VIVEKANANDA INTERNATIONAL FOUNDATION

Occasional Paper
July 2013

# Chinese Intelligence : From a Party Outfit to Cyber Warriors

Ajit Doval, KC

# About The Author

**Ajit Doval** obtained his master's degree in Economics in 1967 obtaining first position in the University of Agra. He joined the Indian Police Service in 1968 and in 1972 was seconded to the Intelligence Bureau. During over three decades of his service with the Intelligence Bureau, he held many senior positions both within and outside the country including North-East, Sikkim, Punjab, J&K, Pakistan, U.K. etc. In the Headquarters, he headed IB's operation wing for long years and was founder Chairman of the Multi Agency Centre and Joint Task Force on Intelligence. He retired as Director Intelligence Bureau in 2005.

A recipient of Kirti Chakra, one of the highest Defence gallantry awards of the country, Shri Doval was also country's youngest officer to be awarded prestigious Indian Police Medal for Meritorious Service at the age of 29, a record that he still holds. A graduate of National Defence College, Shri Doval was elected President of the International Association of Chiefs of the Police for Asia and Pacific region in 2004.

He is presently Director of the Vivekananda International Foundation, a New Delhi based independent Think Tank and research centre.

 

# Chinese Intelligence : From a Party Outfit to Cyber Warriors

Whatever yardstick we choose to apply – size of the economy and its rate of growth, military hardware and pace of modernisation, stability of the polity and the government; size, population and geo-political setting – China qualifies for a major power status. If we decide to be more candid than correct in making a hard headed assessment, its rise is not an assured peaceful rise. Its military build up, maritime ambitions, territorial claims, assertions in the cyber world and space etc have definite security ramifications both for the region and the world at large. The direction, intensity and form of these assertions among other things will be determined by China's self view of its interests, capacities and limitations on one hand and assessment of global response to its actions on the other. In making these policy choices, the intelligence capability of the Chinese state will play a seminal role.

No one has internalised, more than the Chinese, the fact that strategic strength of a nation is directly proportionate to its knowledge dominance. Three millennium back, they believed in Sun Tzu's dictum, 'Know thy self, know thy enemy - a thousand battles, a thousand victories', and they continue to believe it till date. While advances made by China in its economy, military modernisation, defence production and technology acquisition have been intensely studied and analysed, not much is known or written about its intelligence apparatus, its capabilities and vulnerabilities, role in policy making, systems and structures etc. Though China, compared to the past, has opened up in certain fields, its intelligence apparatus, not much understood by intelligence experts and scholars, remains a dark area. It assumes special import in the wake of its acquiring major power status on one hand, and expanding scope of clausewitzian doctrine of "War through other means" like cyber war on the other. It becomes all the more relevant in the Chinese context, as espionage has been integral to its strategic tradition and state craft.

 

## Evolution:

The history of Chinese intelligence is as old as that of the early warring kingdoms of ancient China. In terms of its antiquity, it can be compared only with the history of Indian intelligence that dates back to about 700 BC, perfected by Chanakya during the Mauryan Empire (322 to 185 BC); the only difference being that while the Indians proclaimed 'resorting to secret craft by the state' as unethical and immoral after the Gupta period (320 AD to 600 AD), it remained an uninterrupted part of Chinese state craft. Intelligence played a seminal role in the efforts of successive Chinese dynasties to deal with their external enemies – primarily the warring nomadic tribes- as also tackling internal threats.

In recent history, Sun Yat-sen and Chiang Kai-shek extensively used their spy networks to gather information about the Manchus that led to fall of the Qing dynasty. Intelligence also played an important role during the Sino-Japanese war and later the Civil War that led to the victory of the Chinese Communist Party (CCP) over the Kuomintang. Mao, during this extended civil war, heavily relied on CCP's secret apparatus and covert actions to subdue his political opponents. It is significant that one of the first resolutions adopted by the Politburo of the Chinese Communist Party (CCP), after the creation of People's Republic of China (PRC) in 1949, pertained to the crucial role played by the intelligence.

## Establishment of Communist Rule to Cultural Revolution:

On assuming power, three factors defined CCP's approach towards national security and concurrently the intelligence build up. First was a strong belief that all those who were opposed to the Communist ideology were counter revolutionaries and thus enemies of the Chinese state and the people. Second was an inherent distrust of all foreigners and foreign powers, particularly the Western democracies, who were perceived to be conspiring to undo the socialist revolution. Taiwan and Hong Kong were considered to be bases of their covert activity. Third was a fierce undercurrent of

 

Chinese nationalism that emphasised on avenging 'wrongs of history' and transforming China into a State with high Comprehensive National Power (CNP).

In terms of action points, at the intelligence front, this approach, inter alia, manifested into (i) Creation of a strong security state- policing its citizens, identifying ideological enemies and their neutralisation; (ii) denying access to suspected foreign agents; (iii) penetration into claimed areas of Chinese territory not fully under its control like Tibet, Taiwan, Hong Kong etc. (often referred as homeland territory by the Chinese); (iv) accessing scientific and technical information, mainly from Western sources, to build indigenous military and civilian capacities and (v) leveraging Chinese diasporas abroad for intelligence and counter-intelligence activities, including coverage of activities of anti-communist elements abroad. As the CCP was envisaged to play the central role in this secret activity, intelligence apparatus continued to be controlled by it, albeit with some structural changes. The erstwhile intelligence outfit, Public Security Department (PSD), was re-organised. Its internal security tasks were partly entrusted to the Central Ministry of Public Security (MPS) headed by Gen Luo Ruiqing, foreign intelligence was brought under Liaison Department headed by Li Kenong and some sections were transferred to People Liberation Army's (PLA's) Central General Office and the General Staff Department. Li Kenong was also designated by Mao as Secretary of the Central Committee's Intelligence Commission, Director of the Central Military Commission, Intelligence Department, as also as the country's Deputy Foreign Minister. Central Investigation Department, a field intelligence outfit, worked under Li Kenong.

At this stage, Chinese intelligence had limited exposure to the outside world, confronted problems of access and language and faced a generally hostile anti-communist environment internationally. These factors, abetted by ideological proximity to the USSR made the intelligence apparatus considerably dependent on the Soviets, particularly for external intelligence. KGB, in those days, worked closely with Gen Luo Ruiqing and helped him develop intelligence systems, doctrines, trade craft, training etc., whose footprints can be observed even today. Russians also helped the Chinese develop liaison arrangements with fraternal communist parties through

 

'International Liaison of the Chinese Communist Party'. The intelligence bonhomie with Soviets, however, started cooling off in the mid fifties and by 1960 the operational cooperation almost ceased to exist.

During the 1950s, almost every Chinese embassy had an Investigation and Research Office – a cover name for intelligence staff belonging to the Central Investigation Department. These were the field units for intelligence collection which were low in trade craft, highly secretive in their functioning and comprised of ideologically committed members. One of their major pre-occupation was to keep close watch on other members of the mission. They often remained present during the meetings with their diplomatic counterparts. In the headquarters, the analytical task was carried out by Central Investigation Department's Eighth Bureau, publicly known since 1978 as the "Institute of Contemporary International Relations."

In 1962, just before the Cultural Revolution, Li Kenong died and was succeeded by Luo Qingchang. The legendary Kang Sheng, a confidant of Mao who for long years had headed the Central Department of Social Affairs and in 60s was a member of the Politburo, was entrusted with the overarching responsibility of 'guiding' the country's intelligence apparatus. The infamous Kang Sheng played a vital role during Cultural Revolution in suppressing and neutralising Mao's political enemies. The political confusion that prevailed during Cultural Revolution created serious fissures with the intelligence community also. Reportedly, on the initiative of Lin Biao, the Central Investigation Department was abolished, most of its senior officers shunted to the countryside for re-education and its operators and human assets, both within and outside the country, deputed to the PLA General Staff Second Department. It is suspected that there was an internal conspiracy, in which some intelligence operators of the dissolved Central Investigation Department were used, that led to mysterious death of Lin Biao in 1971 in a plane crash in Mongolia. Following his death, the department was re-established and its representatives sent to missions abroad.

 

## Cultural Revolution:

The role of intelligence in the internal polity of China during the Cultural Revolution (1966-1976), that witnessed millions of killings, deserves a special mention. The revolution created conditions of anarchy and uncertainty, and saw sharp degradation of civil society and violation of human rights. There was extensive abuse of secret police and intelligence services that were responsible for large number of killings of political opponents. The secret apparatus became not only the perpetrator of atrocities but also a victim of it. In April 1967, Secretary General of the Central Investigation Department, Zou Dapeng, committed suicide along with his wife, who herself was a senior intelligence officer. A large number of intelligence operatives were dubbed as renegades or traitors and punished - often for their suspected pre 1949 roles or proclivities. Ironically, these persecutions were spearheaded by none other than the intelligence Tzar, Kang Sheng, who himself was head of the CCP's Intelligence and secret apparatus from 1939-1946. In those turbulent years, Kang, the hatchet man of Mao Zedong, headed the Central Case Examination Group (CCEG) that dealt exclusively in secret coercive practices and dirty tricks to bring about 'cultural' cleansing. At one point of time, at his behest, 88 members/alternate members of the party Central Committee were under investigation for suspected 'treachery', 'spying' or 'collusion with the enemy'. Kang Sheng used his infamous apparatus to crush Mao's ideological opponents dubbing them as enemies of the revolution. The powerful role of Kang and his security services in China's internal power play can be gauged by the fact that Kang Sheng was directed by Mao to supervise drafting of the new Party Constitution, which was adopted at the Ninth Congress in April 1969. He was also 'elected' as one of the five members of the Politburo Standing Committee, along with Mao, Lin Biao, Zhou Enlai and Chen Boda.

## Ministry of Social Security (MSS):

The political developments in China consequent to the death of Mao Zedong (1976), fall of the Gang of Four (1976) and rise of Den Xiaoping heralded a new era in

 

Chinese politics. Following the Third Plenum of the 11th Central Committee Congress, Deng Xiaoping emerged as the most powerful leader and gave a new fillip to the pace of modernisation and structural reforms. Himself a victim of political misuse of intelligence during Cultural Revolution, he wanted to re-structure the intelligence apparatus making it less susceptible to political vagaries. He resurrected the Chinese traditional concepts of Shishi Qiushi (seeking truth from facts), 'Xianzhi' (foreknowledge) and 'Hide Your Strength, Bide Your Time' as some of the guiding doctrines to reform the country's intelligence set-up. He wanted Chinese intelligence to be transformed into a modern professional outfit – in tandem with China's four modernisation programmes - having high technical capabilities and insulated from day to day party control. Deng Xiaoping was also not in favour of intelligence officers using legal cover as diplomats and wanted them to operate under illegal covers like media persons, representatives of business firms, scientists and researchers in universities etc.

Many piecemeal reforms were brought about during 1976 to 1982 that eventually culminated in the formation of the Ministry of Social Security (MSS) in 1983. It was envisaged to be the country's apex intelligence outfit, a position that it continues to hold till today. A formal proposal was initiated by Liu Fuzhi, who at that time headed the Ministry of Public Security (MPS) and was approved by the Political Bureau of the CCP Central Committee. The new outfit that defined its charter as "the security of the state through effective measures against enemy agents, spies and counter-revolutionary activities designed to sabotage or overthrow China's socialist system"[1] was made answerable to the Premier and the State Council. The above charter defined by Liu Fuzhi, however, hid more than it revealed. Unstated, the primary functions of the MSS included collection of foreign intelligence and undertaking covert intelligence operations both within and outside the country. It had a major internal intelligence charter as well. Ling Yun was appointed its first Chief, who on assuming office proclaimed that intelligence would no longer be used to settle ideological differences or allow party barons to use the service to settle factional fights. It was, however, nothing more than a pious wish and propaganda ploy.

 

Major segments of the intelligence and counter-intelligence activities of the Ministry of Public Security (MPS) and remnants of the Chinese Communist Party's Investigation Division under Central Department of Social Affairs (CDSA) were merged into the new outfit. For the first time, foreign intelligence was collected, collated and analysed in a systematic manner on modern lines. As MSS did not have a body of experienced analysts to interpret the data, China Institute of Contemporary International Relations (CICIR), which had existed since 1980 and had a professional research staff, was brought under its control. The organisation, though has an open profile, is a feeder outfit that provides MSS with intelligence assessments based on inputs received from all sources including open sources and interaction with foreign think-tanks. It is a conglomerate of eleven institutes and two research divisions specialising in diverse areas of international interest to China. According to some press reports, "the CICIR has provided intelligence collection support to the MSS and the Foreign Affairs Leading Group (FALG), the Communist Party of China's top foreign-policy body.[2]"

The MSS over the years has emerged as China's largest and most effective intelligence organisation, working under the state council with its headquarters in Beijing. Under Article 4 of the Chinese Criminal Procedure Law, it enjoys police powers to arrest and initiate prosecution in cases involving national security. It has different wings covering foreign intelligence, internal intelligence, counter-espionage and counter-intelligence. There is a certain degree of overlap with the Second Department of the People's Liberation Army (PLA) in respect of foreign intelligence and Ministry of Public Security (MPS) in the field of domestic intelligence.

## Ministry of Public Security (MPS):

Though essentially a national security agency, the Ministry of Public Security (MPS) has a wide intelligence network. Enjoying overriding powers over the police and law enforcing agencies, huge resources and proximity to the CCP makes it a powerful security cum intelligence outfit.

 

In its intelligence gathering and operational role, it keeps a close watch on internal political developments and concurrently reports to the State Council (executive component of the state) and Central Political and Legislative Affairs Committee (party apparatus). Besides collection of intelligence through police organisation at provincial and local levels, MPS performs its intelligence functions using 'working units' of the 'Chinese citizens'. MPS is empowered to draft any citizen to spy over fellow citizens or foreigners living in their area. Surveillance over visiting foreigners is an important function of the MPS which it performs through local law enforcement units besides its dedicated intelligence units. However, deficient in skills, experience and equipment, its trade craft is primitive and crude and easily detectable.

While the intricate network of MPS informers allows the system to keep a close watch on its citizenry, it often leads to erroneous or disproportionate police actions on account of perfunctory reporting, informers settling personal scores through false reporting and intervention by party bosses. Some of the problems encountered by MPS include managing the unwieldy data generated by diverse working groups spread throughout the country, validation and analysis of data, delayed real time flow of information among the provinces and from provinces to the MPS headquarters in Beijing and lack of coordinated decision making process due to two parallel masters - the state executive and the party apparatus. Intervention by the Central Political and Legislative Affairs Committee, that is supposed to deal with coordination problems, often proves to be delayed and non-workable.

As custodian of ideological security, the MPS also performs an important political role of monitoring political opinions of the people, logging people's grievances and collecting information about rivalries among the party cadres/leaders. To assist its political role, it maintains a massive national database covering personal information from national to local levels. The inputs are derived from police reports, inputs of working groups, local level party sources, interception of e-mails and telephonic communications, employment records, data available with banks and industrial concerns, prosecution and immigration records etc. This data is integrated and

 

aggregated to identify 'persons of interest' which in turn are sent to police stations for stipulated action.

Internally, China has created intelligence capacities for a panoptic state where it can identify, monitor, control, intervene and, when required, coerce citizens to submission for furthering perceived national interests. This trend got further strengthened after the Tiananmen Square massacre in 1989, that badly shook China and whose after effects continue to haunt it. Growing unrest in Tibet and Xinjiang and the spate of suicides in Tibet have further unnerved China. The declining face of economic growth, unemployment and exponential rise in agitations and protests have further compounded the internal security landscape.

In 2011, Zhou Yongkang, China's senior party leader in charge of security and stability, emphasised the need of integrating MPS intelligence system for "social management" that would include monitoring political views, moulding public opinion and propaganda to shape people's decision. In furtherance of this policy in December 2011, MPS directed units under it to visit villages and houses to win over their hearts and minds on the one hand and monitor their opinions on the other. This is illustrative of the Chinese management of state affairs intricately intertwining security, development, political and civil society controls. Though it has not drawn the attention of strategic analysts abroad, in last one decade, both the size and influence of MPS has increased substantially. However, to what degree the MPS influences political decision making process and policy formulation needs further investigation.

## Military Intelligence – 2nd General Staff Department (2nd GSD):

The powerful Chinese military apparatus has dedicated intelligence apparatus of its own under the General Staff Department (GSD) of the PLA. Second Intelligence Department (2nd GSD) is one of the most important departments of the military intelligence setup. It is headed by a Director who is assisted by two Deputy Directors and a Political Commissioner. The Director and Political Commissar are equivalent to a Group Army Commander. [3] As it works directly under the General Staff, political

control over it is lesser than in the case of MPS and MSS. STRATFOR, a leading intelligence research organization, avers that border intelligence is one of the primary responsibilities of the MID in which it is assisted by the PLA's reconnaissance units. [4] Specializing in tactical intelligence, it keeps tab of the order of battle (ORBAT) of foreign armies, their doctrines, strategies, location, identity of field formations and profiles of their commanders etc. Its responsibilities include terrain assessment of target areas of military interest, identification of military command and control centres, plotting vulnerable Areas/Points (VA/VPs), equipment profile, counter-intelligence tasks, etc. It also monitors the activities of foreign armies operating in the Asian continent.[5]

Some of the important wings of the 2nd GSD include (i) 'Department 2' collecting information through human assets (HUMINT) with seven bureaus working under it, (ii) 'Department 3' collecting intelligence through communication interceptions (SIGINT) located in seven of its military regions and (iii) Department 4 specializing in battle field Electronic Intelligence. Electronic intelligence is sourced through Electronic Warfare (EW) Regiment/Reconnaissance Units functioning at the Group Army (GA) level. Other departments deal with administration, logistics, training etc.

The 2nd GSD's field formations have Military Reconnaissance Units (MRs) in border areas, Intelligence Analysis Centre at the Divisional level and Intelligence Peace Units at Company levels. During war time, the Intelligence Analysis Centers function at the Battalion Headquarter level also with a limited remit. It also monitors the activities of foreign armies operating in the Asian continent. Earlier the 2nd GSD primarily focused on human intelligence and traditional military intelligence activities but has recently expanded the range of its activities to cover scientific and technological information.[6] [7]

The 2nd Department is further sub-divided in functional bureaus such as Military Intelligence Bureau, Tactical Reconnaissance Bureau, Political Bureau, Confidential Bureau, Comprehensive Bureau and Confidential File Bureau. [8] Military Intelligence Bureau focuses mainly on Taiwan, Macau and Hong Kong; collects technical

intelligence to improve and develop military hardware for the PLA and establishes contact with potential clients for weapons exports concealing PLA's direct involvement in arms trade. The Tactical Reconnaissance Bureau streamlines the information flow from specialized units at the MR level. The 3rd Bureau (Military Attaché Bureau) screens and debriefs military attaches who are deputed to foreign missions abroad. The 4th Bureau's responsibility is Intelligence analysis for Russia, former Soviet republics, and other East European countries. The 5th Bureau is also known as the Foreign Affairs Bureau. Its responsibilities include organizing foreign visits of PLA officers, military exchanges and receiving foreign military visitors. It, at times, works under the cover name of "the Ministry of National Defence Foreign Affairs Office". It has its work divided on territorial lines like America & Canada Bureau, Europe & Asia Bureau, etc. It is learnt that the Press Bureau, known as "Ministry of National Defence Press Affairs Office", also works in conjunction with 2nd GSD. Several PLA Universities and Command colleges are directly subordinate to the Foreign Affairs Bureau.[9] The 6th Bureau focuses on analysis of Intelligence pertaining to the neighbouring Asian countries. The 7th Bureau (Technology and Equipment Bureau) plans and carries out cyber espionage operations through six governmental research institutions and two computer centers. It also enlists the services of individual civilian hackers and uses companies that produce electronic equipment for carrying out its activities. In addition, the 2nd GSD oversees working of the Arms Control Bureau, Space Reconnaissance Bureau, Computer Institute, PLA College of International Relations.

## 3rd General Staff Department:

The 3rd GSD or the Technical Department primarily focuses on signal intelligence (SIGINT) operations of the PLA. In the American jargon, the quintessential SIGINT task is to carry out cyber surveillance or Computer Network Exploitation (CNE). Computer network operations (CNO) in China are often referred to as — "Network Attack and Defense", based on the premise that –"without understanding how to attack, one will not know how to defend". The 3rd Department's SIGINT targets are diplomatic missions, military activities, economic entities, public education

 

institutions, and individuals of interest. There may also be bureaus operating at the Military Districts for conducting network defense and attack, technical reconnaissance, and psychological operations. Bureau Directors and Political Commissars are equivalent in rank to an Army Major-General.[10]

## 4th General Staff Department:

The Electronic Countermeasures (ECM) and Radar Department, also known as the 4th GSD Department, is responsible for developing equipments, doctrines, and tactics for electronic warfare and information. Established in 1990, it maintains a data base of electronic and radar signatures of foreign armies. The department is headed by a Director and two Deputy Directors and has at least, four bureaus, one brigade, and two regiments. It is widely believed that an ECM Brigade is headquartered at Langfang in Hebei Province with subordinate battalion-level entities located in Anhui, Jiangxi and Shandong. Two units, including one with operational or experimental satellite jamming responsibilities, are located at Hainan Islands with the purpose of jamming US satellites. All PLA, PLAAF and PLAN Military Regions have one ECM Regiment. The 3rd and 4th General Staff Departments also operate a joint centre dedicated for network attack/ defense training system.

## General Political Department (GPD):

The GPD functions directly under the Central Military Commission (CMC). It oversees the discipline, political education and indoctrination of PLA personnel. It has an organisation called the China Association for International Friendly Contacts which infiltrates foreign armies in order to subvert loyalty of their personnel and propagate Chinese ideology among them to further their aim. The Political or the Liaison Department also conducts counter-espionage activities in foreign countries to keep a watch on its own intelligence operatives. The GPD maintains Liaison Departments at the Military Region (MR) level. The Department also oversees the Military Museum of the Chinese People's Revolution, Liberation Army Daily, the PLA Literature and Art Press (Kunlun Press), PLA Pictorial, and PLA Press.

 

# Human Intelligence:

The modus operandi of the Chinese intelligence is uniquely Chinese in its application characterised by Chinese cultural traits. As only few cases of Chinese intelligence operations are available for detailed study and analysis, it is generally presumed that Chinese intelligence trade craft is primitive and low in its reach. The famous case of Larry Wu-Tai Chin is indicative that even before People's Republic of China (PRC) came into existence, the CCP's intelligence setup had started recruiting deep penetration sources in target areas. Chin passed on classified information to China while working for the US intelligence community for over 35 years. He supplied a stream of high grade intelligence till his retirement in 1981. He was detected only in 1985 when his cover was blown by a defector leading to his suicide before being brought to trial. The trade craft used for intelligence collection, contacts between the source and handling officers, communications, briefing and debriefing etc. show a high degree of sophistication. The fact that Chin was able to operate undetected for 35 years also indicates high level of secrecy standards in protecting source identity.

The technique and methodology adopted by the Chinese operatives in respect of raising and handling human assets (intelligence sources) is slightly different from those employed by other modern intelligence agencies. Even after the initial 'ice breaking exercises', the handler remains vague and circumspect in specifying his needs and considerations in return. Emphasis is more on personal and friendly relations. Quite often, even when a human asset starts passing on information, he is not consciously aware of working as an intelligence agent. The trade craft used is elementary and the relationship between the handler and the source is nebulous and ill-defined. It is only after considerable period of time that the handler discloses his real intentions, requirements and identity; asking the agent to follow more rigorous trade craft for collection of classified information, fixing of RVs, communications etc. Despite the fact that during its formative years the Chinese intelligence operatives were trained by the KGB, who make a fetish of traditional trade craft, their cultural trait of being circumspect and employing symbols to communicate is discernible in their intelligence practices. Nigel Inkstar, in his 'Chinese Intelligence in the Cyber

 

Age', however, feels that "when the need arises, or when they are sure of their ground, Chinese intelligence officers can be very direct and explicit and capable of deploying sophisticated tradecraft".

Chinese are also known to effectively provide cover identities to its human assets using forged documents. The case of Liu Kang-Sheng, a MSS operative, who was caught using forged Thai and Singaporean passports is illustrative. Though passports of these countries have high security features, it was found that the forged documents were almost perfect in incorporating these features. It is obvious that Chinese intelligence has well developed facilities for forging documents.

Among the Chinese intelligence officers, there is a marked preference for people of Chinese ethnicity and those seen as friends of China for cultivation as human assets. However, this phenomenon is gradually undergoing a change. Valentin Danilov, a Russian physicist who headed the Thermo-Physics Centre at Krasnoyarsk State Technical University (KTSU) and had researched on effects of solar activity on space satellites is a case in point. In 2004, he was sentenced to 14 years imprisonment for passing on classified information to the Chinese. Similarly, Swedes uncovered diplomats in the Chinese embassy in Stockholm who recruited a Uyghur émigré to monitor the activities of Uyghurs in Europe. The case of US nationals Noshir Gowadia and Glenn Duffy Shriver are also illustrative of Chinese intelligence recruiting foreign nationals for espionage. Shriver was arrested for spying in June 2010 while flying to China. He pleaded guilty of unlawful communication of national defence information after a polygraph test and was imprisoned for four years. He had met his Chinese handlers about 20 times and received $70,000 for the services rendered. Gertz Bill reported in Washington Times on March 25, 2013 that "Shriver is not the first spy for the Chinese to target the CIA. U.S. intelligence sources have said at least three CIA officers who reported to Director George J. Tenet in 1999 as having spied for China, but were never caught. One of the agents was paid $60,000 by Beijing".

 

Chinese intelligence pursues its defined operational missions, once defined and approved, most doggedly unmindful of its cost-benefit ratio. Chinese efforts to go for outright purchase of a Stealth aircraft parts manufacturing company for obtaining the in-flight refuelling capability for its Air Force is a case in point. The attempt was foiled at the last moment. It resorts to all means, including most unethical practices to achieve its operational missions. The case of Da Chuang Zheng, a Chinese intelligence agent, who was caught while attempting to steal advanced radar and electronic surveillance technology to China is one among many such cases of heist.

The Chinese have mastered the technique of amalgamating disparate micro intelligence accessed from incongruous sources with no comparable gradations in respect of their authenticity and reliability. This technique of 'Thousand Grains' entails collecting small bits of information and then piecing them together to make intelligence sense. This has particularly been used for acquiring mid level technologies using inputs both from human and technical sources. Widely spread Chinese diasporas working in research and academic establishments, high technology using manufacturing concerns, business houses etc. are often utilised for the purpose. Potential targets are, at times, recruited during their visits to China. Another variation is collecting micro intelligence bits during participation in scientific cooperation programmes, seminars and conferences in foreign countries and visits of scientists under scholar overseas exchange programmes. FBI investigations in 1988 had revealed that the technology for neutron bomb detonated by China was not indigenously developed but acquired from Lawrence Livermore National Laboratories in California. Various Chinese delegations comprising ostensibly of scientists, but actually MSS intelligence operatives, visited the facility and were able to collect the required information in bits and pieces over a prolonged period of time.

Chinese intelligence closely monitors activities of political dissidents and groups both within and outside China, suspected foreign agents, visitors and scholars visiting China and members of diplomatic missions. Human assets are often placed in vantage positions to cover their activities. In June 1989, Shou Huaqiang, a delegate to the Chinese Alliance for Democracy Convention in California, an anti-China dissident

 

group, publically declared that he was an MSS agent sent to spy on the activities of the Alliance. He alleged that he was forced for the job by MSS officers who made him sign an agreement with instructions to disrupt its work.

## Cyber Intelligence:

When the rest of the world was busy celebrating the great strides in Information and Communication Technology (ICT) in the late eighties, the Chinese Strategic Community was busy evaluating its security implications. They realised that they could not allow the revolution in ICT bypass it, lest their modernisation programme come to a naught. At the same time, if allowed free access, it could not escape its concomitant adverse fallouts. The American military successes during the Gulf War during 1990s shook them and made them realise formidable capabilities of war machine supported by the informatics. Internally, in the wake of people's uprising culminating in Tiananmen Square massacre in 1989, there were apprehensions about internal security if people were allowed unchecked access to the outside world through internet. By 1996, the number of internet users in China had touched the figure of 2 million, which was fraught with danger. The 'bourgeoisie' influence through the internet posed a threat to the Chinese Communist Party's ongoing Patriotic Education Campaign launched in early nineties. These developments led China to embark on an ambitious programme of acquiring cyber dominance, both in offensive and defensive modes. It became evident by 2008 that Chinese intelligence had made remarkable strides in this direction on both fronts.

While there is no direct evidence to prove culpability of Chinese intelligence undertaking covert cyber intelligence operations abroad, there is ample circumstantial evidence to infer that. Besides reliable intelligence inputs, tracing large number of cyber attacks to servers in China, technological sophistication of cyber attacks, resources required to carry out the operations at global scale, selection of targets, type of information accessed and long history of Chinese intelligence for science and technology thefts strongly point towards state involvement.[11] Many instances of cyber attacks on countries like the US, Canada, Japan and India have been tracked to China.

 

There are strong pointers to infer that China is indulging in large scale cyber espionage using an army of hackers, drawn from military, intelligence, cyber professionals etc. As an intelligence activity, it has enabled China to penetrate classified domains of target countries to extract technological and systems information and collect military and security related information about programmes and activities of the countries on its intelligence radar. On the internal security front, it is being used to contain and counter liberal and democratic ideas of political dissidents. However, there is little information to assess China's ability to validate and analyse the colossal data collected by it both internally and externally.

The Gulf War, in addition to highlighting the potential of information and communication technology (ICT), also made the Chinese aware of the heavy dependence of Western military systems on these state of the art technologies and attendant vulnerabilities. They saw in it an opportunity of developing asymmetric capabilities which could defeat advanced technical capabilities through counter-electronic systems.

Col Ling Qiu and Col Wang Xiangusi in 1998 in their book 'Unrestricted Warfare' conceptualised how huge US combat superiority emanating from its IT edge could be transformed into their vulnerability. It was a doctrinal shift for preparing People's Liberation Army (PLA) to fight under informationised conditions. According to Nigel Inkster, "the PLA is pursuing a highly ambitious cyber-warfare agenda that aims to link all service branches via a common ICT platform capable of being accessed at multiple levels of command and has created three new departments of Informatisation, Strategic Planning and Training to bring this agenda into being."[12]

Though late to enter the internet domain, China took giant strides, both in development of hardware and software on one hand and training people on the other, that made up for the lost time. The first indications of Chinese capabilities started trickling in the early years of the last decade when hackers broke into US official networks to steal sensitive information which US investigators code-named as 'Titan Rain'. Nathan Thornburgh writing in the Time Magazine said that the targets included

 

US military establishments, NASA, the World Bank, etc Similar attempts were reported from United Kingdom, Germany and New Zealand during 2006-07 detailing cyber attacks that had emanated from China. Mandiant, an American firm dealing with information security, reported that PLA Unit 61398, one amongst many such units, was responsible for the cyber attacks on more than 140 companies the world over since 2006. In 2009, University of Toronto's Information Warfare Monitor Citizen came out with its so-called 'Ghost Net" report detailing intrusion by Chinese hackers into the network system of Indian security establishment and offices of Dalai Lama's secretariat.[13] Though rejected by the Chinese, it was a well researched and accessed professional report which concluded that the cyber operations were being conducted by the "2nd Bureau of the People's Liberation Army (PLA) General Staff Department's (GSD) 3rd Department".[14]

The Chinese have been systematically recruiting and training a pool of cyber professionals to undertake these tasks. In 2005, hacker competitions were held at the regional and provincial levels in China for hiring computer network operators. In 2007-08, the Ministry of Public Security (MPS), internal intelligence cum security outfit advertised job vacancies for hackers under the cover name of computer operators. According to a report in Asia Times of Feb 9, 2010, Chinese embassies were contacting Chinese IT graduates in different foreign universities purportedly for jobs in public security departments but essentially for computer network operations.[15]

China's cyber capabilities are not only confined to military combat needs, espionage and internal security. Economic and Technical intelligence, that have figured high in its national priorities, are also being served through cyber warfare. In target countries, computer networks containing classified data pertaining to trade secrets or denied technologies are being accessed. According to a report of the Office of National Counter Intelligence Executive submitted to US Congress in 2011, US networks were facing Chinese onslaught for trade information, communication technology, data pertaining to scarce natural resources and civilian technologies in energy and health sectors.[16] Accessing critical defence technologies is more alarming. A recent report published in the Washington Post points out that Chinese hackers have broken into

 

several defence production firms involved in the manufacturing of critical military hardware including the Patriot missile system, the Terminal High Altitude Area Defense, or THAAD, as also vital combat aircraft and ships like the F/A-18 fighter jet, the V-22 Osprey, the Black Hawk helicopter and the Navy's new Littoral Combat Ship. The report submitted to the Pentagon by the Defense Science Board underlines the enormity of the Chinese cyber-espionage activities and investment of effort to overcome the US military advantage.[17] One illustrative case is of US company AMSC, specializing in wind turbine manufacturing, having lost its centre software code to the Chinese hackers. This theft led to the company losing 80 % of its revenues. Similar was the experience of Nortel, Canadian Telecommunication giant that went into bankruptcy. Brian, its former security adviser in an interview to CBC on October 11, 2012 said that, "Huawei spent years hacking into Nortel's system and stealing information so it could compete with Nortel on world markets and added that, "These kind of things are not done just by average hackers. I believe these are nation state activities".[18] A disclosure was made by *Daily Mail* in March 2012 that Chinese hackers were able to find "full access" to NASA computers containing information about 13 spacecrafts. It is believed by experts that it helped the Chinese in their quest for outer space utilization programme. Similar evidence of Chinese efforts to beef up its cyber warfare capabilities came to light in 2011 when McAfee, an American cyber security company brought out its White Paper, code named 'Operation Shady Rat'. McAfee reported about the attacks, some of them raging for as long as five years targeting 70 government and private agencies in different parts of the world. Forty nine of these were US based networks while others were located in Taiwan, India, UK, South Korea, etc. Through these digital storms, the Chinese have also been undertaking 'Spear-Phishing' operations that involves sending innocuous e mails to targeted individuals, websites etc and to extract stored data from the computers. Through a detailed and carefully researched trade craft, high potential targets are selected, artificial identities created, and malware messages routed through multiple destinations that are often difficult to trace. A report brought out by the Northrop Grumman in 2009 geographically detailed the modus operandi used first to breach and then to 'exploit' [19]

 

Information about what is the cyber intelligence infrastructure, who controls it, how the key intelligence needs are identified, what is the co-ordination mechanism, how the data is validated and integrated to convert information into usable intelligence are still grey, if not black, areas. Going by the scale of activity and swathe of their operational targets, it presents a highly confusing picture. It is believed that 3/PLA has the highest technological capabilities at least to gain covert entry into targeted domains and access the data. However, except for information of military value, its capability to process other inputs are seriously doubted. The co-ordination mechanism available with the MSS also appears to be inadequate and while the relationship between MSS and MPS, uncomfortable though, is known to some extent, the working mechanism of 3/PLA with other intelligence outfits is a matter of speculation.

## Intelligence in Internal Security:

To make a holistic assessment of what the Chinese call Comprehensive National Power (CNP), it is essential to evaluate its internal stability and political dynamics and the role intelligence services play in this arena. It assumes special import as with the opening of China and its modernisation programme, the Chinese are finding it increasingly difficult to keep a lid over internal dissidence. Murray Scot Tanner in his 'Cracks in the Wall: China's Eroding Coercive State' as back as 2001, observed that, "Beijing's control over the coercive system, as well as that system's capacity to maintain social control appears to be slipping". Since then, the internal security landscape has further deteriorated. There have been well over one hundred thousand incidents of mass protests and agitations in 2012. Large scale visits of Chinese, particularly the students abroad, access to internet and mobile phones, activities of pro-democracy groups and economic affluence have raised the threshold of political awareness. The situation in Tibet has become precarious, particularly after the Olympic Games in 2008. Besides, a large number of protests and agitations, there have been over a hundred cases of self immolation by Tibetans since the Olympics. The rise of Islamic radicalism and violence in Xinjiang is another cause of serious concern. The Tiananmen Square massacre still looms large on the psyche of the people and have accentuated Chinese fears of internal destabilisation which they

attribute to conspiratorial counter-revolutionary forces propped up by external enemies. The anxiety was discernible when in the year 2011, the then Chinese Premier Wen Jiabao, in a public address, stated that *"*We have not yet fundamentally solved a number of issues that the masses feel strongly about*"*. The Jasmine Revolution in 2011 further shook the Chinese administration and they hiked their budget for internal security, reportedly, to $95 billion in 2011 and $111 billion in 2012. It is significant that notwithstanding China's massive military modernisation programme, the internal security budget ranks above the defence budget.

China's internal intelligence apparatus is much more complex and multilayered; with both the party and state having overlapping roles. Department one of MSS, the premier national intelligence agency, handles 'homeland security' while its department six and nine deal with 'counter espionage' and 'counter defection and counter surveillance' respectively.

## The Indian Experience:

The Indian experience of Chinese intelligence dates back to early fifties when its intelligence apparatus started operating in Tibet. It assisted both the CCP and the PLA in degrading Dalai Lama's regime and consolidating its position in Tibet, politically and militarily. Dalai Lama was eventually coerced to sign the 1951 agreement. Extensive reconnaissance of the areas bordering India was done and construction of national highway 219 was undertaken through Aksai Chin connecting Lhasa in Tibet to Xinjiang. The Indian intelligence, though reporting about Chinese activities in Tibet for quite many years to a government that was not listening, had physical confrontation with the Chinese, when on November 21, 1959, Karam Singh, a Deputy Central Intelligence Officer (DCIO) of the Intelligence Bureau was killed at Kongka La (Hot Springs) in Ladakh.[20] The years that followed saw intensified Chinese intelligence activities mainly undertaken by the PLA and party apparatus in Tibet.

Following the exodus of over 80,000 Tibetans, led by the Dalai Lama, in 1959 to India and a deep sense of fear that, his influence over the Tibetans created in Chinese minds, coverage of Dalai Lama and Tibetan refugees in India became a high priority

 

item for Chinese intelligence. Ethnic Tibetans are regularly recruited and infiltrated into India, mostly through Nepal, to cover the activities of the Dalai Lama. Arrest of Pema Tsering, a former PLA combatant, on May 23, 2013 from Dharamshala in Himachal Pradesh for spying is one of the recently reported cases. He infiltrated into India a few years back, acquired an Indian voter ID card in 2011 and was masquerading as a Tibetan refugee.[21]

Intelligence coverage through diplomatic staff has remained in vogue all through and got intensified particularly after 1959. Even during Den Xiaoping's regime when this practice was discouraged, use of legal cover for intelligence operations in India remained unabated. In some instances, Chinese nationals from mainland China with illegal cover are sent to India for coverage of political intelligence, establishing contact with the insurgent and extremist groups and collecting defence related intelligence. One of the illustrative case is of Wang Qing, a young Chinese lady who operated in India using different covers before she was arrested in Dimapur (Nagaland) on January 18, 2011. She flew to Kolkata from Kunming on a tourist visa as an executive of a Chinese timber company, and visited Nagaland where she held a four hour long secret meeting with Naga insurgent leader T Muivah. She was deported and a protest note was sent by the Indian government to the Chinese embassy.

Chinese intelligence has also been active in supporting North-eastern insurgent groups and providing them with weapons, training and financial support. Coinciding with the Cultural Revolution at home, the first group of Naga insurgents, comprising 300 strong Naga rebels, led by Muivah and Isak Swu were imparted military and ideological training in Yunan in 1966 and sent to India with a consignment of arms. This trend continues till today with Chinese assisting the Assamese, Manipuri and other rebels besides Left-Wing extremists.[22] One of the recent cases of Chinese support to Indian insurgents was revealed during questioning of Anthony Shimray, who after his return from China in 2010 was arrested in Nepal. He was assured supply of 1,800 pieces of arms that included AK series rifles, M 16 rifles, machine guns, sniper rifles, and rocket launchers. The shipment was to be loaded from a port in

 

Beihei in China and sent to Cox's Bazar in Bangladesh via a shipping agent based in Bangkok.[23]

One of the marked features of China's intelligence activity in India is its close relationship with Pakistan's ISI. Besides, their close strategic relationship, the advantages enjoyed by Pakistanis in respect of language, appearance, well entrenched local networks account for the special relationship. This cooperation started way back in mid sixties with Dhaka as the operational hub where Chinese and Pakistani intelligence officers first established contacts with the North Eastern insurgents together. With the deepening of this relationship, it got extended to other areas of common interest. Daily Mail (UK) in its report dated September 30, 2012 observed that, "Chinese agencies are financing and providing assistance to Pakistan's ISI to keep insurgent groups active in the North East.[24] However, with Chinese intelligence coming of age, there are indications that it is now launching independent operations.

## Conclusion:

In last six decades, starting from a primitive party apparatus, Chinese intelligence has attained new heights and capabilities. Its intelligence apparatus is highly complex and intricately intertwined between party and the government, internal and external, civilian and military et al with parallel roots of command, control and reporting etc. All this has led to large degrees of duplication and redundancy. Though over the years, governmental machinery has taken control of large segments of intelligence activity, the party apparatus continues to reign supreme. Deeply concerned about internal security, all its intelligence agencies have a marked internal intelligence or counter-intelligence role. The PLA, over the years, has upgraded its intelligence capabilities at tactical, technological and strategic levels, particularly in Asia Pacific Region, South Asia and Central Asia. It has built an extensive technical and signal intelligence infrastructure, and its electronic intelligence capabilities have been considerably augmented by cyberspace and space based platforms. The MSS has evolved itself as the premier foreign intelligence agency and besides diplomatic intelligence, it has been aggressively hunting for technological data and systems

 

information to augment national economic and military capabilities. It continues to bank heavily on Chinese global diaspora that provides it a vast catchment area for human assets for intelligence gathering and espionage. To widen its catchment area, it is expanding its illegal cover for intelligence gathering by using commercial companies and business houses, media agencies, Chinese banks etc. Establishment of nearly 380 Confucius Institutes in 180 countries, Chinese language institutes etc. also are part of its foreign intelligence activities. China envisions for itself a big power role and, silently but steadily, is building up its intelligence capabilities commensurate to that vision.

## Image Sources:

1 http://www.trdefence.com/wp-content/uploads/2011/03/chinese-spy.jpg

2 http://www.techinasia.com/techinasia/wp-content/uploads/2013/01/china-hackers-new-york-times.jpg

# Endnotes

[1] Ministry of State Security, Intelligence Resource Program, Federation of American Scientists, accessed online at http://www.fas.org/irp/world/china/mss/history.htm

[2] Bill Gertz, Inside the Ring: Terrorists' Antics, The Washington Times, May 16, 2012, accesed at http://www.washingtontimes.com/news/2012/may/16/inside-the-ring-terrorists-antics/?page=all

[3] Ibid (3) above

[4] sinodefence.com, accessed at http://www.sinodefence.com/overview/organisation/gsd.asp

[5] sinodefence.com, accessed at http://www.sinodefence.com/overview/organisation/gsd.asp

[6] Ibid (5) above

[7] Nicholas Eftimiade, Chinese Intelligence Operations, 1994.

[8] ibid (8) above

[9] Ibid (8) above

[10] Mark A. Stokes, Jenny Lin and L.C. Russell Hsiao, The Chinese People's

 

Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure, Project 2049 Institute, November 11, 2011

[11] Many instances of cyber attacks on countries like the US, Canada, Japan and India have been tracked to China. On the internal security front it is being used to contain and counter liberal and democratic ideas of political dissidents.

[12] Nigel Inkster (2010): China in Cyberspace, Survival: Global Politics and Strategy, 52:4, 55-56, IISS

[13] Tracking Ghost net: Investigating a cyber espionage network, Information Warfare Monitor, March 29, 2009. accessed at http://www.infowar.monitor.net/ghostnet

[14] Mandiant report, accessed at http://intelreport.mandiant.com/

[15] Willy Lamb, "Beijing beefs up Cyber Warfare capacity", Asia Times, Feb 9, 2010

[16] Foreign spies stealing US economic secrets in cyberspace – Report submitted to Office of the National Counterintelligence Executive, accessed at http:// www.ncix.gov/publication/reports/fecie_all/

[17] Ellen Nakashima, 'Confidential report lists US weapons system designs compromised by Chinese cyberspies. The Washington Post, May 28, 2013, accessed at http://articles.washingtonpost.com/2013-05-27/world/39554997_1_u-s-missile-defenses-weapons-combat-aircraft

[18] CBC News, Oct 11, 2012, 'Former Nortel executive warms against working with Huawei', accessed at http://www.cbc.ca/news/business/story/2012/10/11/pol-huawei-nortel-experience.html

[19] Ibid (13) above.

[20] Ram Pradhan, Debacle to revival: Y.B. Chavan as Defence Minister, 1962-65.

[21] The Indian Express, May 24, 2013, accessed at http://www.indianexpress.com/news/suspected-chinese-spy-arrested-from-dharamsala/1119797/

[22] N Manoharan, China's Involvement in India's Internal Security Threats: An Analytical Appraisal, Vivekanda International Foundation, 2012, accessed at

[23] Is China backing Indian Insurgents, The Diplomat, January 22, 2011, accessed at http://thediplomat.com/2011/03/22/is-china-backing-indian-insurgents/

[24] Abhishek Bhalla, Daily Mail (UK), September 30, 2012, accessed at http://www.dailymail.co.uk/indiahome/indianews/article-2210988/China-inter-services-intelligence-touch-RAW-nerve-Northeast.html

# About the VIVEKANANDA INTERNATIONAL FOUNDATION

The Vivekananda International Foundation is an independent non- partisan institution that conducts research and analysis on domestic and international issues, and offers a platform for dialogue and conflict resolution. Some of India's leading practitioners from the fields of security, military, diplomacy, government, academia and media fields have come together to generate ideas and stimulate action on national security issues.

The defining feature of VIF lies in its provision of core institutional support which enables the organization to be flexible in its approach and proactive in changing circumstances, with a long-term focus on India's strategic, developmental and civilisational interests. The VIF aims to channelize fresh insights and decades of experience harnessed from its faculty into fostering actionable ideas for the nation's stakeholders.

Since its establishment, VIF has successfully embarked on quality research and scholarship in an effort to highlight issues in governance and strengthen national security. This is being actualized through numerous activities like seminars, round tables, interactive-dialogues, Vimarsh (public discourse), conferences and briefings. The publications of the VIF form the lasting deliverables of the organisation's aspiration to impact on the prevailing discourse on issues concerning India's national interest.

**VIVEKANANDA INTERNATIONAL FOUNDATION**
3, San Martin Marg, Chanakyapuri, New Delhi – 110021
Tel: 011-24121764, Fax: 011- 24106698
Email: info@vifindia.org, Website: http://www.vifidia.org