Cyber Security:
Avoiding a 2020 Pearl Harbour

Gurmeet Kanwal

Cyber Meltdown 2020: The First Battle for Ghazwa-e-Hind

January 15, 2020, 1000 hours

The mellow rays of the winter sun glinted off the Drum Major's mace as the colourfully attired pipes and drums band marched past the Chief of the Army Staff to the stirring strains of *Deshon ka Sartaj Bharat* at the end of the Army Day parade. In the speech that followed, the Chief exhorted the Army to be vigilant and prepared to resolutely face the challenges being constantly posed by the neighbour across the western border. The speech was telecast live to the nation and to almost half a million men deployed all along the border, waiting in a state of full readiness in strike corps concentration areas, following a major terrorist strike that led to the breakdown of diplomatic relations. As the Chief walked across to join the foreign diplomats and other guests for tea, his Military Attaché (MA) received a message on his secure cellular phone that the Command Information and Decision Support System had gone on the blink since 0945 hours and that the systems engineers were working furiously to get it operational again. The MA decided to keep the news to himself for the time being and posted an aide de camp to keep in touch with the Military Operations Directorate at the Army Headquarters.

Brigadier **Gurmeet Kanwal** (Retd) is former Director, Centre for Land Warfare Studies, New Delhi.

1030 to 1115 hours

A series of seemingly unrelated and unprecedented events shook the nation's security, information, financial, trade, communications and transportation infrastructure. At 1030 hours, the Finance Minister and the Governor of the Reserve Bank of India (RBI) were informed that the master control network that facilitates inter-bank operations, including the use of ATMs had collapsed and no business could be transacted. The computers were automatically crediting and debiting millions of rupees from one account to another in an unpredictable manner. At 1040 hours, the RBI Governor gave permission to shut down the banking network and go into manual mode.

At 1045 hours, screen-based on-line trading systems at the National Stock Exchange and Bombay Stock Exchange malfunctioned; circuit breakers automatically halted further trading till the fault could be rectified. The engineers suspected that a 'logic bomb' that had been set to activate at a predetermined time had 'exploded'. Chaotic scenes were witnessed inside and outside the two exchanges.

At 1050 hours, the national network linking all ATCs (Air Traffic Controls) at international and domestic airports began generating false tracks and had to be shut down. The controllers at Palam Airport switched to manual control to assist flights circling overhead to land; take-offs and all other operations were suspended and chaos reigned in the air as well on the ground.

At 1100 hours, the Telecommunications Minister was informed that the computers controlling the telephone networks were behaving erratically and that all telephone and videophone calls, fax and e-mail messages and telegrams were being corrupted and directed to wrong destinations; software engineers were analysing the problem. At 1115 hours, his permission was sought to shut down the nation's telecom networks and to implement the contingency scheme to provide limited emergency services on standby circuits so that the computer virus suspected to have zapped the automatic electronic switching stations could be isolated and purged from the system.

1130 hours

At 1130 hours, the National Security Adviser (NSA) told the Prime Minister of the large-scale cyber crisis that was rapidly spreading across the country. At the same time, the Cabinet Secretary authorised the activation of the national emergency communications system and convened a meeting of the National Crisis Management Committee (NCMC). Members of the committee, mostly Secretaries to the Government of India, who could be reached, were told to drop everything and rush to South Block.

Suddenly, without warning, the railways' telecom and traffic control networks stopped responding to commands and electronic routers went on the blink, throwing into jeopardy the fate of thousands of passenger trains and goods trains hurtling over the rails. About five years earlier, a certain left-leaning Railway Minister had prevailed on the empowered Group of Ministers (GoM) to permit the installation of Chinese routers and switches; some of these were among the first to malfunction. The Chairman of the Railway Board reluctantly decided to order all trains to be manually stopped at the next station. The order, however, could not be conveyed to many of the smaller stations.

Soon after this, the defence communications network, named Trishul, the armed forces command and control and communications network, began spewing meaningless gibberish on all control console screens despite the best encryption system having been incorporated. The vital link between the Joint Operations Planning Centre of the Chief of Defence Staff (CDS) and missile control and launch centres for the Agni-I, II and III missile brigades broke down. Contingency communications plans based on the newly-laid Optical Fibre Cable (OFC) automatically began to operate.

Simultaneously, the national power grid began to trip and the lights went out one by one in all the north Indian states. The Defence Minister, who was formulating the strategy for the next round of elections at his party headquarters in Secunderabad, could be reached only by VSAT satellite phone, courtesy a multinational company providing commercial service over the Iridium satellite network. He was informed about the seamless crisis enveloping the nation and the armed forces. Around this time, the master control facility at the Bhopal satellite centre reported that a massive cyber attack had been launched on its computer network, but the firewall had held. However, links to the Gagan series of indigenous satellites that provided Global Positioning System (GPS) navigation had been disrupted.

At 1145 hours, tweeting from inside his cosy jail cell in Lahore, Zaki-ur-Rehman Lakhvi, the operational commander of the Lashkar-e-Tayyeba (LeT), said, "The battle for Ghazwa-e-Hind has begun. The infidels will pay for all their sins." The tweet began to trend all across the large expanse of the Sunni Caliphate in West Asia and on Facebook, Tumblr, Google+, Pinterest and other social networking sites within seconds. It was soon being widely reported by CNN, BBC and other international news channels.

1200 hours

The Prime Minister called for an emergency meeting of the Cabinet Committee on Security (CCS). The members of the CCS moved as per Standard Operating Procedure (SOP) by helicopter from the Air Force Station, Palam, to the underground National Command Post outside Delhi. Due to the extensive communications breakdown, only half the members could be reached initially. The National Crisis Management Committee launched a damage limitation exercise in accordance with contingency plans, except that the complete breakdown of normal communications considerably slowed down the execution of approved responses.

Even as the NSA stood up to commence his briefing to the CCS regarding the origin and the magnitude of the ongoing crisis, the extent of damage, the effect on national vital interests, the immediate vulnerabilities, the political, diplomatic and military options to deal with the emerging situation and his tentative recommendations, news came in that the newly-installed, ultra-modern Air Defence Ground Environment System (ADGES) of the Indian Air Force (IAF) had crashed, rendering the nation's air defences prone to a virtually undetectable air offensive by the adversary. Air defence fighter aircraft of the IAF were scrambled immediately and the forward airfields went into 'runway alert' mode.

Besides conflict on land, at sea, in the air and in space, one of the primary dimensions of future wars will be the cyber-space medium linking computers and information networks. Such wars in the fourth dimension have come to be known as "cyber wars".

It was in a sombre mood that the top brass of the nation's security planning apparatus, including the Chief of Defence Staff and the three Services Chiefs and their Directors General of Operations, heard a visibly embarrassed National Security Adviser, also India's Cyber Tsar, outline the contours of the unprecedented preemptive cyber-offensive launched by a wily and ruthless adversary. Clearly, the nation had been caught off guard as the adversary had exhibited an unanticipated ability to wage war without a shot being fired. The cyber offensive launched against India was the electronic equivalent of the Pearl Harbour disaster.

Cyber War: A New Form of Warfare

Besides conflict on land, at sea, in the air and in space, one of the primary dimensions of future wars will be the cyber space medium linking computers and information networks. Such wars in the fourth dimension have come to be known as "cyber wars". In the coming decades, the ability to wage war in cyber space is likely to acquire a deterrent value that rates between the threat of a conventional military attack and a nuclear strike. The strategic landscape has changed forever, somewhat like when nuclear weapons first appeared on the scene in 1945. Regardless of what term is used to describe this new war-form of the future, it is clear that an information and knowledge driven new type of war-form has emerged. Its manifold nuances and far-reaching implications need to be studied and analysed in detail so as to formulate a viable national-level strategy to defend against it as well as wage it successfully.

Future wars between contending protagonists are likely to be all-encompassing, perpetually ongoing conflicts. The distinction between peace and war will be blurred. Not all military operations in future will be violent and physically destructive.

Future wars between contending protagonists are likely to be all-encompassing, perpetually ongoing conflicts. The distinction between peace and war will be blurred. Not all military operations in future will be violent and physically destructive. Since the aim will be to subdue the enemy without fighting, non-violent operations to cripple a society and to deny it the ability to wage war may be launched to wreck its information grids and systems, banking and telecom systems, transportation and traffic control systems, power grids and computer networks, even during seemingly peaceful interludes. At the core of the new military doctrine for fighting what Alvin and Heidi Toffler have called “Third Wave” wars, will be the concept that the control and manipulation of information and widespread knowledge of the enemy’s military, industrial, diplomatic, political, civic and cybernetic assets, with a view to paralysing them without actual fighting, will be essential prerequisites for success. The weapons of choice will be computer 'logic' bombs set to detonate at a particular time, electronic viruses to infect the adversary's computers, non-nuclear high-energy Electro-Magnetic Pulse (EMP) to 'fry' the components of radars, electronic networks and computers and advanced 'hacking' techniques to gain access to the adversary's computer networks and manipulate them to own advantage.

The weapons of choice will be computer 'logic' bombs set to detonate at a particular time.

The emergence of the cyber war battlefield will be both an evolutionary and a revolutionary development. In so much as it will utilise most of the existing military concepts, weapons systems and organisations, it will be evolutionary. It will be revolutionary in that it will seek to provide new capabilities to commanders to influence and subvert the will of their opponents through imperceptible but nonetheless debilitating non-violent means as a prelude to more conventional operations, should they become necessary—a type of cybernetic intelligence preparation of the battlefield.

The military is generally characterised as an extremely conservative force in society—a rigidly hierarchical organisation which is resistant to change and does not easily accept revolutionary new doctrines. It is in this context that the peep into future history, conjectured here, is offered as a plausible scenario in the mega media age ahead. Only forward looking and innovative armed forces will be able to take up the challenges of integrating information-age technologies into military operations to dominate the cyber war battlefields of the future so as to subdue the adversary without fighting.

While much will change in the mega media age, cyber wars will not be "remote, bloodless, sterile or risk-free." There will be a marked reliance on knowledge and information. Preparation of the battlefield will involve gathering maximum intelligence about the enemy, while preventing him from knowing much about oneself. It will imply turning the "balance of information and knowledge in one's favour, especially if the balance of forces is not.” The aim will be to dislocate, paralyse and incapacitate the opposing commanders’ minds to force the adversary to capitulate without fighting. The results which are likely to be achieved will be decisive and out of all proportion to the effort applied. However, fundamental military revolutions, particularly evolutionary ones, require detailed analysis, thorough study and meticulous experimentation before they can be absorbed into the doctrinal lexicon and implemented at the functional level.

Only forward looking and innovative armed forces will be able to take up the challenges of integrating information-age technologies into military operations to dominate the cyber war battlefields of the future so as to subdue the adversary without fighting.

Threats and Vulnerabilities

India’s rapidly growing economy is almost as heavily dependent on computer and communications networks as the economies of the developed Western countries. It also faces similar cyber security challenges. The Indian armed forces and the Central Armed Police Forces (CAPFs) are becoming increasingly more dependent on computers for command, control, communications and surveillance than before. The country is relying more and more on e-governance. The national e-governance programme seeks to provide more than 1,200 services online. The number of internet users in India grew from 1.4 million in 1999 to over 15 million in 2003 and over 100 million today. Exponential growth is expected in the next 15 to 20 years as internet penetration increases. The Indian Railways sold 44 million tickets worth US$ 875 million online in 2009. India’s critical information infrastructure includes the telecom sector, the banking sector, the stock exchanges, the aviation sector, the energy sector and other utilities.

Key cyber security vulnerabilities include the following:

- India does not design and manufacture its own computer chips and operating systems and is entirely dependent on imports. Processors, routers, crypto and security solutions are all being outsourced from abroad. Geographic Information System (GIS) and Management Information System (MIS) solutions are also mostly sourced from other countries. All of these are vulnerable to manipulation at the manufacture stage.The Stuxnet virus that had almost completely destroyed Iran's Natanz nuclear facility by causing the centrifuges to spin out of control is a good example of surreptitiously taking over control of a network. According to cyber security expert Ralph Langer, it was a dangerous cyber-weapon that "changed global military strategy in the 21st century."

India's critical information infrastructure includes the telecom sector, the banking sector, the stock exchanges, the aviation sector, the energy sector and other utilities.

- India's capacity to check the integrity of imported chips is extremely limited. In fact, there is apprehension in government circles about allowing Chinese companies like Huawei to bid for contracts in the telecom sector, particularly where the armed forces are the direct users.
- *Jihadi* groups targeting India have been honing their cyber skills and also trying to recruit cyber experts – a potentially alarming development.
- There is a need to ensure that background checks are carried out on the workforce employed for the establishment and functioning of critical networks. This has not been been done so far.

India does not design and manufacture its own computer chips and operating systems and is entirely dependent on imports. Processors, routers, crypto and security solutions are all being outsourced from abroad. Geographic Information System (GIS) and Management Information System (MIS) solutions are also mostly sourced from other countries.

Hacking of computer networks is also a key vulnerability. Indian computer networks and e-mail accounts have been hacked frequently by state actors. Some incidents are given below:

- Former National Security Adviser M K Narayanan had told *The Times,* London, before laying down his office that China's cyber warriors had hacked into computers in the Prime Minister's Office (PMO) on December 15, 2009. At least 30 computers may have been penetrated.
- Chinese cyber spies were also reported to have broken into, and stolen documents from, hundreds of government and private offices around the world, including those of the Indian Embassy in the US.
- According to data released by the Computer Emergency Response Team-India (CERT-IN), 90, 119, 252 and 219 government websites were defaced by various hacker groups in the years 2008, 2009, 2010 and January-October 2011, respectively.
- On July 12, 2012, in the "biggest cyber attack on the country's official computer networks, over 100,000 e-mail addresses of top government officials were hacked in a single day." An official said, "The MEA (Ministry of External Affairs) and the MHA (Ministry of Home Affairs) took the biggest hit… strategic information related to critical sectors, including troop deployment, was compromised." An National Technical Research Organisation (NTRO) official said, "We would not like to name the state actors, but D4 – destroy, disrupt, deny and degrade – process was initiated and counter offensive launched."[1]

Threat from China

There is a need to ensure that background checks are carried out on the work-force employed for the establishment and functioning of critical networks. This has not been been done so far.

While the emerging cyber threats originate from various sources, including non-state actors, among nation-states, the Chinese are suspected to be the leading purveyors of offensive cyber strategies and Pakistan is working hard to play catch up. Though information about the People's Liberation Army's (PLA) cyber warriors has begun to appear in the public domain only recently, PLA watchers across the world have known for long about China's well-conceived doctrine on information operations and cyber war. China's cyber war doctrine is designed to level the playing field in a future war with better equipped Western armed forces that rely on Revolution in Military Affairs (RMA) technologies and enjoy immense superiority in terms of weapons platforms and Intelligence, Surveillance and Reconnaissance (ISR) and command and control networks. The Chinese Army uses more than 10,000 cyber warriors with degrees in information technology to maintain an e-vigil on China's borders. "Chinese soldiers now swipe cards and work on laptops as they monitor the border with great efficiency… electronic sentinels functioning 24 hours a day." Parallel to this effort, China is also engaged in raising a private army of hackers who will wage cyber war against the state's enemies from their laptops at home.

The denial of information, strategic deception and the achievement of psychological surprise have for long been an integral part of the Chinese military doctrine. The Chinese find Information Warfare (IW) extremely attractive as they view it as an asymmetric tool that will enable them to overcome their relative backwardness in kinetic military hardware. They are devoting considerable time and energy to perfecting the techniques of IW to target the rapidly modernising Western armed forces that are becoming increasingly more dependent on the software that runs computer networks

The Chinese find Information Warfare (IW) extremely attractive as they view it as an asymmetric tool that will enable them to overcome their relative backwardness in kinetic military hardware.

and modern communications. In Chinese thinking, IW presents a level playing field for projecting power and prevailing upon the adversary in future wars. However, it has not been possible to ascertain from open public sources whether IW is fully integrated with the doctrine of people's war under modern conditions or if it is still treated as a separate but complementary pattern of war (*zhanzheng xingtai*). There is also some confusion created by the use of the term informationised warfare (*xinxihua zhanzheng*) instead of IW (*xinxi zhanzheng*). However, there is no ambiguity in the manner in which the Chinese view information operations:

- Intelligence operations, which include intelligence, reconnaissance and protection.
- Command and Control (C2) operations to disrupt enemy information flow and weaken his C2 capability while protecting one's own.
- Electronic warfare by seizing the electromagnetic initiative through electronic attack, electronic protection and electronic warfare support.
- Targeting enemy computer systems and networks to damage and destroy critical machines and networks and the data stored on them.
- Physical destruction of enemy sources like information infrastructure such as Command, Control, Communication, Computer, Intelligence, Surveillance, Reconnaissance (C4ISR) through the application of firepower.

The Chinese call their pursuit of information warfare and other hi-tech means to counter Washington's overwhelmingly superior conventional military capabilities "acupuncture warfare", a term that first surfaced in a 1997 PLA National Defence University publication entitled

“On Commanding War-Fighting under High-Tech Conditions”. Acupuncture warfare (also called “paralysis warfare”) was described as “paralysing the enemy by attacking the weak link of his command, control, communications and information as if hitting his acupuncture point in *kung fu* combat.” Acupuncture warfare is a form of asymmetrical warfare dating back to the teachings of Sun Tzu, China’s preeminent military strategist from the 5th century BC. For quite some time now, the PLA has been simulating computer virus attacks in its military exercises. According to a US Congressional Research Service (CRS) report entitled “Cyber Warfare”, authored by Steve Hildreth, China is developing a strategic information warfare unit called “Net Force” to neutralise the military capabilities of technologically superior adversaries. This new information warfare unit will “wage combat through computer networks to manipulate enemy information systems spanning spare parts deliveries to fire control and guidance systems.”

China is developing a strategic information warfare unit called “Net Force” to neutralise the military capabilities of technologically superior adversaries.

With Indian society becoming increasingly dependent on automated data processing and vast computer networks, India will also become extremely vulnerable to such information warfare techniques.Besides the threat of Distributed Denial of Services (DDoS) attacks on its critical information infrastructure, India faces the threats of cyber warfare, cyber terrorism, cyber espionage and cyber crime. India’s inimical neighbours have ensured that the cyber security challenges faced by India are more pronounced than even those faced by many European countries. China’s “one million laptop warriors” are a major cause for concern.Major infrastructure like telecom, railways, air traffic control, banks, stock exchanges, power grids and the C4I2SR systems of the armed forces are all dependent on computer networks, which are vulnerable to cyber attacks and cyber manipulation. The nothingness of cyber space connects China's laptops warriors directly with Delhi, Mumbai, Kolkata, Chennai, Bangalore and Hyderabad and other Indian cities, as also India's strategic establishments. The fact that cyber war can be launched from virtually any place on the earth even during peace-time makes acupuncture or paralysis warfare even more diabolical.

Cyber Security Infrastructure

India has been a late starter in planning to overcome cyber security challenges. It is only recently that the Indian government has taken note of the seriousness of the threat. The enforcement of cyber security draws sustenance from the Information Technology Act, 2000, as amended by the Information Technology (Amendment) Act, 2008. The Act provides a legal framework to address the issues connected with security breaches of information technology infrastructure. The government has notified Intermediary Guidelines Rules 2011 under Section 79 of the Information Technology Act, 2000.The cyber security infrastructure includes the National Information Board, the Computer Emergency Response Team-India (CERT-IN) that scans the Indian cyber space for untoward incidents, a small number of regional CERTs and the National Technical Research Organisation (NTRO).

The National Informatics Centre (NIC) provides network and systems services to the central and state government departments and also conducts periodic security audits. All government departments either have already formulated or are in the process of formulating cyber security policies for the protection of their cyber networks. The government is known to have formulated a crisis management plan. Periodic information technology security risk assessments are being carried out to determine the acceptable level of risks consistent with the criticality of functional or business requirements. The Ministry of Defence (MoD) has established the Defence Information Assurance and Research Agency (DIARA) to deal with all cyber security related issues within the armed forces. The Department of Information Technology has initiated a programme on cyber-forensics specifically focussed on developing infrastructure for investigation and training of law enforcement and judicial officers in the use of cyber forensic tools.

The Cabinet Committee on Security has initiated steps to evolve a comprehensive cyber security strategy. Mr. Gulshan Rai of CERT-IN, was named the first National Cyber Security Coordinator (NCSC). It is proposed to establish a National Critical Information Infrastructure Protection Centre (NCIPC). This will be a command and control nerve centre that will monitor protection of the critical infrastructure. The NCIPC will, in all probability, be managed by the NTRO, India's technical intelligence gathering agency. The NTRO and Defence Intelligence Agency (DIA) are best suited to plan and execute offensive cyber operations. The National Security Adviser (NSA) will in all probability be at the apex of India's cyber security strategy as the chief planner and trouble-shooter.

The NTRO and Defence Intelligence Agency (DIA) are best suited to plan and execute offensive cyber operations. The National Security Adviser will in all probability be at the apex of India's cyber security strategy as the chief planner and trouble-shooter.

A task force on cyber security assembled by the Institute of Defence Studies and Analyses (IDSA), New Delhi, made the following salient recommendations in its report:[2]

- The NSA should be the overall coordinator of the planning and execution of India's cyber security policy.
- A Cyber Coordination Centre should be established at the operational level.
- The MHA should be the nodal agency for handling cyber-terrorism and cyber-crime.

A nodal agency must be created to spearhead India's cyber war efforts under a national cyber security adviser who should report directly to the NSA.

- Headquarters (HQ) Integrated Defence Staff (IDS) should be the nodal agency for preparing the country for cyber warfare in all its dimensions.
- The National Security Council Secretariat (NSCS) should be the nodal agency for coordinating the efforts to protect the critical infrastructure of the country.
- The Department of Information Technology should be tasked with creating the necessary situational awareness, strengthening the public-private partnership, promoting international cooperation and other residual measures.
- The Department of Information Technology's CERT-IN should be the nodal agency to create and share cyber-space situational awareness in the country.
- Cyber security education, Research and Development (R&D) and training should be an integral part of the national cyber security strategy.
- Disaster management and recovery must be an integral part of the national cyber security strategy.

Avoiding a Cyber Pearl Harbour

India can ill-afford to continue to ignore this new challenge to its security as it may result in a cyber Pearl Harbour in a future conflict. High costs can be imposed on the country even during peace-time. The country should adopt a carefully thought through inter-ministerial, inter-departmental, inter-Services, multi-agency approach to dealing with emerging cyber warfare threats and must develop appropriate responses. No single agency in India is charged with ensuring cyber and IT security. A nodal agency must be created to spearhead India's cyber war efforts under a national cyber security adviser who should report directly to the NSA. It is apparent from the announcements made in November 2012 that the government is taking prompt action on the pragmatic recommendations made by the IDSA Task Force and those made by other organisations like the Confederation of Indian Industries (CII). A closely coordinated public-private partnership is necessary to overcome future infrastructure security challenges.

The armed forces must be part of the overall national effort from the very beginning so that emerging tactics, techniques and procedures can be incorporated into doctrine and training. Hence, like other major armed forces, India too needs a Cyber Command to lead efforts within the military to safeguard computer networks from hackers and cyber attacks and to plan and execute offensive cyber warfare strategies. The strategy must be defensive to guard India's vulnerable assets, such as military command and control networks and civilian infrastructure dependent on the use of cyber space, as well as offensive to disrupt the adversary's C4I2SR systems and develop leverages that can be exploited at the appropriate time. With some of the finest software brains in the world available to India, it should not prove to be an insurmountable challenge.

Like other major armed forces, India too needs a Cyber Command to lead efforts within the military to safeguard computer networks from hackers and cyber attacks and to plan and execute offensive cyber-warfare strategies.

Notes

[1] Ajmer Singh, "Over 10,000 e-mail IDs hit in 'Worst' Cyber Attack," *The Indian Express*, December 18, 2012.

[2] *India's Cyber Security Challenge*, IDSA Task Force Report (New Delhi: Institute for Defence Studies and Analyses, March 2012).