major projects like supercomputers.” During the same interview Ma went on to state that 863 research grants should be used to “improve high-tech military weaponry and equipment, which is the technological foundation for winning a war being fought under high-tech conditions.” [REF?]

Indigenous Technology Development

Language used in FYPs, the MLP, and by various CCP and PLA officials reveals that Chinese policy makers are using civilian and military organizations to indigenously R&D cyber capabilities. In 2011 Congressional testimony focusing on Chinese espionage and technology, Adam Segal posited that China is employing this strategy in order to decrease dependence on foreign technologies.[8] This may be true but other questions remain unanswered. Primarily, why are the Chinese developing specific cyber technologies and how can these new indigenous capabilities be fielded for national security applications? In order to answer these questions, it is necessary to examine exactly what types of capabilities the Chinese are investing in.

863 Program Overview

China’s R&D Grant Programs

China utilizes four national-level grant systems to fund R&D projects deemed to be of critical economic and national security importance. The four grant programs are the State High-Technology Research and Development Program (863), the National Key Basic Research Program (973), the National 242 Information Security Program, and finally the Ministry of State Security’s 115 Program. Each of these grant systems have reportedly funded information technology projects that can be fielded for military applications.[9]

The four grant programs are not entirely isolated from one another –possible overlap exists. For example, a collection of materials released in 2010/11 by entities associated with the University of Electronic Science and Technology’s School of Computer Science and Engineering reveal potential R&D project overlaps. By combining information from university press releases with student and professor resumes, evidence suggests military-specific IT R&D was simultaneously being conducted with 863 Program grants as well as with funding from the Ministry of State Security’s 115 Program.[10][11]

[8] Adam Segal, “Innovation, Espionage, and Chinese Technology Policy,” Prepared Statement before the House Foreign Affairs Subcommittee on Oversight and Investigations

[9] Bryan Krekel, Patton Adams, George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage,” Prepared for the US-China Economic and Security Review Commission by Northrop Grumman Corporation, 7 March 2012, www.uscc.gov

[10] “网络与信息系统团队,”电子科技大学: 科研学术科研机构, Accessed 9 August 2012, www.ccse.uestc.edu.cn; “我校积极参与国家 863 计划军口部分’十二五’项目申报工作,” 电子科技大学：新闻中心, 13 October 2011, www.rd.uestc.edu.cn/

Classified Military-Specific IT Projects

Established in 1986, the State High-Technology Research and Development Program (863) is a national grant system whose primary objective is to “accelerate China’s high-tech development.”[12] The Ministry of Science and Technology plays a significant administrative role in the day-to-day operations of the Program. However, a so-called “steering group” appears to have a great deal of power managing major issues. The steering group coordinates 863 Program priorities with China’s State Council, the country’s top decision-making body. The group is composed of members from MOST, PLA General Armament Department, the State Administration for Science, Technology and Industry for National Defense (SASTIND), and the Ministry of Finance.[13] The exact bureaucratic power hierarchy within the steering group is ambiguous, but Chinese government sources list the General Armament Department as the sole entity responsible for planning and organizing the 863 Program’s military-specific projects.[14]

Internally, the Program is headed by Director Ma Songde and is organized into a number of expert groups responsible for selecting and administering grant projects. The Committee of Experts (COE) is the key powerbroker within the Program and has 44 members. In regards to IT R&D projects, the COE is divided into three panels – networks and communications (网络通信技术), advanced computer technologies (先进计算技术) and information security technologies （信息安全技术）. These panels are comprised of individuals from government and industry and appear to be tasked with screening IT R&D grant applications.

The 863 Program differs from China’s other national grant systems, primarily because of its separate and often classified funding for military projects. During a 2006 interview, Program Director Ma Songde stated that 90% of 863’s R&D projects are not classified.[15] His statements are difficult to verify because of the lack of budgetary transparency. For instance, the Program’s published budget for 2009 was roughly 5.1B Renminbi but that number does not include 863 funding earmarked for the R&D of military systems.[16] The specifics of the funding as well as the breadth of the military program’s research is unclear due to redactions of key pieces of information from documents. However, available documents indicate that 863 military-specific grants are funding classified IT R&D projects.[17][18]

[12] Ministry of Science and Technology of the People’s Republic of China, “National High-Tech R&D Program (863 Program),” Science and Technology Programmes, accessed 1 August 2012, www.most.gov.cn

[13]“863”计划,” 中国国家数字化图书馆:科研申请, Accessed 2 August 2012, www.nlc.gov.cn

[14] “863”计划,” 中国国家数字化图书馆:科研申请, Accessed 2 August 2012, www.nlc.gov.cn

[15] 光明网, “马颂德：863 计划管理将更加公开公正,” 淮南市科学技术 15 August 2011, www.hnkjj.gov.cn

[16] Bryan Krekel, Patton Adams, George Bakos, Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage,” Prepared for the US-China Economic and Security Review Commission by Northrop Grumman Corporation, 7 March 2012, www.uscc.gov

[17] “863 及 973 项目,” 合肥工业大学: Data Mining and Intelligent Computing Laboratory, Accessed 10 August 2012, www.dmic.hfut.edu.cn

Cyber Research and Development

863 Program funding is not limited to developing information technologies. The last three FYPs have outlined six so-called "high-tech priority fields," which are areas Chinese policy makers believe are of strategic national importance. These priority fields are biotechnology, advanced materials technology, manufacturing and automation, energy technology, environment technology and information technology.[19] A sample of publically available 863 Program documents, research proposals, and grant applications confirm that Program funding is being used for projects relating to these six fields. [REF?] These same documents also show that grants worth millions of U.S. dollars are being given to both civilian and military organizations to develop a wide variety of dual-use projects in information technology, some of which seem to support new cyber capabilities with national security applications.

Overview of 863 IT Projects

Since 2008, the 863 Program and the Ministry of Science and Technology have released a string of annual research guidelines and applications that explain what types of cyber technology R&D grants are available. These guidelines are broken down under a hierarchical system of R&D categories, published in Mandarin, and then released to both civilian and military organizations across China. Roughly ten months after MOST releases the guidelines, the 863 Program publishes a report explaining which organizations were awarded grants for that year.[20]

These guidelines and reports offer a unique view into the organizational structure of China's cyber R&D base. Through the analysis of these reports, it is possible to breakdown which entities are responsible for the R&D of certain technologies. Furthermore, and perhaps more importantly, they reveal exactly what types of cyber capabilities the Chinese are currently developing.

Core R&D Fields

Since the MLP was published in 2006, the 863 Program's information technology projects have focused on researching and developing four primary scientific fields: advanced computing, networking and communications, virtual reality, and micro/optoelectronics.[21] These four areas were listed in the 11th and 12th FYPs and appear to represent the apex of China's IT

[18] 李卫海, "李卫海申请 2009 年度中国科学技术大学校友基金会优秀青年教师奖材料," An Award Application, accessed 10 August 2012

[19] Ministry of Science and Technology of the People's Republic of China, "National High-Tech R&D Program (863 Program)," Science and Technology Programmes, accessed 1 August 2012, www.most.gov.cn

[20] "2012 年度国家 863 计划信息技术领域备选项目," 863 计划, 2012

[21] "国家 863 计划确定 2012 年度信息技术领域支持重点," 中国科学院信息化研究与应用快报, 1 April 2012, www.ecas.cn

R&D priorities. Under the auspices of developing these four core areas, China is also developing an extensive list of potentially dual-use cyber capabilities.

Projects:

Advanced Computing

- Analytics
    - Systems Management Platforms and Applications for (High-Risk/Risky) Open Source Internet Data Extraction, Integration and Analysis
    - Large-scale Chinese (Semantic) Language Information Processing Methods, Technology and Systems
- Multicore Processor Programing and Runtime Support Technologies
    - Trajectory and Process Optimization Software
- Advanced Storage of Large Data
    - Semiconductor-based memory storage systems
    - Efficient storage of meta data
- Cloud Integration
    - Operational monitoring systems
- Simulation Technologies
    - Behavioral Modeling Techniques
    - Designed to automatically model interactions within a 400 square meter operational space

Networking and Communications

- High-speed routing and switching systems
    - Ultra-high Speed (1 Tbps+) Long Distance (1,000km+) Fiber Optic Transmission Systems
    - Ultra-Large Capacity Fiber Optic Switching and Networking Research
- Visible Light Communication (VLC)
    - Non-coherent Light Scattering Distortion Detection
    - Development of Visible Light (380nm-780nm) Communications Systems
    - Indoor Systems
        - Multipath Interference and Link Vulnerability Research
- Security
    - Anti-attack Node Routing Technology
        - Node Communications and Safety
        - Intrusion Tolerance of Malicious Technologies
    - Encryption

Virtual Reality

- Key Technologies, Techniques and Systems Applications for 3D Content
    - Physical Systems

        - Accelerometers
        - Electromyography Sensors
            - Designed to Capture Gestures
            - Write Gesture Recognition Algorithms
            - Develop Miniaturized Wearable Gesture Caption Device
- Real-Time Situational Awareness for Digital Methods and Systems
    - Real-time Graphics Rendering Engines
    - Precise Tracking & Positioning Systems
- Large-scale Multi-mode 3D Demonstrations/Displays
    - Helmet Display Systems
        - Horizontal Field of View Greater than 70 Degrees
        - Integration for Immersive Gaming Applications
    - Multisensory Experience Synchronization Control and Displays
    - Large-scale 3D Holographic Displays
- Human-Computer Cooperation Based on Auditory Information Processing and Interaction Technology
    - Precision Natural Feature Tracking and Registration Platforms
    - Non-contact Body Posture Awareness Technologies

Microelectronics

- Field Programmable Logic Devices and Gate Arrays (FPLD/GAs)
- Synchronous Dynamic Random-Access Memory (SDRAM)
    - Submicron Liquid Crystal Cell Manufacturing
    - Micro High Resolution (1024x768) LCOS Chips
- Multiband Transceiver Circuits
    - Jam-resistant, block-resistant, and noise-resistant
- Advanced Remote Data Processing Sensors
    - Hyperspectral-imaging applications
- Internal and External High-precision Navigation Technology

China's Cyber R&D Base:
Civil-Military Integration

The strength of the China's cyber R&D base lies within its hybrid civil-military organizational structure. Chinese policy makers recognize the dual-use role of cyber capabilities and openly advocate utilizing the 863 Program's research base to develop new technologies. This has allowed the government to openly distribute 863 R&D funds to civilian organizations so that they can develop potential national security applications. For example, many of China's top civilian universities and research institutes are simultaneously developing cyber technologies with entities associated with the People's Liberation Army (PLA) and the Ministry of Public

Security.[22] [23] Furthermore, Chinese policy makers are seeking to incorporate university-industry and military-industry collaborations into the cyber R&D base by awarding information technology R&D grants to state-owned enterprises and private companies.

Civilian Universities and Research Institutes

China's central government is employing civilian universities and research institutes to research and develop dual-use cyber systems. The 863 Program has designed a hierarchical grant management system incorporating the Ministry of Education, the Chinese Academy of Sciences, and the Ministry of Public Security.[24] And although the exact relationship between these organizations and the 863 Program remains unclear, these three organizations have been designated "recommended divisions" tasked with overseeing the "primary units" responsible for the actual R&D of a capability.

863 grant funding is also being distributed directly to provincial level Ministries of Science and Technology. Once at the provincial ministry level, funding patterns suggest that cyber R&D grants are being awarded to computer science schools at local science and technology universities. This differs from 863 grants administered by the Ministry of Education, who in 2012 tended to award grants to China's top-tier universities (such as Beijing, Renmin, Tsinghua, Shanghai Jiaotong, etc.).

Industry

Many of China's largest telecommunications companies, including ZTE, Huawei, Haige and China Electronics Technology Group have received 863 IT R&D grants.[25] This is partially a result of the Chinese leadership advocating the development of civil-commercial-military cyber R&D parks. These parks, commonly referred to as high-tech development zones, are massive areas where high-tech companies and research institutes can enjoy a preferential business environment. Parks like the Wuhan East Lake High-Tech Zone are home to a wide variety of organizations that received 863 cyber R&D grants in 2012, including the Wuhan Institute of Posts and Telecommunications and the ZTE Corporation.[26] (Both Wuhan Institute and ZTE were awarded funds from the same grant category to develop fiber optic switch and network applications.)

In 2012, multiple municipal-level science and technology commissions (STCs) awarded 863 grants to both private and semi-autonomous companies located within that municipality's jurisdiction. Examples of this include the Chongqing STC administering a grant given to China

[22] 2012 863 Alternative IT Grants, #1 – PLA, Huawei, and all of the universities and institutes

[23] 李卫海, "李卫海申请 2009 年度中国科学技术大学校友基金会优秀青年教师奖材料," An Award Application, accessed 10 August 2012

[24] "2012 年度国家 863 计划信息技术领域备选项目," 863 计划, 2012

[25] "2012 年度国家 863 计划信息技术领域备选项目," 863 计划, 2012

[26] "Wuhan East Lake High-Tech Park: Facts & Figures 2010," Hong Kong Trade Development Council, 19 September 2011, www.hktdc.com

Electronic Technology Group's 24th Research and Development Institute, and the Shenzhen Trade, Industry, and Information Technology Commission being the 'recommended division' overseeing a grant awarded to Huawei Technologies. These STCs play a major role in administering national 863 grants to local research institutions because they are "responsible for the formulation of the budget [for] local scientific and technological funds…and the supervision and administration of their use."[27] Although the exact relationships between STCs and the majority of companies they have recommended receive 863 funds are unknown, it is worth noting that allegations of corruption are associated with some of China's municipal-level STCs.[28]

People's Liberation Army

Numerous PLA-sponsored organizations have received 863 grants to R&D dual-use cyber projects, including universities and the offices of the General Staff Department. As for academic institutions, the primary universities receiving grants are the PLA National University of Defense Technology and the PLA Information Engineering University – both of which report directly to the PLA General Staff Department[REF?]. The schools operate robust computer science programs that have received grants to R&D projects associated with 863's four core IT priorities.

National University of Defense Technology (NUDT)

Having been recognized by the State Council for its cyber developments in the fields of space technologies and high-performance computer systems, NUDT (国防科学技术大学) is one the primary national defense research institutions in China. The university emphasizes a doctrine called "Joint-Training," which focuses on training PLA officers for "informationized warfare" (信息化战争).[29] Through this training, dozens of research projects related to military applications are currently being pursued at the university. Although the majority of these projects are not being funded by 863 grants, NUDT has been awarded 863 funding to R&D microelectronics, information security technology, and virtual reality platforms. The specifics of these awarded grants have not yet been published but NUDT is currently developing a number of relevant military applications, including unmanned aerial vehicle and satellite control systems, target recognition software, and cryptography.[30]

Information Engineering University (IEU)

Established after a 1999 merger of two PLA research institutes, the Information Engineering University works on a breath of projects ranging from geographic information systems to cyber security. As for IT R&D, IEU has been awarded a variety of 863 grants.[31] In

[27] "Shanghai Municipal Science and Technology Commission," Office of the Shanghai Government, 3 October 2009, www.shanghai.gov.cn

[28] "Yubei Science and Technology Commission, Moon Cake Boxes Bribery Jailed for Possession of Cash," Like News, 20 July 2012, www.likenews.us

[29] 杨学军, "校长致辞," 国防科学技术大学, Accessed 10 August 2012, www.nudt.edu.cn

[30] "研究子方向二," 国防科学技术大学, Accessed 3 August 2012, www.nudt.edu.cn

[31] "2012 年度国家 863 计划信息技术领域备选项目," 863 计划, 2012

regards to the dual-use nature of these grants, IEU prides itself on its military research strengths and "rejects any scientific research programs that have little relation with the actual combat."[32] Since the university is reluctant to accept non-military related research projects, yet they are recipients of 863 grants, it is probable that IEU's 863 grants are solely being used to fund the R&D of the PLA's cyber capabilities.

Technical Readiness Levels

Through the analysis of China's R&D priorities and technical readiness levels (TRLs), it is possible to project what new cyber capabilities the Chinese might field for intelligence platforms and weapons systems. TRL assessments eliminate some speculation about operational capabilities because they help distinguish field-ready applications from projects in the infant stages of R&D.[33] That said, this research will focus on China's near-term C4ISR[34] capabilities that can be fielded for signals intelligence (SIGINT) and geospatial intelligence (GEOINT) platforms. The section will conclude with an examination of how China may incorporate new cyber technologies in advanced weapons systems designed to increase the PLA's asymmetric warfare capabilities.

SIGINT Systems

Of the 863 Program's four key research priorities, projects being developed under the auspices of advanced computing and networking/communications are the most relevant for signals intelligence. R&D projects focusing on advanced information analytics have the potential to significantly impact the way China's foreign and domestic intelligence ministries collect and analyze information.

The 863 Program has awarded multiple grants to universities and research institutes across China for the development of natural language processing systems.[35] Such artificial intelligence platforms allow computers to extract meaningful data from human language input systems (IE a computer monitoring a telephone conversation and red flagging the data when a certain word was spoken). According to 863 grant applications the Chinese are looking to develop these technologies for Mandarin language processing. These systems could be used to better monitor domestic SIGINT traffic for surveillance and information control purposes. That said, if China is capable of fielding analytical platforms for Mandarin, it is possible that the systems could be reconfigured for foreign language monitoring capabilities. This is a logical progression because it is more difficult to develop

[32] "Information Engineering University Docks Research with Battle Demands," Ministry of National Defense of the People's Republic of China, 19 April 2005, www.mod.gov.cn

[33] This TRL assessment was conducted by examining what types of deliverables 863 grant applications call for (ex. basic observations, analytical concepts, system prototype, etc.).

[34] C4ISR – Command and control, communications, computers, intelligence, surveillance, and reconnaissance

[35] "2012 年度国家 863 计划信息技术领域备选项目," 863 计划, 2012

systems that monitor tonal languages like Chinese than it is develop similar systems for non-tonal languages (English, Japanese, German, etc.).[36]

A 2009 grant application calls for the development and demonstration of different platforms capable of controlling and monitoring computer networks. The application lists dozens of technologies but the most relevant for near-term field-ready SIGINT capabilities concerns a system utilizing deep packet inspections (DPIs) for data exfiltration. DPIs are commonly used as a network management tool because they monitor data as it flows through a network, often for virus and spam detection. However, DPIs can also be utilized for SIGINT capabilities like data mining, eavesdropping and censorship.[37]

The 2009 application specifically calls for the development of a system that utilizes DPIs for network analysis and data extraction. More specifically, a multidimensional data extraction platform capable of characterizing user behaviors, monitoring and modeling the physical characteristics of data, and classifying languages. [38] China could field such a system for foreign SIGINT interceptions, monitoring and analysis.[39]

Geospatial Intelligence Systems

Throughout the 11th and 12th Five-Year periods, the 863 Program has been tasked with researching and developing projects related to Earth observation and navigation technologies. Within this R&D category, 863 grants are being awarded to develop cyber capabilities designed to support geospatial systems. Many of these cyber technologies can be used for both civilian space purposes as well as for the deployment, collection and analysis of geospatial C4ISR platforms and military systems.

The majority of cyber technologies being developed for geospatial projects concern navigation and positioning systems, remote sensing, and geographic information systems. Capabilities being funded by 863 to support these systems include high-performance parallel computing and debugging applications, heterogeneous data integration platforms, and highly advanced microelectronics.[40]

[36] Lin-Shan Lee, "Structural Features of Chinese Language - Why Chinese Spoken Language Processing is Special and Where We Are," Taiwan University and Academia Sinica, Accessed 27 July 2012, www.iis.sinica.edu.tw

[37] Duncan Green, "How Deep Pack Inspection Works," Wired Magazine, 27 April 2012, www.wired.co.uk

[38]"国家高技术研究发展计划（863计划）信息技术领域“新一代高可信网络”重大项目2009年度课题申请指南," 863计划, 2009

[39] Side Note: Huawei Technologies have been accused of utilizing similar systems to remotely intercept data - www.infosecisland.com/blogview/21681-Huawei-Boasts-of-Remote-Data-Interception-Capabilities.html

[40] 2012年度国家863计划地球观测与导航技术领域备选项目," 863计划, 2012, 2011年度国家863计划地球观测与导航技术领域备选项目," 863计划, 2011

In regards to microelectronics, the 863 Program emphasizes the R&D of reconfigurable circuits and radio frequency-field programmable gate arrays (RF-FPGAs). Since 2008, 863 has highlighted the importance of "enhancing [China's] wireless communication chips" for geospatial applications.[41] The Program has funded reprogrammable radio frequency circuits, data conversion circuits and signal conversion technologies. 863 applications assert that many of these technologies are being developed to support the second-generation Beidou satellite navigation systems. Although this is plausible, some of these electronics can also be fielded in other military and intelligence collection satellites.

A 2012 report concerning grants awarded to R&D GIS technologies reveals that China is currently funding the production of advanced remote data processing sensors, hyperspectral-imaging applications, and interoperable satellite communications systems.[42] The grant states that hyperspectral-imaging systems are to be used in satellites but stops short of saying whether the satellites are oriented for military or civilian purposes. If designed for geospatial C4ISR platforms, advanced space-based sensors can be used for terrain analysis as well as to automatically detect and identify a hidden target's radiation signature. Additionally, these sensors will provide the Chinese with the capability to detect what type of material a target is made of.[43] Even though the technical readiness level of the overall system is currently unverifiable, the fact that the Chinese are funding the production of working sensors reveals that the capability may be deployable by 2015.

863 Program grants are also funding the development of jam-resistant global positioning systems (GPS) capabilities for China's satellites. Since 2008, grant applications have sought "jam-resistant and block-resistant" multiband transceiver circuits for satellites.[44] Additionally, grants have funded R&D for noise elimination and suppression technologies used in radio-frequency integrated circuitry. The exact technical readiness levels for these technologies remains unknown, but it is possible to project how China may field such capabilities.[45]

The development and deployment of advanced block-resistant circuitry and transceivers reduces the vulnerability of China's military and commercial satellites to electronic jamming measures. Outside of geospatial systems, such technologies could potentially be fielded in highly advanced weapons systems that rely heavily on GPS (ex. smart bombs, drones, soldier's handheld GPS devices, etc.). By deploying these technologies the Chinese may be capable of effectively operating satellites and weapons systems even

[41]"国家高技术研究发展计划 (863 计划) 信息技术领域'面向软件无线电的宽带数据变换和可重构射频集成电路'重点项目申请指南," 863 计划, 2008

[42]"2012 年度国家 863 计划地球观测与导航技术领域备选项目," 863 计划, 2012

[43] Joe Pappalardo, "Hyperspectral Sensors: The Flying Eyes that See the Invisible," Popular Mechanics, 28 June 2011, www.popularmechanics.com

[44]"国家高技术研究发展计划(863 计划)信息技术领域'面向软件无线电的宽带数据变换和可重构射频集成电路'重点项目申请指南," 863 计划, 2008

[45] No information connected to these grants has since been published.

when they are under attack by hostile jammers.[46] As noted in this scenario, the 863 Program's R&D of cyber technologies have broad implications that reach far beyond C4ISR capabilities.

Asymmetrical Warfare & Cyber Capabilities

The 863's current cyber R&D projects have the potential to directly impact China's asymmetric warfare capabilities. Microelectronics, simulation modeling platforms, and a variety of software applications can be fielded in advanced military systems designed to increase China's power projection and anti-access capabilities.

Many of the technologies listed under the C4ISR section can also be fielded in both traditional and asymmetrical warfare systems. For example, hyperspectral imaging sensors can be used to detect the deployment of chemical warfare agents as well as in surveillance cameras on UAVs and targeting systems on signature detecting/guided air-to-air, air-to-ground and ground-to-air missiles. [47][48] China could potentially field these sensors for anti-ship ballistic missiles (ASBM) systems, which would strengthen the PLA's ability to detect, track and strike a moving warship.[49]

Outside of hypersectral sensors, 863 grants are funding the development of other technologies that can be used in ASBM systems. The Program has provided funding through 2014 for the development of 'fully functional' synthetic aperture radar (SAR) systems and support systems like high-resolution image processing applications and image matching software. [50] Broadly speaking, SAR capabilities will allow China to collect geospatial intelligence during inclement weather and nighttime.[51] Specifically for ASBM systems, if China can effectively field SAR applications they may be capable of producing "fire and forget" missiles that utilize automated target recognition software. [52] It is important to note that the 863 Program is not the only organization currently developing

[46] Robert Ackerman, "Jam-Proof Signals to Guide Navigation," Signal Magazine, November 2001, www.afcea.org

[47]Colin Lewis, "Chemical Agent Standoff Detection and Identification with a Hyperspectral Imagining Infrared Sensor," Optics and Photonics for Counterterrorism and Crime Fighting, 31 August 2009, www.spiedigitallibrary.org

[48] John Nella, "Hyperspectral Air-to-Air Missile Seeker," United States Patent and Trademark Office, Issue Date 27 June 2000, www.google.com/patents

[49] Jonathan Soloman, "Defending the Fleet from China's Anti-Ship Ballistic Missile: Naval Deception's Roles in Sea-Based Missile Defense," Georgetown University, 15 April 2011, www.georgetown.edu

[50]"地球观测与导航技术领域 "面向对象的高可信 SAR 处理系统" 主题项目申请指南," 国家高技术研究发展计划(863 计划), 20 October 2010

[51] "What is Synthetic Aperture Radar?," Sandia National Laboratories, 2005, www.sandia.gov

[52] Mark Stokes, "China's Evolving Conventional Strategic Strike Capability," Project 2049 Institute, 14 September 2009, www.project2049.net

SAR applications in China – the PLA GAD's Integrated Planning Department's Preliminary Research Bureau is also funding SAR R&D. [53]

Conclusions

Understanding how the 863 Program works reveals what cyber capabilities Chinese policy makers believe are of critical importance to the country. From the 2006 MLP through the 11th and 12th Five-Year Plans, China has utilized the 863 Program to R&D four key technological areas: advanced computing, networks and communications, virtual reality, and microelectronics. These are incredibly broad topics but through the analysis of what projects the 863 Program is funding in any given year, it is possible to identify which specific technologies China is most interested in developing. Additionally, grant applications reveal the technical readiness levels for high-priority systems like navigation and guidance chips, remote sensing platforms, and language analytics.

As China mobilizes and restructures its military to fight in asymmetric combat, the cyber R&D base will play a critical role in the development of C4ISR platforms and advanced weaponry. Following the 863 Program's openly distributed and classified military-specific grants reveal the deep scope of civil-military integration (CMI) within China's cyber R&D base. Dozens of universities, military organizations and intelligence ministries are all receiving funds to R&D dual-use cyber capabilities. CMI is rampant, constantly encouraged by high-ranking officials, and most importantly offering the PLA a springboard to advance military interests.

China is utilizing a clandestine funding system to bankroll the R&D of military-specific cyber capabilities in the civilian and industrial spheres. These capabilities have the potential to directly impact how China's intelligence ministries and the People's Liberation Army operate. As 863 projects administered from 2008-2010 become field-ready, China's C4ISR and weapons platforms will grow stronger and more robust.

[53] Mark Stokes, "China's Evolving Conventional Strategic Strike Capability," Project 2049 Institute, 14 September 2009, p. 10, www.project2049.net