The Real Culprit – The PLA's Strategic Support Force

Yossef Bodansky

February 2020

Executive Summary

* The primary Chinese threat to Western computers and communications comes from the PLA's Strategic Support Force.

* Presently, the scope, breadth and depth of the penetration of, and spying on, all computer and communication networks by the PLA SSF is second only to these by the US NSA. The Chinese are catching up fast.

* The preeminence and reach of the PLA SSF should guide the EU's decision making regarding the selection of future 5G systems, technologies and software. The viable security threat does not emanate from one specific company.

* Hence, the ONLY way to mitigate the viable threats and still benefit from the huge potential of 5G technologies is to build sophisticated security centers that will thoroughly check and certify all systems irrespective of labels and origin. Technologies and systems for effective and reliable security testing and validation of 5G systems have been developed in the US, Europe and Israel.

About ISPSW

The Institute for Strategic, Political, Security and Economic Consultancy (ISPSW) is a private institute for research and consultancy. The ISPSW is an objective, task-oriented and politically non-partisan institute.

In the increasingly complex international environment of globalized economic processes and worldwide political, ecological, social and cultural change, which occasions both major opportunities and risks, decision-makers in the economic and political arena depend more than ever before on the advice of highly qualified experts.

ISPSW offers a range of services, including strategic analyses, security consultancy, executive coaching and intercultural competency. ISPSW publications examine a wide range of topics connected with politics, the economy, international relations, and security/ defense. ISPSW network experts have held – in some cases for decades – executive positions and dispose over a wide range of experience in their respective fields of expertise.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Analysis

On 30 December 2019, the PLA celebrated the fourth anniversary of its newest branch - the Strategic Support Force (SSF).[1] The PLA SSF is equal in institutional hierarchy to the likes of the PLA Rocket Force, PLA Air Force, and PLA Navy. The SSF was officially established in late 2015. During 2019, the profile of the SSF rose prominently in Beijing. For the first time, a large contingent of SSF troops marched in the PLA's great parade on 1 October, wearing uniforms of ground troops, navy personnel and air force troops, along with a large variety of combat vehicles with diverse electronic warfare systems. On 12 December, the recently appointed Commander of the PLA Strategic Support Force Li Fengbiao was promoted by Xi Jinping to the rank of full General (4 stars) as part of the start of Xi Jinping's modernizing and streamlining of the Chinese High Command.

The PLA SSF is responsible for both the Chinese space operations, including space warfare, and the wide and not clearly defined electronic/cyber operations (including information operations). A primary mission of the SSF is providing the Forbidden City with strategic intelligence from all-source technical means - from satellites to hacking. The analysis and delivery of the collected intelligence is done through the Intelligence Bureau within the PLA's Joint Staff Department that controls the country's most leading think tanks and research institutions who conduct the pertinent analysis and make policy recommendations. It was the marked expansion in the SSF's electronic/cyber operations that brought the praise and high-profile during 2019.

Back in December 1929, during the Gutian Conference (that received immense political attention stressing its clairvoyance and enduring relevance in December 2019), Mao Zedong asserted that "the Chinese Red Army is an armed body for carrying out the political tasks of the revolution" in order to "establish revolutionary political power." Implementation is undertaken in the context of the "Three Warfares" - the broad umbrella definition of political warfare. The first of the "Three Warfares" is the struggle for influencing media and public opinion; the second is influencing foreign decision-makers and their China policies; and the third is shaping the legal context of Chinese actions and intentions. More recently, the PLA embraced the "Unrestricted War" concept, introduced in early 1999, that includes wreaking havoc on the Internet among the instruments and methods of "semi-warfare, quasi-warfare, and sub-warfare, that is, the embryonic form of another kind of warfare." Presently, the PLA SSF is the combat arm most adapt for the conduct of the non-kinetic elements of the "Three Warfares" and "Unrestricted War" concepts.

*

The PLA Strategic Support Force was established in the second half of 2015 as an outcome of the 2013 decision on the profound reforming and modernization of the PLA in order to meet the challenges of future warfare particularly against the US and its allies. The SSF is defined as a "new-type combat force" that is responsible for addressing all challenges emanating from the emerging "strategic frontiers" - space, cyberspace, and the electromagnetic domain - as well as conduct and/or support the conduct of wartime operations in these domains. The SSF was created by merging and markedly expanding the pertinent units of the PLA and a few intelligence and counter-intelligence elements. It was declared operational by the end of the year.

[1] For general background on the PLA SSF and their wartime roles see (1) Elsa B. Kania and John K. Costello, The Strategic Support Force and the Future of Chinese Information Operations, *The Cyber Defense Review*, Spring 2018; (2) John Costello and Joe McReynolds, *China's Strategic Support Force: A Force for a New Era*, China Strategic Perspectives No. 13, Center for the Study of Chinese Military Affairs, Institute for National Strategic Studies, National Defense University Press, Washington, DC, October 2018; (3) Adam Ni and Bates Gill, The People's Liberation Army Strategic Support Force: Update 2019, *China Brief*, Volume 19, Issue 10, 29 May 2019, The Jamestown Foundation, Washington DC.

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de

Presently, the SSF in answerable directly to the Joint Operations Command (JOC) under the Central Military Commission (CMC) that is chaired and run by Xi Jinping. The raw data the SSF collects are analyzed by the Intelligence Bureau within the PLA's Joint Staff Department. For the conduct of their routine operations, the SSF also has direct links to specific departments of the Communist Party of China (CPC), the Ministry of State Security (MSS - that is, Chinese Intelligence), the National Cyberspace Administration of China, etc.

The SSF is divided into several administrative and managerial Departments such as political work, staff, logistics, etc. like all PLA units. Significantly, the SSF has its own security and counter-intelligence elements - a reflection of its unique importance and the assessment of the foreign threats arrayed against it. Operationally, the SSF has two main branches - the Space Systems Department and the Network Systems Department.

The SSF maintains dedicated regional branches at the five joint force Theater Commands and national-level elements of the Rocket Forces, the Air Force and the Navy, with distinct cyberspace command elements down to the Independent Operational Group (IOG) level in order to support combat operations particularly during major wars against sophisticated militaries. The main wartime information support missions include the following: centralizing collection and management of intelligence collected by technical means; providing strategic intelligence support to theater and IOG commands; enabling very long distance and power projection operations; supporting strategic defense in the space and nuclear domains; and enabling three-dimensional joint operations through the intelligence, communications and informatization domains.

The singular importance of the PLA SSF can also be gleaned from the background of the new commander Li Fengbiao who assumed command in spring 2019. He was promoted to General in late 2019 even though he had been promoted to Lieutenant General only in mid-2016. Li Fengbiao rose to prominence as the commander of the 15th Airborne Corps (2011-2014) - the CMC's quick reaction "Fire Brigade" that is supposed to deal with, that is, crack down swiftly and ruthlessly, any domestic disturbances and insurrections before they become widespread and threatening, as well, spearhead special operations and military interventions worldwide. The latter is a role they now share with the SSF (that provides intelligence and communications preparations). Hence, the selection of Li Fengbiao to command the expanding SSF and his fast track promotion reflect the great trust by Xi Jinping and the CMC, and their conviction that such a stalwart is needed in this sensitive position in these tumultuous times.

*

The Network Systems Department of the Strategic Support Force - that is the PRC's Cyberspace Force - was organized by the transfer from the General Staff Department of both operational units and research institutes.

The key elements of the Network Systems Department are:

1. The former 3PLA with their twelve distinct Bureaus. This is the PLA's preeminent centralized collector of all electronic intelligence - including hacking of other people's computer systems and communications networks. The 3PLA has its own research institutes (mainly the 56th, 57th and 58th RIs) that were also transferred to the SSF.
2. The former 4PLA that is responsible for all forms of electronic warfare - both defensive and offensive. The 4PLA has its own research institutes (mainly the 54th RI) that were also transferred to the SSF.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

3. The Information Engineering University that trains the future officers, scientists and experts, as well as oversees all basic research pertinent for the SSF throughout the PRC. This university controls and supervises more than a dozen highly specialized academies and research centers all over China that are subordinated to the Network Systems Department.

4. The 311 Base that is the PRC's primary agent for political warfare that is still closely affiliated with the Liaison Bureau within the Political Work Department. The 311 Base's tactical unit for information operations has been fully integrated into the SSF's Network Systems Department. Significantly, the 311 Base is a content creating unit. It's integration into the SSF reflects both the political reliability of the SSF and Beijing's cognizance of the great pace of information activities and the imperative for swift capitalization on opportunities and swift reaction to moves by others.

Although the SSF's Network Systems Department is prepared for crucial roles in wartime - the unique importance of their routine operations is stressed as being optimized for the new trend the PLA identifies as "peacetime-wartime integration". Indeed, the routine status of the SSF is defined as "perpetual mobilization" - denoting constant operations such as the collection and analysis of strategic intelligence. In this context, the primary mission-role of the Network Systems Department is defined as "Network Reconnaissance" - that is, mapping computer networks and their communication nodes, as well as retrieving, collecting and analyzing information found in them and in associated computers and data collections.

By the time of their incorporation into the SSF's Network Systems Department, the 3PLA was already responsible for the bulk of the PLA's cyber espionage operations and forces. The 3PLA was also known as the GSD's Third Department. The 3PLA's cyber reconnaissance/intelligence missions were largely handled by its 12 Technical Reconnaissance Bureaus. These Bureaus were, and still are, responsible for the PRC's wide variety of cyber espionage and signals intelligence. Significantly, one of the main components of the 3PLA was the Shanghai-based Second Bureau that was a vastly expanded reincarnation of Unit 61398 - the main hacking arm of the PLA. Also of note was the Shanghai-based Twelfth Bureau that was a vastly expanded reincarnation of Unit 61486 - another cyber espionage and hacking unit specializing in targeted economic espionage aimed to enable the PRC gain technological advantages. The 3PLA's Second and Twelfth Bureaus were fully integrated into the SSF and have since been markedly expanded and improved, and given greater hacking and spying authority over computers, the Internet and telecommunications.

Ultimately, the quintessential impact of the integration of the 3PLA operations under the SSF's Network Systems Department has been establishing a centralized effort under strict military control. The hacking and cyber espionage units receive their specific tasks and priorities solely from the very top - Xi Jinping's CMC via the JOC - in accordance with the national-level decisions made in the Forbidden City. These can be spying on foreign governments and institutions, and/or acquiring sensitive technologies and know-how. Because of the sensitivities - both security and political - of this all-out effort, the highest echelons of the CMC resolved to place the endeavor within the confines of a single military entity and not involve outside entities such as academic institutions and commercial companies - be they private or SOEs. There are unconfirmed reports that this effort is called the Third Department of the SSF's Network Systems Department in reference to the erstwhile 3PLA.

The only interaction with the Chinese industrial mammoth happens if there is a need to plant specialized components inside pieces of equipment produced in China. Toward this end, the SSF has special channels through the CPC and the MSS to provide the PLA SSF experts safe access to the government-controlled production lines and personnel. Presently, the best-known case is the surreptitious planting of tiny microchips

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

(the size of a grain of rice) on computer motherboards produced in China for Supermicro, a US company, and supplied to both sensitive government and corporate entities that was discovered a few years ago. Indeed, the US investigation of the Supermicro motherboards revealed that the actual design of the microchips originated with the PLA and that their insertion during the manufacturing process by SOE subcontractors was done by PLA operatives. This venue is taken because the workers in the production lines are answerable only to, and are tightly controlled by, party and state security cadres. Consequently, PLA operatives can infiltrate production lines without notifying, let alone seeking permission from, the owners. This is the case even when the huge production facilities are officially owned by manufacturing private companies, be they Chinese or foreign, as well as SOEs. These companies own the facilities and production lines - but not the people therein.

The extent of Beijing's awareness of, and apprehension from, the evolution of cyberspace espionage and hacking is best reflected in the recent drastic policies regarding the use of computers and software made for foreign companies even if they were produced in China. In fall 2019, Beijing ordered all government offices and public institutions to replace all their foreign equipment and software including Windows (even though there is a Beijing-approved Chinese version of Windows 10). Back in 2017, the Forbidden City ordered the PLA SSF to develop a purely Chinese operating system specifically in order to replace Windows and other Microsoft software because of the hacking and back-door threats Beijing was convinced had been integrated into the software by the US NSA. With the PLA's substitute software ready for use in mid-2019, Beijing ordered the quick replacement of some 20-to-30 million hardware units within three years at a pace of 30% in 2020, 50% in 2021, and the remaining 20% in 2022. Politically, this undertaking will only further escalate the unfolding technological decoupling and Cold War between the PRC and the US.

Presently, the scope, breadth and depth of the penetration of, and spying on, all computer and communication networks by the PLA SSF is second only to these by the US NSA. And the Chinese are catching up fast.

*

This grim reality - the preeminence and reach of the PLA SSF - should guide the EU's decision making regarding the selection of future 5G systems, technologies and software. The viable security threat does not emanate from one specific company - no matter how badly maligned by the Trump Administration. The security threats apply equally to all systems and/or components produced and assembled in China - no matter if for Chinese companies, for Scandinavian companies, or for anybody else. Banning or limiting one company or another will have zero impact on the real threat to European networks, computers and overall communications.

Leading security experts have long concluded that all electronic systems - large and small - should be considered potentially compromised, and not just by China. Indeed, it has long been the conviction of the UK GCHQ that everything (that was not thoroughly inspected) is "dirty" irrespective of where it was produced. The GCHQ has adamantly refused to point a finger at the PRC as the sole culprit. The working principle of the GCHQ is that 100% of all electronic systems - from industrial machines to laptops and mobile phones - "had been penetrated by third parties stealing information."

Hence, the ONLY way to mitigate the threats and still benefit from the huge potential of 5G technologies is to build sophisticated security centers that will thoroughly check and certify all systems irrespective of labels and origin. Technologies and systems for effective and reliable security testing and validation of 5G systems have been developed in the US, Europe and Israel. Once such security centers are established - there is no reason to exclude anybody from the European markets provided they are certified as secure. (Chinese vendors, by the

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

way, strongly support the establishment of such security centers because they know they cannot sell anything until they are certified to be secure. Ultimately, these vendors want to sell a lot of products to EU customers.)

Meanwhile, the US ire aimed at the Chinese company leading the introduction of 5G systems and technologies hides Washington's real motives. A new era is fast approaching - ushered in by 5G technologies - in which the ability of the NSA to decipher by "brute force" commercially-encrypted communications will be severely curtailed. Widespread use of 5G communications will allow both private and commercial networks to have effective end-to-end encryption - thus permitting individuals to have more control over their own data. The subsequent introduction of Quantum computers, communications and encryption will further augment and invigorate this trend. On 28 January, David P. Goldman predicted in the *Asia Times* that as result of this development, "screens will go dark at the National Security Agency in a couple of years, and the US will have little intelligence to share." This threat to the omnipotence of the NSA, rather than worries about the security of European computers and communications, seems to be the real reason behind the relentless campaign by the Trump White House.

***

Remarks: Opinions expressed in this contribution are those of the author.

Giesebrechtstr. 9
10629 Berlin
Germany
Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06
E-Mail: info@ispsw.de
Website: http://www.ispsw.de

About the Author of this Issue

Yossef Bodansky has been the Director of Research at the International Strategic Studies Association [ISSA], as well as a Senior Editor for the *Defense & Foreign Affairs* group of publications, since 1983. He was the Director of the Congressional Task Force on Terrorism and Unconventional Warfare at the U.S. House of Representatives between 1988 and 2004, and stayed on as a special adviser to Congress till January 2009. In the mid-1980s, he acted as a senior consultant for the U.S. Department of Defense and the Department of State.

He is the author of eleven books – including *Bin Laden: The Man Who Declared War on America* (*New York Times* No. 1 Bestseller & *Washington Post* No. 1 Bestseller)*, The Secret History of the Iraq War* (*New York Times* Best-seller & *Foreign Affairs Magazine* Bestseller), and *Chechen Jihad: Al Qaeda's Training Ground and the Next Wave of Terror* – and hundreds of articles, book chapters and Congressional reports.

Mr Bodansky is a Director at the Prague Society for International Cooperation, and serves on the Board of the Global Panel Foundation and several other institutions worldwide.

Yossef Bodansky

Giesebrechtstr. 9
10629 Berlin
Germany

Tel +49 (0)30 88 91 89 05
Fax +49 (0)30 88 91 89 06

E-Mail: info@ispsw.de
Website: http://www.ispsw.de