STUDY OF INNOVATION AND TECHNOLOGY IN CHINA

RESEARCH BRIEF

2015-9 January 2015

The Human Capital Ecosystem Underlying the PLA's Network Weapons Development

Joe MCREYNOLDS, Leigh Ann RAGLAND, and Amy CHANG

Over the past two decades, China's military and political leaders have increasingly come to a consensus that the global web of computer and digital networks in the aggregate constitutes a distinct warfighting domainand the question of how to attain superiority in this new domain has become central to strategic thinking at all levels of the People's Liberation Army (PLA). Although China's network weapon development is highly secretive, researching the human dimensions of this process offers revealing insights. Over the past decade, the General Staff Department's 3rd and 4th Departments have built up a robust human talent ecosystem to support their network weapon development activities. This policy brief examines the personnel requirements of network weapons development and some of the key PLA institutes that appear to play key roles in human capital development in this area.

The Study of Innovation and Technology in China (SITC) is a project of the University of California Institute on Global Conflict and Cooperation. SITC Research Briefs provide analysis and recommendations based on the work of project participants. Author's views are their own.

This material is based upon work supported by, or in part by, the U.S. Army Research Laboratory and the U.S. Army Research Office through the Minerva Initiative under grant #W911NF-09-1-0081. Any opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect the views of the U.S. Army Research Office.

INTRODUCTION

Over the past two decades, China's military and political leaders have increasingly come to a consensus that the global web of computer and digital networks in the aggregate constitutes a distinct warfighting domain, the 'network domain,' a subcomponent of the broader 'information domain' that is roughly akin to the U.S. doctrinal concept of 'cyberspace.' Questions of how to attain superiority in this new domain have become central to the People's Liberation Army's (PLA) strategic thinking at all levels. In public speeches and writings, PLA operational commanders speak of dominance in the network domain as being essential to winning modern wars fought under informatized conditions.

Although China's network weapon development is highly secretive, researching the human dimensions of this process offers revealing insights. The PLA has built a robust human talent ecosystem in support of their network weapon development activities, integrating human capital from China's military, civilian, and private-sector information security and computer science communities into a comprehensive effort to develop network warfare capabilities that could one day challenge the United States' current supremacy in cyberspace. The PLA Information Engineering University (解放军信息工程大学, IEU) and PLA University of Foreign Languages (解放军外国语学院, UFL) under the General Staff Department's 3rd Department (总参谋部三部), as well as the GSD 4th Department's PLA Electronic Engineering Institute (解放军电子工程学院, EEI) appear to play key roles in this area.

The unique characteristics of this domain arguably make the human dimension far more central to understanding China's development of network warfare capabilities than is the case in traditional land, air, sea, and nuclear domains.

TYPES OF NETWORK WEAPONS AND ASSOCIATED PERSONNEL REQUIREMENTS

Although network weapons are almost kaleidoscopic in their potential variety, for the purposes of understanding the human side of their development they can be loosely grouped into three major categories based on the mix of human capital their development relies on.

The first consists of common technical penetrations of opposing systems via the exploitation of common vulnerabilities in the code of software and hardware discovered on those systems. Exploitation requires a moderate or greater level of technical ability to discover, depending on the particular vulnerability in question.

The second involves targeted attacks that require the adversary's personnel to take some unwitting action against their own interests, such as downloading an attachment or visiting a website. These attacks generally demand some level of linguistic and cultural intelligence support capability from the attacker in order to be carried out successfully. On a technical level, however, these attacks are often not as sophisticated, since the target's actions unwittingly inhibit their own technical defenses.

The third type includes a wide range of sophisticated attacks at the cutting edge of network warfare research. Depending on the specific attack vectors in question, the mix of human and technical capabilities required will vary. Their only common denominator is that such attack vectors rely on extensive technical research by scientific professionals to uncover. Such 'trump card' attack methods are relatively likely to be held in reserve in case of a significant conflict, as opposed to deployment in peacetime for espionage purposes.

With regard to China's human ecosystem for network weapons development, the more advanced technical and scientific training that personnel in the PLA General Staff Department's 3rd or 4th Department receive, the greater the likelihood that they are involved with the third type of network weapon development rather than the first or second type. Conversely, the relative usefulness of the first and second weapon types for China's unacknowledged peacetime computer network exploitation (CNE) activities places a greater emphasis on the discretion, consistency, and ideological reliability of the personnel involved in order to maintain operational security. Personnel affiliations with specialized General Staff Department (GSD) research institutes generally correlate with assignments to more sophisticated tasks, whereas Technical Reconnaissance Bureau (TRB) personnel tend to carry out lower-order tasks, such as modifying existing malware to better evade antivirus and intrusion detection software, in direct support of PLA operations.

THE PLA'S INTERNAL HUMAN CAPITAL ECOSYSTEM FOR NETWORK WEAPON DEVELOPMENT

Within the PLA, the development of network weapons appears to occur primarily within the GSD's 3rd and 4th Departments (3PLA and 4PLA), as well as their various subordinate organizations. The latter include IEU, 3PLA Technical Reconnaissance Bureaus (技术侦察局), and EEI, as well as various subordinate research institutes such as 4PLA's 54th Research Institute (总参四部第五十四研究所). PLA organizations outside of 3PLA and 4PLA, including defense technical schools such as the National University of Defense Technology (国防科学技术大学, NUDT), also take a technical development role, and foreign language talent is primarily drawn from UFL when needed.

Since the primary avenue through which 3PLA and 4PLA cultivate their specialized human capi-

tal is their defense technical schools such as IEU and EEI, this brief examines the academic tracks, incentive structures, and recruiting policies of defense technical schools relevant to future network weapons personnel at the undergraduate and graduate levels.

Undergraduate programs are a focal point in the PLA's network weapons human capital ecosystem for a number of reasons. First, although undergraduates lack the technical knowledge of graduate students, their academic track assignments at this stage are a major determinant of their future careers within the PLA, including the crucial distinction of whether they proceed down a command/operational career track or a technical specialist career track. Second, through their relatively large numbers, graduates of these programs form the backbone of the PLA's network warfare workforce. Third, at the same time, researchers working toward or holding graduate degrees are disproportionately engaging in leading-edge network attack and defense research that holds long-term importance to the PLA. Finally, these institutions attract human capital from a number of sources. Increasingly, they are doing so not only from within the PLA, but also by attracting talent from the relevant civilian educational and commercial ecosystems at the graduate level.

As for what becomes of these personnel after they finish their studies, although definitive conclusions cannot be drawn based on the anecdotal sources publicly available, there is substantial evidence of relatively low morale within 3PLA's network warfare programs. Poor pay, social isolation, and drudgery are all cited as negative factors by TRB members. Technical-track TRB officers often possess some skill-sets valued in the IT industry, but their salaries are paltry in comparison to their private-sector counterparts. As a result, at times TRB members may search for side jobs in white-hat (professionals who engage only in legal activities) and grey-hat (hackers who engage in both legal and illegal activities) software development in order to augment their incomes, with some even turning to low-level criminal activity to enrich themselves.

For these reasons, 3PLA jobs appear to have developed a negative or undesirable image within the civilian technical education system whose human capital the PLA is trying to attract. Although the promise of a subsidized education ensures that the PLA will continue to produce an ample supply of new technical talent through its dedicated education pipelines, this sense of disadvantage and dissatisfaction may pose longer-term retention challenges for 3PLA's network weapon development programs, since its officers do possess skill-sets valued in the private sector.

THE PLA'S INTERACTIONS WITH THE CIVILIAN HUMAN CAPITAL ECOSYSTEM FOR NETWORK WEAPON DEVELOPMENT

Over the past decade, the PLA has increasingly shifted the center of gravity of its human talent pipeline for network weapons development toward formally integrating civilian human capital on a number of levels, including research and training collaboration with civilian companies and universities, network warfare academic competitions that aim to identify new talent, and initiatives such as the National Defense Student program that aim to attract top civilian technical talent into the PLA.

One of the most important avenues for 3PLA and 4PLA recruitment through civilian universities is the National Defense Student or *guofangsheng* (国防生) program. The program allows students at civilian universities to matriculate directly into the military, either by going on duty or entering a defense technical graduate program, and is a central part of a broader scheme by the PLA to select a much greater percentage of its officer corps from among civilian university graduates. However, recruitment from civilian universities is not limited to National Defense Students. 3PLA and 4PLA both actively recruit from the wider pool of civilian graduates of relevant technical programs, much as the Ministry of State Security has historically done. Senior researchers and leaders of military research institutes also interface directly with upcoming civilian talent by serving part-time as PhD advisors within information security and computer science departments at top civilian technical universities.

Nevertheless, China's best information security researchers generally have little interest in joining the PLA. In order to take fuller advantage of civilian talent beyond their recruiting pool, 3PLA and 4PLA have established procedures for contracting out research work to civilian entities, including not only universities but also companies in the IT and information security sectors. The scope of these commissioned projects explicitly includes research into network attack and defense technologies, and may serve as an important vehicle for utilizing civilian human capital in the service of network weapons creation. For universities, these guidelines also attempt to maximize the benefits the military accrues from tapping civilian human capital by emphasizing informal information sharing and knowledge transfer, such as through ad-hoc technical seminars and workshops, in addition to strict completion of project requirements. There appears to be significant competition between universities for these projects, with schools spending significant sums of money on preliminary research projects conducted in the hope of attracting the PLA's funding.

It appears that a variety of civilian corporations and individuals participate in the PLA's network weap-

ons development, whether by selling knowledge of exploits or developing tools for the PLA's use through channels such as the GSD's industry commissioned projects. However, other top white-hat Chinese information security researchers have said that they see significant disincentives to their firms taking on military projects. Although the PLA's network warfare research funding is often valuable to research programs at civilian universities, the sheer quantity of the military's in-house research into network attack and exploitation vectors has driven the price the government is willing to pay to external actors for 'zero-day' vulnerabilities and other exploits to unusual lows, at a time when white-hat private-sector 'bug bounty' programs from multinational corporations such as Microsoft are becoming increasingly generous in their awards.

Furthermore, whereas a civilian university may have many defense research projects going on simultaneously across a range of research and development spheres, a civilian company with no prior dealings with the PLA may see the high fixed costs of compliance with PLA technical standards and procurement practices, as well as the potential for damage to the company's reputation in international markets, as factors weighing against entering into a relationship with the military. Although it remains common for private-sector actors to cooperate with the PLA on these tasks, the best technical talent may increasingly look elsewhere.

Although there were pervasive rumors a decade or more ago within the Chinese information security community of collaboration between the hacker community and the PLA's network warfare units, such arrangements appear less prevalent today. The more talented and professional among the early generations of Chinese hackers have gone on to found professional information security consultancies and software development studios, which can and do contract with the PLA; however, the PLA's formal human talent pipeline for network weapon development and network warfare operations is now mature and robust enough that its constituent organizations have no need to rely on informal and unreliable irregulars. When such "lone wolf" actors still participate in this ecosystem, they appear to do so by proactively launching broad network penetration efforts and then attempting to sell any valuable information obtained to either the PLA or relevant Chinese commercial entities.

CONCLUSIONS

Over the past decade, the GSD's 3rd and 4th Departments have built up a robust human talent ecosystem in support of their network weapon development activities with the support of senior PLA and political leaders. This ecosystem integrates talent from a wide variety of sources and does not appear to be reliant on single points of failure. Although this is partially a reflection of the less capital- and infrastructure-intensive nature of network weapon development when compared to the creation of fighter aircraft or missile warheads, in the context of the PLA's ongoing struggles in modernizing its defense research, development, and acquisitions systems and defense industries it is nevertheless a considerable feat. At present the system seems to be gearing up for additional evolution, with defense technical schools such as IEU dramatically increasing their emphasis on attracting civilian technical talent to relevant graduate programs.

However, additional challenges remain. Retention of the PLA's network warfare workforce is likely to become an increasing problem, assuming that opportunities for IT and information security professionals in China's private sector continue to outstrip those offered by the military. Although the PLA can leverage private-sector talent to some extent in network weapon development, the massive scale of Chinese network domain espionage activities requires a more controlled, regularized workforce that can only be properly maintained "in house."

The next major human challenges for the PLA in this sphere will likely be related to morale and retention of specialized talent. As the PLA's network warfare apparatus has become more regularized and its members' level of professionalism and talent has increased, losses due to high turnover become increasingly costly wastes of the PLA's training and educational investment. Furthermore, beyond their technical talents, PLA officers involved in network warfare development possess important institutional memory regarding the PLA's targets—particularly the Western military-industrial-commercial-scientific complex—that cannot easily be replaced. It remains to be seen how the PLA will grapple with these challenges in the coming years.

Joe MCREYNOLDS is a research analyst at Defense Group Inc.

Leigh Ann RAGLAND is a research analyst at Defense Group Inc.

Amy CHANG is a research associate at the Center for a New American Security.